jamk

# The Evolution of Mobile Malware

Arttu Reijonen

Master's thesis
April 2024
Master of Engineering in Information Technology, Cyber Security

jamk | Jyväskylän ammattikorkeakoulu
University of Applied Sciences

jamk

**Description**

**Reijonen, Arttu**

**The evolution of mobile malware**

Jyväskylä: Jamk University of Applied Sciences, April 2024, 65 pages.

Degree Programme in Cyber Security. Master's thesis.

Permission for open access publication: Yes

Language of publication: English

**Abstract**

From the discovery of the first mobile malware in 2004 to the advanced variants encountered in 2024, this thesis explores how mobile malware has evolved in parallel with the development of mobile devices. The research is structured based on a comprehensive analysis of the development of mobile malware, its consequences for users and society, and the actions taken by the cybersecurity community in response to these constantly evolving risks. The study clarifies the evolution of mobile malware from minor inconveniences to advanced tools with the ability to cause substantial financial and personal harm, employing a comprehensive literature review, analysis of case studies, and investigation of statistical data.

The key findings reveal a significant rise in the complexity and diversity of mobile malware, which may be attributed to the advancements in mobile device technology and the increasing importance of these devices in our daily lives. The dynamic and diverse characteristics of mobile threats is highlighted by the presence of financially motivated malware, the advancement of evasion techniques, and the emergence of state-sponsored and politically motivated malware. Moreover, the thesis examines the consequences of developing technologies on the evolution of mobile malware and provides predictions on future trends.

This study highlights the importance of adopting a comprehensive approach to mobile security, which includes user education, innovative technology solutions, and comprehensive cybersecurity policies. Such measures are essential in order to effectively tackle the risks and consequences associated with mobile malware. The growing number of mobile malwares is not only a technological challenge but also a political one that requires a cooperative effort to protect the security and confidentiality of digital data in an ever more mobile society.

**Keywords/tags (subjects)**

Mobile Malware, Cybersecurity, Smartphone Security, Mobile Technology, Cyber Threats, Digital Privacy.

jamk

**Kuvailulehti**

**Reijonen, Arttu**

**Mobiilihaittaohjelmien kehitys**

Jyväskylä: Jyväskylän ammattikorkeakoulu. Huhtikuu 2024, 65 sivua.

Kyberturvallisuuden koulutusohjelma, ylempi ammattikorkeakoulututkinto, YAMK-opinnäytetyö

Julkaisun kieli: Englanti

Julkaisulupa avoimessa verkossa: kyllä

**Tiivistelmä**

Tämä opinnäytetyö tutkii, kuinka mobiilihaittaohjelmat ovat kehittyneet rinnakkain mobiililaitteiden kehityksen kanssa, kun ensimmäinen mobiilihaittaohjelma löydettiin vuonna 2004 aina edistyneempään muunnelmiin, joita löydettiin vuonna 2024. Tutkimus perustuu kattavaan analyysiin mobiilihaittaohjelmien kehityksestä, sen vaikutuksista käyttäjiin ja yhteiskuntaan sekä kyberturvallisuusyhteisön toimiin vastatakseen näihin jatkuvasti kehittyviin uhkiin. Tutkimus havainnollistaa mobiilihaittaohjelmien kehitystä pienistä haitoista edistyneisiin työkaluihin, jotka voivat aiheuttaa merkittäviä taloudellisia ja henkilökohtaisia vahinkoja. Tutkimus hyödyntää kattavaa kirjallisuuskatsausta, tapaustutkimusten analysointia ja tilastotietojen tutkimista.

Tutkimuksen tulokset paljastavat mobiilihaittaohjelmien monimutkaisuuden ja monimuotoisuuden lisääntyneen merkittävästi, mikä voi johtua mobiililaitteiden teknologian edistymisestä ja näiden laitteiden kasvavasta merkityksestä jokapäiväisessä elämässämme. Mobiiliuhkien dynaamisia ja monipuolisia ominaisuuksia korostavat taloudellisesti motivoituneiden haittaohjelmien lisääntyminen, evaasointitekniikoiden kehittyminen sekä valtion tukemien ja poliittisten haittaohjelmien ilmaantuminen. Lisäksi opinnäytetyössä tarkastellaan teknologioiden kehittämisen vaikutuksia mobiilihaittaohjelmien kehitykseen ja annetaan ennusteita tulevaisuuden trendeistä.

Tämä tutkimus korostaa kokonaisvaltaisen lähestymistavan omaksumista mobiiliturvallisuuteen, joka sisältää käyttäjäkoulutuksen, innovatiiviset teknologiaratkaisut ja kattavan kyberturvallisuuspolitiikan. Tällaiset toimenpiteet ovat välttämättömiä, jotta mobiilihaittaohjelmiin liittyviä riskejä ja seurauksia voidaan torjua tehokkaasti. Mobiilihaittaohjelmien lisääntyvä määrä ei ole vain teknologinen haaste, vaan myös poliittinen haaste, joka vaatii yhteistoimintaa digitaalisen datan turvallisuuden ja luottamuksellisuuden suojelemiseksi yhä liikkuvammassa yhteiskunnassa.

**Avainsanat (asiasanat)**

Mobiilihaittaohjelmat, tietoturva, kyberturvallisuus, älypuhelin

**Contents**

**Figures**

# 1 Introduction

The way we work, communicate, and access information has changed as a result of mobile devices becoming an indispensable part of everyday life. The turn of the millennium marked a significant moment in the history of technology with the rise of smartphones, which not only brought unprecedented convenience but also introduced new types of challenges in the security of mobile devices users. This thesis explores the evolution of mobile malware in parallel with the development of smartphones, spanning from creation of the first mobile malware in 2004 to the present day. The goal is to also explore the origins of mobile malware, investigating its development over time, and assessing its impact on users and society at large.

## 1.1 Background

The change of the millennium witnessed the emergence of smartphones, which marked an important moment in the history of mobile technology. These devices offered users an extensive range of different capabilities, from email communication and web browsing to location services and entertainment. As smartphones and other mobile devices gained popularity, they also attracted the attention of malicious actors, leading to the development of mobile malware.

Mobile malware, malicious piece of software designed to target smartphones, tablets, and other mobile devices, has emerged as a significant threat to personal privacy, data security, and overall digital safety. With the development of smartphones, the technological landscape has evolved, and new forms of functionality and connectivity have emerged. This dynamic landscape of mobile malware evolution is marked by evolving attack vectors, complex methodologies, and an increasing influence on individuals, organizations, and society. The development of new advanced smartphones and other mobile devices additionally reflects the development of new advancements in the mobile malware technology. With each generation of new mobile devices and mobile services is being met with more complex and harmful mobile malware threats.

## 1.2 Research Objectives and Questions

The objective of this thesis is to provide an analysis of the development of mobile malware, starting from the first discovery of mobile malware in 2004 leading up to the present day in 2024. In

addition, we will provide a brief overview of the future developments in mobile technology and mobile malware. The primary objective of this thesis is to provide comprehensive research of the evolution of mobile malware since the rise of smartphones in 2000. The more specific objectives and research questions include:

1. What types of mobile malware have been the most prevalent and damaging over the past two decades?
2. How have mobile malware attack vectors and infection methods changed with the proliferation of smartphones and mobile applications?
3. How has the threat landscape of mobile malware shifted over the years?
4. How have advancements in mobile technology influenced the complexity and sophistication of mobile malware?

## 1.3 Research Method

The methodology used in this thesis combines an extensive literature review, analysis of malware case studies, examination of statistical data regarding mobile malware. This methodology provides a detailed understanding of the complex landscape of mobile malware and its effects on mobile security.

This study utilizes a variety of methodologies, including the following approaches:

- **Literature Review:** A comprehensive review of existing literature and scholarly articles will provide historical context and insight into mobile malware evolution.
- **Data Analysis:** Extensive data analysis will be conducted to evaluate trends in mobile malware, incorporating statistical data on malware samples and threats.
- **Case Studies:** Case studies of notable mobile malware incidents will be examined to gain deeper insights of the strategies and patterns used by malicious actors.

## 1.4 Structure of the thesis

The structure of this thesis is organized to facilitate an exploration of the evolution of mobile malware in tandem with smartphone development. Through this comprehensive exploration, this thesis aims to provide deeper knowledge on the evolution of mobile malware and its combined history with the development of smartphones, which will lead to a deeper understanding of mobile security in the digital age.

The thesis begins with introduction and provides the background information on the topic of the thesis. Following the introduction, a history smartphones and mobile malware will be presented, along with a summary of its various types and the risks they represent. We will next examine the development of smartphones and mobile malware from 2000 and 2024. Ultimately, the gathered data will be analyzed allowing the formulation of predictions of the future of mobile malware and mobile devices.

# 2 Historical Overview

## 2.1 The Rise of Smartphones in 2000

As a result of the launch of smartphones at the turn of the millennium, an important milestone in the development of mobile devices was reached. Communication, access to information, and the management of people's day-to-day lives were all drastically changed as a result of creation of these devices. BlackBerry models were among the first smartphones that gained widespread popularity, especially with customers in the business domain. Through the introduction of encrypted communications, a built-in keyboard that makes typing faster and easier, and emailing functionality, they defined a standard for the operation of future devices and a commercial benefit.

During this period, companies such as Nokia, BlackBerry, and Palm were at the leading edge of the smartphone market. In particular, Nokia was a strong competitor, thanks to its Symbian platform, which enabled the company to manufacture an extensive range of smartphones that were appealing to both general consumers and business personnel. In 2007, Nokia held a market share of 49.4 percent of the whole mobile market (Ettinger, 2023). Email, web browsing, multimedia capabilities, and access to a wide range of services were some of the functionalities that these devices, which established the groundwork for modern smartphones, offered.

The introduction of the Apple iPhone in 2007 was another groundbreaking moment. With its simple touchscreen interface and user-friendly design, the iPhone completely changed the smartphone market and improved customers experiences while using their devices. In addition, it created the concept of an app store, which is a centralised place where users may download applications developed by third parties. This resulted in an enormous increase of the capabilities of smartphones beyond the ability to make and receive phone calls and texts.

## 2.2 Mobile Malware History and Key Milestones

The advent of mobile devices also introduced new security challenges, including the emergence of mobile malware. "Cabir," the first known mobile virus, was discovered in 2004 and was designed to target devices running on the Symbian OS (Apvrille, 2014). This marked the beginning of a new era in cybersecurity, where also the mobile devices became a target for malicious actors. The development of new mobile malware has since followed the evolution of mobile technology, with each advancement in device capability being matched by more sophisticated and harmful malware variants.

Not long after Cabir, another notable example of mobile malware emerged, showcasing the growing interest of cybercriminals in exploiting mobile platforms. One such instance was the discovery of Commwarrior in 2005, which similarly to Cabir targeted Symbian devices. The capacity of Commwarrior to spread via MMS messages, which was an unusual attack vector at the time, made it interesting (Apvrille, 2014). This demonstrated the adaptability of creators of malware to take advantage of mobile specific communication mechanisms for replication. This represented a significant shift in malware threats, from those that required physical access to devices or relied on user actions, such as downloading and executing malicious software, to those capable of spreading autonomously across networks.

This Trojan was a mobile version of the well-known Zeus Trojan, which initially targeted computers. Developed to infect mobile devices running Symbian and Android operating systems, ZitMo first appeared in the year 2010. The main objective of the attack was to steal mobile transaction authentication numbers, which are used as a two-factor authentication method in online banking services. The attackers could get around safety measures and access victims' bank accounts without authorization. ZitMo marked a significant shift in malware creation, suggesting that hackers were beginning to be finding ways to gain profit financially from these attacks on mobile devices (Maslennikov, ZeuS-in-the-Mobile – Facts and Theories, 2011).

The emergence of these early mobile malware variants was just the tip of the iceberg. More advanced methods of evasion, distribution, as well as exploitation were introduced by every new generation of malware. As mobile devices grew in popularity and functionality, they became in-

creasingly essential to both private and professional lives, storing a wide range of sensitive information. As a result, attackers found them to be more and more appealing targets, which caused a variety of malware types and delivery methods to emerge. As a result, the history of mobile malware is not limited to a handful of single events, but rather represents an ongoing competition between criminals wanting to take advantage of new developments in technology and cybersecurity experts attempting to protect users' information.

## 2.3 Initial Challenges and Vulnerabilities in Early Smartphones

The early generations of smartphones encountered numerous security challenges, including restricted processing power, insufficient security features, and limited awareness about mobile security among users and developers. Despite their innovation, early mobile operating systems failed to anticipate the scope and complexity of threats that would appear, creating an environment that was open to exploitation. Frequently, the security models were too simplistic, emphasising user experience and fundamental functionality over a thorough security plan. Because of this oversight, there were several opportunities for criminals to exploit vulnerabilities for unauthorised access, data theft, and malware distribution. Furthermore, smartphones' groundbreaking connectivity characteristics also made them vulnerable. For instance, Bluetooth was frequently used as a distribution channel for early mobile malwares. Security oversights negated the ease of wireless connection, making it possible for viruses and worms to spread from one device to another with little to no human involvement. For example, Symbian, the operating system for Nokia smartphones, did not include features like the need for signed applications until 2006 (Snyder, 2019).

On the user side, there was a lack of awareness about the potential risks associated with mobile devices. Treating mobile devices as more secure than PCs, many users overestimated the risk of malware infection and the importance of security controls like frequent software updates and cautious downloading behaviour. To capitalise on this ignorance, attackers employed social engineering, phishing, and other tactics to trick users into compromising their own devices.

On the development side, innovation and functionality were sometimes given more priority over security in the rush to get new features and applications to market. Therefore, operating system

updates and programmes were released without proper security testing, leaving open the possibility of exploiting vulnerabilities and backdoors. The open nature of Android and other mobile ecosystems made it possible for third-party apps to spread from sources other than the official app stores. Since many of these sources were not subject to strict security checks, they could easily act as transmitters of malware.

During the early stages of smartphone use, the regulatory environment did little to mitigate these risks. Data protection laws and regulations specific to mobile computing were lacking or non-existent, leaving a grey area in terms of legal protection and recourse for affected users. Due to the absence of regulations, it was challenging to successfully tackle mobile malware and many users were not aware of their rights or the best practices for device protection.

## 2.4 Mobile Malware Types

### 2.4.1 Trojans

Trojans are not self-replicating like viruses or worms, yet they can be equally harmful. They are called "Trojans" after the ancient Greek story of the wooden horse that led to the fall of the city of Troy. Trojan horses operate in a similar manner, deceiving individuals into running them by pretending to be safe or useful applications and once activated, a Trojan can perform a vast range of malicious activities.

Users are typically tricked into executing Trojans through social engineering techniques, which are a common method of spreading malicious programs. This may occur as a result of downloading software from websites that are not trustworthy or that have been compromised, as well as through email attachments or deceptive advertisements.

### 2.4.2 Spyware

Spyware is a type of malware that is designed to secretly monitor and collect information from the target device without the user's consent, often leading to privacy breaches. It can be installed on a user's device through deceptive methods, such as included with legitimate software, through vulnerabilities in software, or by tricking the user into installing it by pretending to be a legitimate application.

The information that is collected can be used for a variety of harmful purposes, including identity theft, fraud, spying on companies, or targeted advertising based on the user's personal likes and habits. Detecting and removing spyware can be challenging because it is designed to hide its presence from the user. In addition, spyware usually disguises itself as legitimate software or interacts with it.

### 2.4.3 Ransomware

By encrypting the data on the device, ransomware prevents unauthorized users from accessing the device or certain files on the device. In most cases, attackers will demand ransoms in order to decrypt the data. In the end, it is a form of digital extortion, with the criminals often demanding payment in cryptocurrency in order to either release the decryption key or unlock the device. Because it is difficult to trace, cryptocurrency has become a popular method of payment among criminals.

A device can be infected with ransomware by a variety of techniques, including phishing emails that contain malicious attachments, exploiting vulnerabilities in software, or through deceptive adverts on websites.

### 2.4.4 Adware

Adware automatically delivers advertisements, which can be intrusive and sometimes serve as a vector for more malicious payloads which can possibly lead to privacy breaches. Pop-up adverts, banners within software or web browsers, and unwanted email messages are all examples of the types of advertisements that might be displayed to user. Although there are some instances of adware that are not malicious, the term has come to be associated with software that is unwanted or intrusive and that impacts the user experience as well as their privacy. The primary purpose of adware is to produce profit for its creators by displaying advertisements to the user.

### 2.4.5 Worms

The malicious software known as worms have the ability to replicate itself and spreading across networks by taking advantage of vulnerabilities in software that is running on mobile devices.

Worms take use of the fact that they can replicate themselves and move from one device to another. Unlike viruses, which require the host to spread the infection by executing or sharing the malicious file, worms may spread themselves across networks, taking advantage of vulnerabilities in operating systems, software applications, or network configurations.

Although some worms have been developed simply to spread and consume bandwidth, others carry payloads that can cause harm. These payloads may erase files, encrypt files, steal information, or develop backdoors for hackers in the future. The simple act of spreading can also be damaging because it might result in overload on the network and a decrease in the performance of the system (Santosh K. Smmarwar, 2024).

## 2.5 Mobile Malware Threats

### 2.5.1 Fake Applications

Fake applications offer a serious risk since they pretend to be legitimate applications while secretly carrying malicious code that is designed to steal personal information, control the infected device, or carry out other harmful actions. Unknowingly downloading these fake apps from unofficial sources or misleading links places users' devices and sensitive data at danger. Users may download these applications without their knowledge. The threat can be easily mitigated by ensuring that mobile applications are only downloaded from reliable sources (Guardsquare, 2019).

### 2.5.2 Open Wi-Fi

Open and unsecured Wi-Fi hotspots may expose user’s device for different types of security threats. Data transferred between your device and the network on an open Wi-Fi network is not encrypted, which leaves room for data to be intercepted and read by cybercriminals. Passwords, credit card numbers, and other private data may fall under this category (Osborne, 2023).

In order to fool people into connecting to their network, cybercriminals can create a Wi-Fi network with a name that is similar to that of an actual service. The attacker can monitor all data transmission or point users to phishing websites once they are connected to this hotspot. An attacker also might insert malicious software into a file transfer, for instance, if a user shares data across a

network. Certain malware can also use vulnerabilities in the operating system to automatically infect a device when it connects to a network. Safeguarding personal information and security of devices requires being aware of possible dangers and taking caution when using unsecured Wi-Fi networks.

### 2.5.3 SMS Spoofing

SMS spoofing is the method of manipulating a text message's sender to make it appear as though it came from a different source. This could be an alphanumeric text, like the name of a company, a person's name, or another phone number. Spoofing can be used for a variety of purposes, for example, a business may send messages to its clients using only its name rather than a phone number, or it may be employed for more malicious purposes like fraud and scams. In order to steal sensitive information or spread false information, attackers may utilize SMS spoofing to pretend to be a bank or another organization that the victim trusts.

### 2.5.4 Mobile phishing

Phishing is the deceitful act of posing as a reliable or legitimate email or SMS source in order to obtain private information. These kinds of attacks can be countered with social engineering strategies. Links in phishing emails may direct recipients to dangerous websites. Afterwards, they attempt to acquire confidential information such as credit card numbers, usernames, passwords, and confidential business information. These kinds of attacks typically involve spam emails or other messages sent to a large number of recipients, and they are rather common (Speed).

# 3 Impact of Mobile Malware

## 3.1 Privacy Breaches and Personal Data Security Risks

Malware that targets mobile devices frequently targets personal data that is saved on the device of the user, which can result in potential breaches of privacy and identity theft. There are many different types of data that can be stored on a user's device, and malicious software might gain access to all of them. These kinds of data include contact lists, emails, financial information, and location data. This not only violates the privacy of individuals, but it also puts them at danger of being targeted by malicious actors such as phishing, identity theft, and scams. In particular, spyware and Trojans are meant to silently break into devices and capture personal data without the user's knowledge or agreement. This is accomplished using covert techniques. These types of malwares take use of vulnerabilities in operating systems and programmes, as well as, in certain cases the user's lack of awareness of security precautions. It is possible for the data gained to consist of contact lists, emails, texts, as well as information regarding the user's location and activity on the internet related to browsing.

In addition, the widespread use of smartphones and their constant internet connectivity make them an ideal target for hackers. A further expansion of the attack surface and the creation of new potential for privacy violations are both prompted by the integration of mobile devices into the Internet of Things (IoT) network.

Researchers have found that the number of malware attacks on mobile devices has surged by a factor of 500% in the first few months of 2022. The study highlights the increasing concerns over mobile data security, with a significant percentage of data breaches attributed to mobile devices and especially Android devices (Henry, 2022). This data shows that data privacy and mobile security is more relevant now more than ever.

It is necessary for users and developers to use a multi-layered approach to security in order to mitigate the probability of these threats. Some of the methods in which this can be accomplished include applying patches to vulnerabilities in operating systems and applications on a regular schedule, utilising security software that can be relied upon, and practicing increased caution while

downloading applications and granting permissions to them. Additionally, regulators and communities concerned with cybersecurity are working to provide more enhanced privacy safeguards and security solutions that are more dependable in order to safeguard customers' personal information.

## 3.2 Economic and Financial Risks

The financial and economic consequences of mobile malware attacks extend beyond individual victims to also affect companies and the global economy. In addition to causing immediate financial losses, mobile malware attacks can also result in decreased productivity, reputational harm, and substantial costs related to recovery. When it comes to individuals, the consequences can range from financial losses brought on by forged transactions to the expense of removing the effects of a malware infection, which may include the need to replace the equipment or the loss of valuable personal data. Mobile malware attacks often result in direct financial damage to individuals and organisations, which is one of the most typical impacts of these attacks. One example is the theft of financial information that leads to fraudulent acts. Other examples include unauthorised transactions, payments of ransom to unlock encrypted data, and ransom payments. For example, banking Trojans are designed to steal login credentials and manipulate transactions from financial apps.

Companies, especially small and medium-sized enterprises, may experience disruptions in operations, lose confidential information and have significant financial costs associated with breach remediation and reputational damage. An organization's reputation can be seriously damaged by a mobile malware attack for several reasons. In the event that consumers' financial and personal information is compromised as a consequence of weak security measures, it is possible that individuals will develop a decreased level of trust in the organisation. Additionally, the negative publicity that the incident generates may cause the company's customer base and income to decrease for an extended length of time following the incident. The enormous financial impact that cybercrime has on the global economy is reflected in the fact that it is estimated that the global cost of cybercrime, which includes mobile malware, will reach trillions of dollars yearly. According to estimates, the worldwide cost of cybercrime was predicted to be more than eight trillion dollars in the year 2022 (Hernandez, 2023).

## 3.3 Effects on Society and Politics

Malware found on mobile devices has an enormous impact on both society and politics. Malware on mobile devices has a significant impact on public confidence in digital technology and may limit the use of essential mobile services such as online banking and e-commerce. This is because society is becoming increasingly dependent on digital platforms for essential services such as healthcare, communication, and financial transactions.

For example, over 50,000 devices were infected with the Pegasus spyware, which was developed by the Israeli cybersecurity company NSO Group. This spyware became a powerful tool for political manipulation and suppression of opposition between the years 2016 and 2020. Its primary purpose was to enable remote surveillance of iOS and Android smartphones, and it was meant to target those devices (Shankland, 2022). It is possible for Pegasus, which is considered to be one of the most intrusive forms of spyware, to transform a mobile device into a tool that is capable of continuous surveillance without the user ever being aware of its presence and it was meant for Pegasus to spread without experiencing any contact from the target. Known as a "zero-click attack," this kind of attack aims to infect a device by sending a message to the intended recipient's phone and then taking advantage of vulnerabilities in the recipient's software.

The use of Pegasus spyware has been the subject of a substantial amount of discussion, notably with regard to its use against journalists, activists, political figures, and human rights workers all over the world. Through the surveillance of communications and the distribution of false information, these incidents bring to light the potential for malware to gain influence over political processes, manipulate public opinion, and damage democratic processes overall. Monitoring, intimidating, or suppressing political personalities, journalists, and activists has also been accomplished through the use of mobile malware landscape by state-sponsored actors and malicious organisations.

In an effort to fight against cybercrime and safeguard the personal information of users, governments and international organisations are responding by establishing more stricter laws and regulations surrounding data protection and cybersecurity. Additionally, these measures raise concerns regarding data privacy and the overreach of the government, despite the fact that their primary objective is to minimise the occurrence and impact of mobile malware. A higher emphasis has

been placed on regulatory and legal measures as a result of the impact that mobile malware has had on society. At times, these restrictions might have a negative effect on individual users as well as the user experience.

# 4 The Emergence of Smartphones (2004-2010)

## 4.1 Adoption of Smartphones

The emergence and widespread use of smartphones prompted a significant shift in the telecommunications industry between 2000 and 2010. Throughout this time, mobile phones evolved from being basic devices used mostly for texting and making phone calls to more advanced tools with a variety of features like email, multimedia access, internet browsing, and the ability to use a constantly growing library of different applications. Complicated programs might now run more smoothly on mobile devices because to the development of 3G internet networks and mobile technology advancements. Around this time, smartphones began to grow into an essential part of daily life for millions of people worldwide.

The way individuals communicate with technology were drastically changed by the development of smartphones, which made it possible for consumers to access information and digital services while on the go. A variety of well-known smartphones were released during this period, most notably the Apple iPhone in 2007 and the BlackBerry and Nokia N series. Because of its large app store, sleek design, and touchscreen interface, the iPhone significantly changed consumer expectations and the global market. It exceeded expectations for what could be achieved with a mobile device, encouraging competitors, and driving growth and creativity in the mobile industry.

The impact of smartphones expanded outside of individual users, having effect also on various sectors of the economy and society. Businesses had to adapt to a world where consumers were constantly connected, which led to the development of mobile friendly e-commerce websites and strategies for mobile marketing. Social interactions also evolved, with instant messaging apps and social media platforms becoming central hubs to what and how people used to communicate.

Additionally, because smartphones are so widely used, it is now simpler to collect and analyse vast amounts of data, which has led to advancements in fields like big data analytics and the Internet of Things. This era also brought attention to the significance of digital literacy and raised new concerns about the digital divide because different socioeconomic groups did not have equal access to this cutting-edge technology.

## 4.2 Operating Systems and Security Features

During the same time as smartphones were being introduced, specialized mobile operating systems were developed in order to provide support for the more advanced features of these new devices. The evolution of smartphones between the years 2000 and 2010 is directly tied to the development of these operating systems, which turned out to be the foundation for the operation of mobile devices by offering a platform for applications, multimedia content, and networking possibilities. The launch of early mobile operating systems, such as Symbian, BlackBerry OS, Palm OS, and Windows Mobile, as well as later operating systems, such as iOS and Android, had a significant impact on the user experience of smartphones.

When compared to their predecessors, these operating systems were significantly different since they offered an open platform that enabled the development of applications by third parties. As a result, the capabilities of smartphones were significantly expanded. Devices are now capable of doing far more than simply sending and receiving text messages and making phone calls, thanks to the introduction of 3G networks and other improvements in mobile technology. They may now be utilized for a wide range of applications, including but not limited to email, access to multimedia content, internet browsing, and many others.

With the release of Android, by Google in 2008 and iOS by Apple in 2007, smartphones saw a major change because of simplified user interfaces, centralized app stores, and improved connection features. The introduction of these platforms resulted in a revolution in mobile computing, leading to innovation across all sectors and having impact on competitors. In particular, the centralized app stores provided a validated collection of applications, which resulted in a decrease in the number of applications that were infected with malware. This marked an innovative approach to the distribution of applications and the protection of users.

The security controls that were included in these early mobile operating systems were quite basic in functionality. The primary focus of these security features was to prevent unauthorized access to the device by utilizing patterns and personal identification numbers (PINs). However, as the capabilities of smartphones improved, the security challenges that they presented also increased. Public key signatures on apps, cryptographic algorithms, and a variety of protocols such as HTTPS and WTLS were among the early security features. As the threat landscape evolved and became

even more complex, the developers of operating systems started to implement security mechanisms that were progressively more complex. Examples of these include encryptions that secure user data, remote wipe capabilities that enable users to delete data from devices that have been lost or stolen, and app permissions that allow users to manage access to data and system functionalities. The recent malware attacks on mobile devices have made it quite obvious that there is an increasing demand for strong security measures that can protect the privacy of users and maintain the integrity of the device (Snyder, 2019).

## 4.3 First Instances of Mobile Malware

In 2004, the Cabir worm, which was believed to be the first instance of mobile malware, was discovered. This event marked a significant turning point in the history of mobile malware. Cabir was a mobile phone virus that infected Symbian devices and demonstrated how vulnerable mobile devices were to malware infections, despite the fact that its effects were relatively minor. Cabir was merely the beginning of newly discovered threat landscape that is continually expanding. This early version of the mobile virus spread through Bluetooth connections, infecting devices to display the message "Caribe" on the screen. This act demonstrated the potential for mobile devices to be abused.

Following Cabir, the mobile malware landscape began to expand, with more harmful apps being developed. CommWarrior, discovered in 2005, also targeted devices running on Symbian OS and spread through MMS messages in addition to Bluetooth, representing a more malicious threat by sending messages without user consent and causing expenses. Mobile service providers have claimed that CommWarrior was responsible for as much as 3.5% of their mobile traffic, and they have ultimately agreed to pay those who have been affected by the attack (Apvrille, 2014).

These occurrences made clear how essential it is to improve security procedures and educate users and developers about the possible risks connected to mobile devices. The development of mobile malware such as Cabir and its successors demonstrated the crucial requirement of establishing strong security mechanisms to protect against attacks of this type. This period also triggered a response from the cybersecurity sector and mobile OS developers, leading to the creation of security software focusing on antivirus protection, firewalls, and the deployment of app permissions and sandboxing (Snyder, 2019).

## 4.4 Statistics and Key Events from 2004 to 2010

Initially, the number of reported malware variants was relatively low, primarily due to the limited functionality of early mobile devices and the early stages of mobile internet connectivity. The latter half of the decade, on the other hand, witnessed an obvious rise in the number of malicious software types that targeted mobile devices. This was a direct result of the development of smartphone technology, the increasing number of mobile applications and increasing user base.

Kaspersky Lab had identified 106 families and 514 types of harmful programmes aimed at mobile devices by mid-August 2009. These figures have increased to 153 families and more than 1,000 varieties by the end of 2010. In other words, compared to 2009, 65.12% more new harmful programmes aimed at mobile devices were discovered in 2010. In just 17 months, their quantity had nearly doubled (Maslennikov, Mobile Malware Evolution: An Overview, Part 4, 2011). See Figure 1 that shows the mobile malware families and variants that were discovered by the end of 2010.

| Platform | Number of Families | Number of Variants |
|---|---|---|
| J2ME | 45 | 613 |
| Symbian | 74 | 311 |
| Python | 5 | 60 |
| Windows Mobile | 16 | 54 |
| AndroidOS | 7 | 15 |
| Sgold | 3 | 4 |
| MSIL | 2 | 4 |
| IphoneOS | 1 | 2 |

Figure 1. Mobile Malware Families and Variants (Maslennikov, Mobile Malware Evolution: An Overview, Part 4, 2011)

Figure 2 illustrates the detection of new varieties of mobile malware that were discovered during the years 2004 and 2010. According to the chart, there were only about 400 different mobile virus versions that were discovered between the years 2004 and 2009, however, following that, the number of detected new variants significantly rose. During the period from 2009 and the end of

2010, there was a growth of 175%. The increase in numbers can be explained by multiple different factors. Among these contributors are the following:

1. **Growing user base:** The late 2000s saw a significant increase in the use of smartphones as a result of the introduction of new smartphone models that were more reasonably priced by Samsung and Apple.

2. **Mobile network:** Improvement in network speeds and network access, this progress not only improved the use of mobile devices, but it also provided new opportunities for cybercriminals to exploit, such as phishing and network-based attacks.

3. **App Stores:** The late 2000s saw the launch and quick growth of mobile application marketplaces like the Apple App Store and Google Play. While these platforms greatly expanded the smartphone ecosystem with a different set of applications, they also served as a distribution route for malicious software.

4. **Introduction of Banking Trojans:** The first mobile banking Trojan was developed. This caused an increase in the amount of banking trojans as criminals attempted to capitalise on mobile malware.

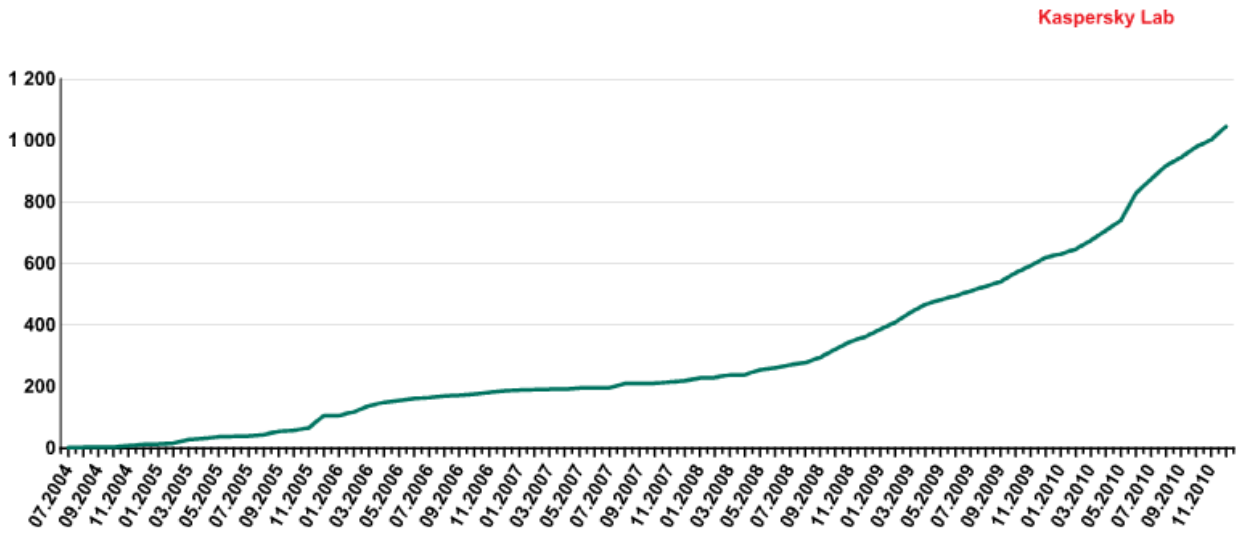


Figure 2. The increase in the number of known variants between 2004 and 2010 (Maslennikov, Mobile Malware Evolution: An Overview, Part 4, 2011)

Some of the key events from 2011 to 2015 include the following:

**Cabir Worm (2004):** The early 2000s saw the emergence of mobile malware, starting with the discovery of the Cabir worm in 2004. Cabir was the first recorded case of a virus that could infect mobile phones, with the virus primarily focusing on Symbian powered smartphones. Due of its lack of

effectiveness, experts and researchers believe that the worm was created by the hacking organization 29A as evidence or an experiment showing that mobile malware truly exists.

Cabir was distributed via wireless Bluetooth technology. It first scanned for nearby Bluetooth devices in discoverable mode before attempting to transfer itself as a SIS file (Symbian Installation Source). Without an internet connection, the worm spread to other devices via the Bluetooth link, If the user approved and opened the file once it was sent, the worm would automatically install itself on the device. Cabir had no particular malicious intent, but its primary goal was to propagate to other devices and show the word "Caribe" on the screen of the infected device. Although Cabir only drained the energy and might have caused some discomfort to affected devices, it is deemed important since it demonstrated that mobile malware is possible. It increased the public's and cybersecurity experts' awareness of mobile device vulnerabilities and the potential for more dangerous threats. The discovery of Cabir motivated researchers to work even harder on developing mobile security solutions, such mobile antivirus software. It also made manufacturers of smartphones and software developers pay greater attention to security, which enhanced Bluetooth security and the security architecture of mobile operating systems overall (Apvrille, 2014).

**CommWarrior (2005):** The number of mobile malware variations increased dramatically after discovery of Cabir. A new mobile worm variant called CommWarrior was identified in 2005, and it specifically targeted Symbian powered smartphones, namely those running the Series 60 platform. Compared to its predecessor, the Cabir worm, which was mostly spread over Bluetooth, Commwarrior was more aggressive due to its ability to spread via both Bluetooth and MMS (Multimedia Messaging Service). Because it used the mobile network for transmission, this technique made it possible for Commwarrior to spread outside of the infected device's, possibly even over national borders. Worldwide, more than 18 countries had reported cases of the virus. Over 115 000 mobile devices were infected and over 450 000 MMS were transmitted without the victims' knowledge (Apvrille, 2014).

Upon infection, Commwarrior would install itself on the device and set up to automatically start on device reboot, ensuring its continued existence. Following that, it would continuously scan for new devices to infect via Bluetooth and MMS, sending out messages with varying language to trick users into clicking on the harmful file. Because of the two distribution methods, Commwarrior may

charge the device owner for MMS messages sent and can rapidly drain the battery of the infected device by continuously monitoring Bluetooth devices. Furthermore, the device's stability and performance may suffer as a result of its existence.

**RedBrowser (2006):** Unlike its predecessors, which focused on the Symbian OS, RedBrowser was among the first known malware threats directed at devices running the Java 2 Micro Edition (J2ME) platform. This implied that it could infect not only smartphones but also a wide range of mobile phones that supported Java applications.

RedBrowser was usually installed from websites by pretended to be genuine applications. It pretended to be an application that offered to provide free WAP (Wireless Application Protocol) services to consumers by using free SMS messages. Once downloaded and installed, it would perform malicious acts without the user's knowledge or consent. RedBrowser's primary malicious behavior involved sending unwanted SMS messages to premium-rate numbers, resulting in significant charges to the user's mobile phone account. This is exactly how the malware was designed to function in the background, occasionally evading consumers' attention until they started noticing unexpected expenses (Apvrille, 2014).

Platform security mechanisms have improved as a result of the threat posed by malware such as RedBrowser. These improvements include tighter application validation procedures and the implementation of permissions systems, which limit the operations that apps may execute on a device.

**InfoJack (2008):** First identified in 2008, Infojack was a trojan that infected Windows Mobile devices. It would take advantage of vulnerabilities in the operating system to discreetly install itself without the user's permission. Notably, it disabled security software and prevented security upgrades from being installed on compromised devices, exposing the way for more harmful activities. Due to the backdoor's ability to grant unauthorized remote access, sensitive data and personal information could be stolen, increasing the device's vulnerability to further malware challenges. InfoJack was able to spread to many devices via memory cards or shared network connections thanks to corrupted software (Gostev, 2008).

Updates for the Windows Mobile operating system improved mobile antivirus software, and increased user awareness of the importance of downloading software only from trustworthy sources are just a few of the actions that have been taken in the field of mobile security since InfoJack's formation. The InfoJack malware highlighted the importance of having strong mobile security protocols and exercising caution while controlling software installations on mobile devices.

**Ikee (2009):** The "Rickrolling worm," also called the Ikee virus, first surfaced in November 2009, and was designed to target iPhones that had been jailbroken. This worm exploited devices that had SSH (Secure Shell) installed with the default password unchanged, a common scenario among jailbroken iPhones used to install unauthorized apps. Upon infection, the Ikee virus would replace the device's original wallpaper with an image of pop musician Rick Astley, well known for the hit song "Never Gonna Give You Up" thus the term "Rickrolling." Beyond this practical joke, the virus looked for other weak points in the network to spread itself. Being among the first malware to target iPhones specifically, the Ikee virus gained attention for drawing attention to the security issues connected with jailbreaking devices and using default passwords (Neil Bergman, 2013)

**Zitmo (2010):** The Zitmo virus, short for "Zeus in the Mobile", is a mobile malware that emerged around 2010 as a counterpart to the notorious Zeus (or Zbot) malware that targeted online banking systems on personal computers  The purpose of Zitmo is to compromise mobile devices, namely those with Symbian and Android operating systems, in order to get beyond the two-factor authentication procedures that many online banking services need (Kaspersky, 2011).

After a device was compromised, attackers were able to get around 2FA and access victims' online banking accounts without authorization thanks to Zitmo's ability to capture bank-sent SMS messages that contained one-time passwords or mobile transaction authentication numbers. Malicious software downloads or phishing operations were the usual methods used to spread the malware, tricking victims into installing it under the pretense of a security update or a genuine banking program.

Based on the Key events and statistics, it is possible to conclude that between 2004 and 2010, the majority of known mobile malware variants were not intended to cause much actual harm to infected devices other than slight inconvenience and very minor financial loss. it was only after the introduction of mobile banking services, did attackers become more interested in the financial gain of malware development, leading to the development of more sophisticated banking trojans. The introduction of the first banking trojan, Zitmo, started the era of banking trojans.

While it's difficult to identify the exact number of mobile malware variants affecting mobile devices between 2000 and 2010, this period marked the beginning of a significant increase in mobile security threats. Because of the growing number of malicious software for mobile devices, there is an immediate need for improved security controls and increased knowledge among both users and developers. The growing number of mobile malware variants on mobile devices highlighted the fact that defending mobile devices in a world that is becoming more interconnected is becoming an increasingly difficult task.

# 5 The Verge of Smartphones (2011-2015)

## 5.1 Rapid Growth of Smartphone Users and Platforms

A significant shift took place in the smartphone industry over the years 2011 to 2015, which came with a significant rise in the number of customers adopting smartphones all over the world. During this time period, there was also a shift in the way in which people used technology to connect with one another, access information, and manage their day-to-day lives. The widespread availability of smartphones and the democratization of access to the digital world resulted from the fact that they shifted from being a luxury item to a necessity for millions of people. Figure 3 illustrates the growth of smartphone ownership in the United States of America between the years 2011 and 2022.

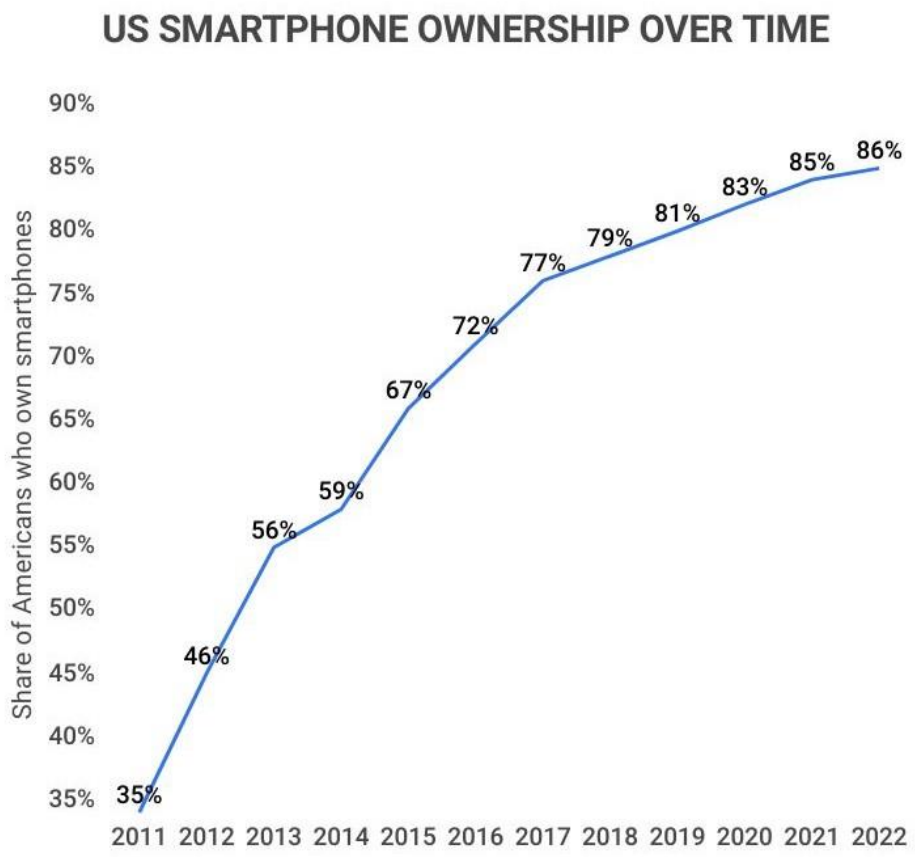


Figure 3. Smartphone ownership over time in USA (Kolmar, 2023).

There were a number of significant factors that contributed to the rapid rise smartphone adoption among users. To begin, the launch of lower priced models made it possible for a greater number

of people to own a smartphone. As low-cost, high-quality alternatives for Apple and Samsung's flagship phones, manufacturers from China and other Asian regions joined the market, bringing smartphones to emerging markets.

Secondly, this increase was greatly facilitated by the rapid expansion of mobile networks. Globally, the introduction of 3G and the start of 4G LTE networks brought higher internet speeds and more reliable connectivity. The user experience was enhanced as a result of these advancements in mobile connectivity, which made it possible for applications that are becoming increasingly complex and bandwidth-intensive, such as social media platforms, online gaming, and streaming services, to become more significant in people's day-to-day lives (Galazzo, 2020).

In addition, the ecosystem surrounding smartphones prospered, the creation of mobile apps grew rapidly, and millions of apps were available for download on the Apple App Store and Google Play Store. Apps became the primary selling point of smartphones, accelerating adoption, and being used for anything from health monitoring and education to mobile banking. The rapid growth had a significant impact on the situation. As a result of the increasing number of people who rely on their smartphones for day-to-day activities such as buying, consuming content, and navigating. It was around this time that the culture of being "always connected" began to gain traction, with social media and quick access to information becoming more and more common.

## 5.2 Emergence of Android and iOS

Android and iOS were the two primary manufacturers that dominated the market during this period. Android, which was developed by Google, quickly became the most frequently used smartphone operating system due to the fact that it is open-source and flexible, which allowed it to be adopted by a wide range of manufacturers. On the other hand, Apple's iOS, which is characterized by its closed environment, has maintained a considerable market share. This is because it is appealing to customers who are looking for premium products that prioritize privacy and security. The competition between these platforms sparked innovation and resulted in significant improvements in device capabilities, app development, and user experience.

Android's open-source architecture made it possible for a wide range of manufacturers to have access to a customizable platform, which is what enabled its quick adoption and widespread distribution. As a result of Android's open-source nature, it is now accessible to a larger variety of consumers, with options ranging from high-end mobile devices to solutions that are more reasonably priced. The method that Google took resulted in the creation of a competitive market, which allowed manufacturers to improve their devices by adding features and customizations that separated them from those of their competitors while still allowing them to take advantage of the core Android experience. The Android operating system had several significant modifications over this time period, each of which introduced significant new security features and enhanced the overall user experience (digicontentexperts, 2023).

On the other hand, Apple's iOS managed to maintain its position by offering a high-end ecosystem that was managed and distinguished by the seamless integration of hardware and software. Apple's strategy ensured that its user base had a consistent and optimized experience across all of its products, which in turn increased brand loyalty among Apple's user base (Meyer, 2010). The introduction of Siri in 2011 along with the release of the iPhone 4S marked a significant step forward in the capabilities of smartphones and laid the foundation for the development of voice-activated assistants in the years to come.

The competition between Android and iOS was not limited to the operating platforms, rather, it included the market for mobile applications as well. Both the Google Play Store and the Apple App Store have established themselves as increasingly important parts of the mobile experience. They serve as entry points for users to access a wide variety of features and services. During this period, there was a rise in the production of mobile applications, as developers were eager to capitalize on the rapidly growing market. The willingness of Apple's user base to pay for apps and in-app purchases helped to maintain the App Store's reputation as a more profitable platform. Google Play, on the other hand, was appealing to developers who were looking for scalability and reach because it offered a larger audience. This was due to the majority of Android's market share.

The rise to prominence of iOS and Android has had a significant influence on mobile technology and user experience. Their rivalry sped up technological development, resulting in breakthroughs in touchscreens, mobile processors, and camera technologies, which raised customer expectations

for smartphones. Furthermore, at this time, both platforms introduced features and services that used user data to deliver customized content, recommendations, and functionality, bringing in a more personalized user experience.

## 5.3 The App Store Threats and Evolution of Malware Tactics

Both the ecosystem of smartphones and the threats that targeted mobile users saw significant changes between the years 2011 and 2015. The emergence of App Stores as primary locations for software distribution provided an opportunity for malicious actors to take advantage of. Criminals were looking for innovative methods to circumvent the increasingly strict safety measures that were being implemented by the iOS and Android platforms during this time period, which resulted in a significant shift in the development of malware techniques.

One of the most concerning events was the spread of malicious software through the official App Stores themselves. By taking advantage of vulnerabilities or disguising their true nature, attackers were able to distribute programs that contained malware despite the strict requirements that were in place for software evaluation. These programs frequently appeared to be real programs, drawing users in with tempting features to trick people into downloading them. This was done to deceive users into downloading them. Once they were installed, they were capable of carrying out a wide range of harmful operations, including the theft of personal information and credentials as well as turning the devices into botnets (Neil Bergman, 2013). Additionally, during this period, there was an increase in the misuse of premium services. This was due to the fact that malicious software would covertly sign users up for expensive services, which would result in substantial costs. During this period, designers of viruses developed techniques that were progressively more complex. One of the most prevalent methods was repackaging trustworthy applications with malicious code and then distributing these trojanized versions through phishing websites or third-party app stores. Using well-known programs as a trojan horse, this technique spread malicious software and made a profit off the popularity of the programs.

Another significant development was the rise of ransomware on mobile devices. In an approach that is similar to the common methods that are used against personal computers, mobile ransomware would potentially lock users out of their devices or encrypt their data, and then demand ransom payment in order to unlock them. This type of attack highlighted the personal value of the

data stored on smartphones, leveraging it as a means of extortion. A further development that occurred during this time period was the proliferation of spyware applications that were meant to covertly monitor the actions of users, collect sensitive data, and even track their physical position. These apps often targeted individuals or were used in targeted attacks against specific groups or organizations.

The rise of app store threats and the evolution of malware tactics prompted a response from both the technology industry and regulatory organizations. For the purpose of identifying and preventing malicious applications, app stores have upgraded their review processes and included automated procedures. There was a significant contribution made by security companies and researchers in the process of finding and reporting hazards which resulted in the removal of harmful applications more quickly.

Additionally, during this time period, mobile antivirus and security applications that were designed to protect users from mobile malware, phishing, and other forms of attacks were on the market and started to gain more popularity. The fact that these advancements offered capabilities such as app screening, browser protection, and anti-theft measures made them essential parts of mobile security. It was during this time period that malware strategies underwent a significant evolution, which highlighted the continued competition between hackers and security professionals. For the purpose of combating the dynamic threat landscape, it highlighted the importance of maintaining a state of constant alertness, enhancing security policies, and educating users.

## 5.4 Statistics and Key Events from 2011 to 2015

The increase in the number of new unique variants of mobile malware during this period is a clear indication of the growing interest of cybercriminals in taking advantage of the expanding user base of smartphones. The use of social engineering to distribute smartphone viruses has grown in popularity. Phishing emails, SMS, and even fake app updates were used by malicious actors to deceive users into installing malware, taking advantage of the users' trust. A rise in the distribution of malicious applications through official app stores was another trend that occurred during this period. Even while app stores, and the Apple App Store in particular, undergo strict app review procedures, there are examples in which malicious software was able to circumvent the review process. This highlights the necessity of implementing stricter security processes and standards for app

evaluation. Similar issues affected Google Play, as many malicious apps took advantage of the less strict screening procedures to gain access to consumers. On multiple occasions throughout this period, the significance of user awareness and education in the prevention of mobile risks was highlighted.

According to the findings of a research that was carried out by McAfee, the total number of mobile malware samples increased from over 2 million in 2013 to over 12 million by the end of 2015. Over the course of just 3 years, there has been a growth of about 500 percent (McAFEE, 2013, 2016). Banking trojans intended for financial gain formed a significant portion of these attacks, with Android devices being the most commonly targeted. The figure 4 shows the exponential growth of identified malware samples between 2011 and 2015.

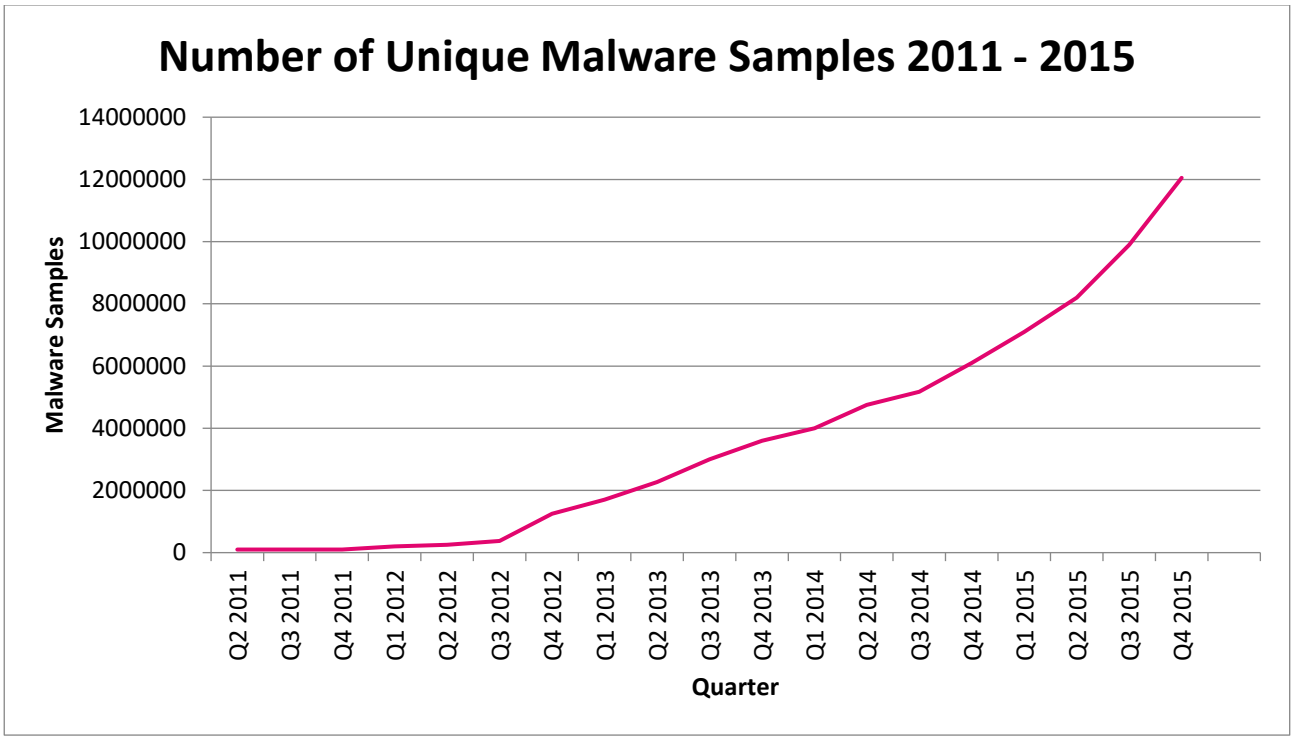


Figure 4. Number of Unique Malware Samples 2011- 2015 (McAFEE, 2013, 2016).

The Figure 4 demonstrates how the number of unique mobile malware samples began to rise rapidly in 2012–2013. From Q1 2013 to Q1 2014 we can see nearly a 100 percent increase in just one year alone. This growth can be tracked to several different factors:

1. **Growing user base:** The figure 3 illustrates how, between 2012 and 2014, the percentage of persons using smartphones increased by almost 22%. By 2015, billions of people worldwide were using smartphones, providing a vast landscape for attackers to exploit.

2. **Mobile OS updates and technology advancements:** During the years of 2011-2015 smartphones manufacturers were on a steady competition. Revolutionizing the markets continuously and further accelerating technological breakthroughs due to consumer demand. Mobile operating systems were demanded to add new features with every update, which enhanced functionality but also brought forward new attack vectors and weaknesses that hackers quickly took advantage of.

3. **Financial Motivation:** The rise in mobile financial and banking activities made mobile devices an appealing target for cybercriminals. Financially driven malware, especially Trojans, could directly lead to financial gain by stealing user's credit card details, banking credentials, or carrying out fraudulent transactions.

4. **Application stores:** Because it was so simple to submit apps to both official and unofficial app stores, criminals were able to spread malicious programmes far and wide. Even with the screening procedures in place, skilled attackers managed to get past the security checks in the app store.

5. **Increased Connectivity:** The growth of internet access on mobile devices and the use of cloud services increased the potential for malware spread and data theft. The fact that devices were nearly always online expanded the attack surface.

6. **Lack of User Awareness:** Figure 3 illustrates the growing number of people owning a smartphone during 2012-2014, the lack of user awareness with smartphone devices could also explain the growing number of unique malware variants. Antivirus software developer McAfee discovered in a 2012 study that 19.32 percent of users either had their antivirus software turned off or not installed at all (Speed).

According to a study conducted by Kaspersky Lab in 2013, 98.1% of all mobile malware discovered in 2013 targeted Android devices. This could be explained by the fact that Android is an open-source operating system, in opposition to iOS, which operates within a closed ecosystem. Android phones also account for a significant percentage of the worldwide smartphone market, which could have an impact on these figures. According to the findings of the study, the vast majority of mobile malware that was detected in 2013 was designed to obtain financial information from users. In the year 2013, the amount of discovered mobile malware variants designed for phishing, stealing bank card information, and withdrawing money from bank accounts has increased by 20% (Lab, 2014).

Some of the key events from 2011 to 2015 include the following:

**DroidDream (2011):** The DroidDream Malware, which first appeared in 2011, was one of the very first widespread attacks on Android smartphones to have an effect on the Google Play Store. After installing DroidDream, which was hidden among authentic apps on the Google Play Store, compromised smartphones and gaining access to sensitive information and allowing the installation of additional malicious components. DroidDream gained root access to the smartphone by taking advantage of vulnerabilities that were already known to exist inside the Android operating system. With root access, DroidDream could retrieve sensitive user information from the device, including device IDs, location information, and potentially other personal information stored on the device.

The discovery of DroidDream resulted in the detection of more than 50 infected applications in the Google Play Store, with estimates ranging from 50,000 to 200,000 users affected before the apps were deleted (Brewster, 2011). Google replied by not only removing infected apps from the store, but also remotely removing them from customers' devices using an Android Market security feature.

**Find and Call (2012):** Find and Call was the first reported piece of malware to make through Apple's strict app approval process and make it onto the Apple Store. It appeared to be a utility software, but really gathered contact information from users' address books and upload these contacts to a remote server. It would then send spam SMS messages with links to download the malware.

Both Apple and Google quickly responded by removing the "Find and Call" app from their own app stores once the malicious purpose of the app was uncovered. Furthermore, this event caused a review of app submission and review processes, with both firms aiming to strengthen restrictions and improve detection of similar malicious apps in the future.

**FakeToken and Svpeng (2013):** Bank customers in Russia were the initial target of these banking trojans, however, they demonstrated a growing trend of mobile malware targeting mobile banking services. In both cases, malicious software was designed to infect Android smartphones with a particular functionality that was designed to steal financial information from vulnerable users. FakeToken could intercept SMS messages used for two-factor authentication, while Svpeng locked phones and demanded ransom, indicating the early usage of ransomware tactics on mobile.

**WireLurker and Masque Attack (2014):** New attack vector had been invented by WireLurker, which targeted both Mac and iOS devices. It achieved this by infecting iOS devices with malicious software that was installed on Macs. Initially, it gained popularity for its capacity to infect iOS devices that had not been jailbroken by installing third-party applications from infected Macs through the use of USB.

The Masque attack was a security vulnerability in iOS that allowed malicious programmes to masquerade as legitimate applications when they were downloaded from websites other than the App Store. It had the potential to replace real apps on an iOS device with malicious duplicates without the user's knowledge, resulting in data theft and unauthorised access.

**XcodeGhost (2015):** A hacked version of Apple's Xcode integrated development environment (IDE), which is Apple's official tool for developing applications for macOS, iOS, watchOS, and tvOS, was leveraged to create several iOS applications that contained malicious code. It compromised the app development tool rather than directly targeting the devices or applications that were being targeted. Using this method, malicious software could be installed in legitimate applications without the developers of the programme being aware of it. It was possible for users' smartphones to get compromised when they downloaded and installed the malicious applications. It was possible for this malicious software to obtain passwords and other sensitive information and send it to remote servers. The XcodeGhost incident was significant because of the size of the infection and its emergence in the App Store, which is recognised as a secure location for downloading programmes. Hundreds of legitimate apps were infected, including some popular ones, potentially harming millions of users.

Based on the key events and statistics, it is possible to conclude that between 2011 and 2015, the trends in new mobile malware creation were directed towards mobile banking services and application marketplaces. For the first time, attackers attempted to profit financially from mobile malware development by targeting users' banking information or encrypting their data and demanding ransomware money in exchange for releasing it. Android and iOS competition became extremely beneficial to attackers, as these two technological giants attempted to launch new software and services with little regard for security, revealing new attack vectors daily.

# 6 Advancements in Mobile Technology (2016-2020)

## 6.1 Transition to 4G and Early 5G Networks

There was a significant advancement in mobile communication technology that occurred between the years 2016 and 2020, and it was the transition from 3G networks to 4G LTE networks. Because it did more than just provide improved internet connections, this transition led to an increase in the amount of data that was consumed as well as the amount of traffic that was on mobile internet. Also, it brought about a fundamental change in the way that customers utilised their mobile devices. Mobile users are now able to take advantage of real-time gaming, high-definition video streaming, and the expansion of social networking platforms thanks to the arrival of 4G LTE.

Additionally, the introduction and rollout of 5G networks, which started towards the end of this decade, promised to further revolutionise mobile communication with its groundbreaking capabilities. Early deployments of 5G demonstrated the technology's capacity to achieve download speeds that are up to one hundred times faster than those of 4G and with significantly lower latency. This opened the door to much wider support for developing technologies such as virtual reality (VR), augmented reality (AR), and the Internet of Things. Additionally, it was anticipated that 5G will accelerate advancements in areas such as telemedicine, driverless vehicles, and smart cities, in addition to improving consumer applications.

The transition also made it clear how important it is to have reliable mobile security options. As network speeds and capacities increased, the attack surface for potential cyber threats also increased. As a result of the increased speed with which more data might be transferred, potentially hazardous behaviour could take place that is both more rapid and more widespread than ever before. The cyberattacks that were directed at mobile networks got increasingly sophisticated during this period. Some of these cyberattacks attempted to exploit the vulnerabilities of 4G networks and, later, the infrastructure that was being developed for 5G networks. Because of the difficulty that network operators and security specialists are experiencing in developing new standards and technologies to protect themselves against these constantly evolving threats, the 5G architecture has been updated to include encryption algorithms and security measures that are more advanced than those that were previously implemented (Castle, 2019).

## 6.2 Development of More Advanced Smartphones

During this time period, there was a rapid advancement in smartphone technology, which resulted in a generation of new benchmarks for usability, performance, and efficiency. The mobile market was fundamentally transformed as a result of the significant developments in smartphone technology that occurred during this era. These advancements included significant improvements in processing power, display technology, camera systems, and battery life.

Smartphone manufacturers made leaps in processing capabilities, with multicore processors becoming standard. These new processors were not only quicker but also more energy efficient, which meant that they made it possible for users to perform advanced computational operations and multitasking in a more seamless manner without having to physically move their hands. Computing units (CPUs) from Qualcomm's Snapdragon and Apple's A-series were at the forefront of these advancements. These CPUs integrated artificial intelligence (AI) directly into the chipset, which improved a wide range of capabilities, including real-time language translation and photography. Memory (RAM) and the capacity of the internal storage both increased significantly at the same time. In order to satisfy the ever-increasing demand for powerful gaming, augmented reality (AR), and massive amounts of multimedia storage, top-tier devices will have up to 16 gigabytes of random-access memory (RAM) and one terabyte of storage space by the end of the year 2020.

OLED and AMOLED screens were common in high-end smartphones during this time, marking a substantial advancement in the field. In contrast to their LCD counterparts, these displays had better contrast ratios, colours that were more vibrant, and a more efficient use of battery power. The designers of smartphones have pushed the boundaries of smartphone design by introducing edge-to-edge and foldable screens. These innovations have provided customers with new form factors and increased screen real estate. The advent of higher refresh rates, up to 120Hz, resulted in an improvement in the visual experiences of users. This facilitated a more fluid scrolling experience and enhanced gaming. As a result of manufacturers adding several cameras sets into their smartphones, a revolution in smartphone photography took place. This meant that the quality of both still images and movies was significantly improved. Mobile smartphones would never have been able to attain such vast photography capabilities without the wide-angle, telephoto, and macro lenses that are included in these multi-camera systems. Using computational photography that is powered by artificial intelligence, image processing has been dramatically improved, which

has led to the introduction of features like as super-resolution zoom, night mode, and portrait mode with sophisticated bokeh effects. As a result of these improvements, photography of a professional standard became more readily available to the general population.

In order to meet the rising energy demands of smartphones, battery technology also progressed as smartphones gained processing power. The amount of time required to recharge mobile devices has been significantly reduced as a result of the introduction of technological advancements such as larger batteries and rapid charging technologies by manufacturers. The smartphone's central role in the digital ecosystem of the user was brought into sharper focus by the increasing popularity of wireless charging as well as the invention of reverse wireless charging, which enabled smartphones to charge other electronic devices such as smartwatches and earbuds.

The advancements in smartphone technology have led to an increase in the usage of mobile devices in both daily life and the business, while simultaneously resulting in a considerable improvement in the user experience. By laying the way for future developments, smartphones have evolved into indispensable instruments that can be used for a variety of purposes, including productivity, creativity, communication, and entertainment.

## 6.3 Increase in the Variety of Malwares

In addition to advancements in mobile technology, there was a corresponding increase in the complexity and diversity of mobile malware throughout the years 2016–2020. Considering the fact that smartphones were becoming increasingly integrated into both personal and business sectors, cybercriminals found them to be increasingly appealing targets.

Ransomware attacks on mobile devices became more sophisticated, with attackers targeting both individual users and businesses. The data of the user would be encrypted by these malicious programs, making it unreadable, and they would demand a ransom in cryptocurrency in order to decrypt it. Malware developers started using approaches that were more adaptive and polymorphic, which meant that they were responsible for building malware that could alter its code or behavior

in order to avoid being discovered by traditional antivirus software. Due to the adaptability of security software, it became increasingly difficult to identify and eliminate threats. As a result, the industry began to embrace detection methods that were more dynamic, and behavior based.

As a result of the widespread adoption of mobile banking applications, more sophisticated varieties of banking Trojans have emerged. Malwares like these were developed with the purpose of gaining unauthorised access to mobile devices via smartphones and stealing financial information. They frequently purported to be reliable banking applications in order to trick victims into entering their login information, which was then transmitted to the attackers. The increasing use of mobile payment systems has made it easier for these Banking Trojans to be exploited in a greater number of ways, highlighting the importance of implementing stronger security protocols in financial applications (Malware, 2021).

During this period, there was also a significant rise in the presence of spyware and stalkerware apps. These malicious programmes were developed with the intention of secretly monitoring the activities of the user, which may include tracking their whereabouts, recording their phone calls, and logging their keystrokes. Specifically, stalkerware became a tool for domestic violence, enabling people to follow their partners in secret. The widespread use of these intrusive applications brought attention to the negative aspects of mobile technology's accessibility and the significance of privacy safeguards in mobile operating systems (Glazova, 2021).

As a result of the expansion of the Internet of Things, malicious software started to target not only mobile phones but also other connected devices, such as smartwatches, fitness trackers, and home automation systems along with smartphones. Attacks like these usually targeted vulnerabilities that had not been patched and security standards that were insufficient. As a result, these devices were enlisted in botnets for coordinated attacks such as Distributed Denial of Service (DDoS) attacks or used as entry points for wider network invasions.

Another concerning trend was the increase in supply chain attacks, where malware was embedded in legitimate apps or software updates. Attackers were able to circumvent traditional security protocols and gain access to a wide range of devices all before the malicious activity was identified. This was accomplished through the utilization of this technology. The level of sophistication

of these attacks brought to light the intricate nature of mobile ecosystems as well as the challenges that arise when attempting to defend them against attacks that exploit relationships of trust.

## 6.4 Statistics and Key Events from 2016 to 2020

The widespread adoption of smartphones and the growth of mobile technologies, particularly the transition to 4G and the beginning rollout of 5G networks, are the primary factors that are driving the exponential increase in the number of unique mobile malware samples and events that occurred during the period from 2016 to 2020. This era was characterized by a wide variety of malware variants and attack vectors which can be linked to the creativity of cybercriminals in their pursuit of the possibilities presented by the expanding digital landscape. Figure 5 illustrates the number of new malware samples that were found between the years 2016 and 2020.

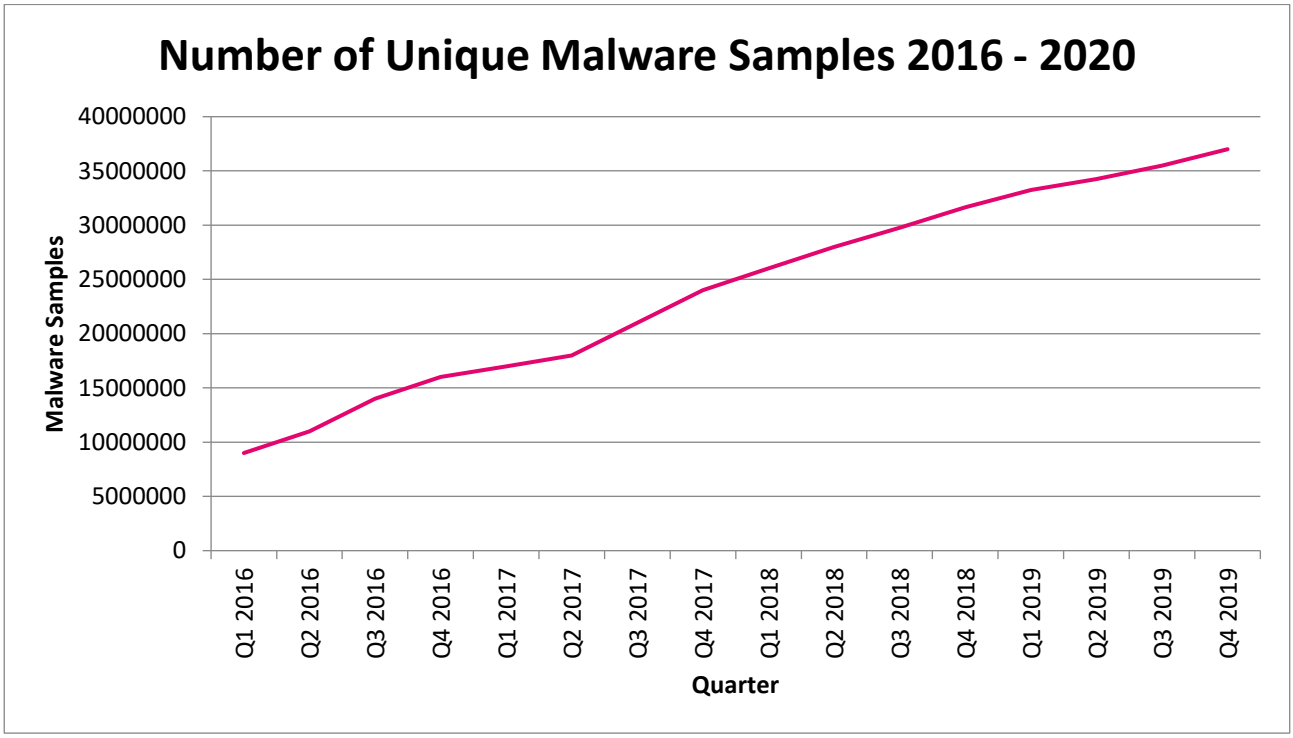


Figure 5. Number of Unique Malware Samples 2011- 2015 (McAfee, McAfee Mobile Threat Report, 2020) (McAfee, McAfee Labs Threats Report, 2018)

Millions of new malware samples are discovered every year, according to figure 5 from McAfee Threat Reports and which demonstrates the continuous growth of an mobile malware over the years. During the period from 2016 to 2020, the development of mobile malware reflected not only the extent to which individuals rely on mobile devices for both personal and professional purposes, but also the sophisticated ways that attackers utilized in order to take advantage of this dependence. In the Threat Report 2020 McAfee states that in the last couple of years they have witnessed diversification of malware types and attack vectors, demonstrating the creativity with which criminals have used the growing digital ecosystem (McAfee, McAfee Mobile Threat Report, 2020).

Research conducted by Kaspersky Labs indicates that there was an obvious increase in the amount of adware assaults that occurred in the financial year 2019. According to the research, the number of adware installation packages found has doubled from 2018 and from the new malware threats discovered in 2020 57.26% were AdWare (Chebyshev, 2020). Adware has emerged as one of the top three dangers detected during the period of 2016-2020, which indicates that cybercriminals are looking for ways to make money quickly and easily. Figure 6 is an illustration of the classification of new mobile malware samples according to their type in the years 2019 and 2020.

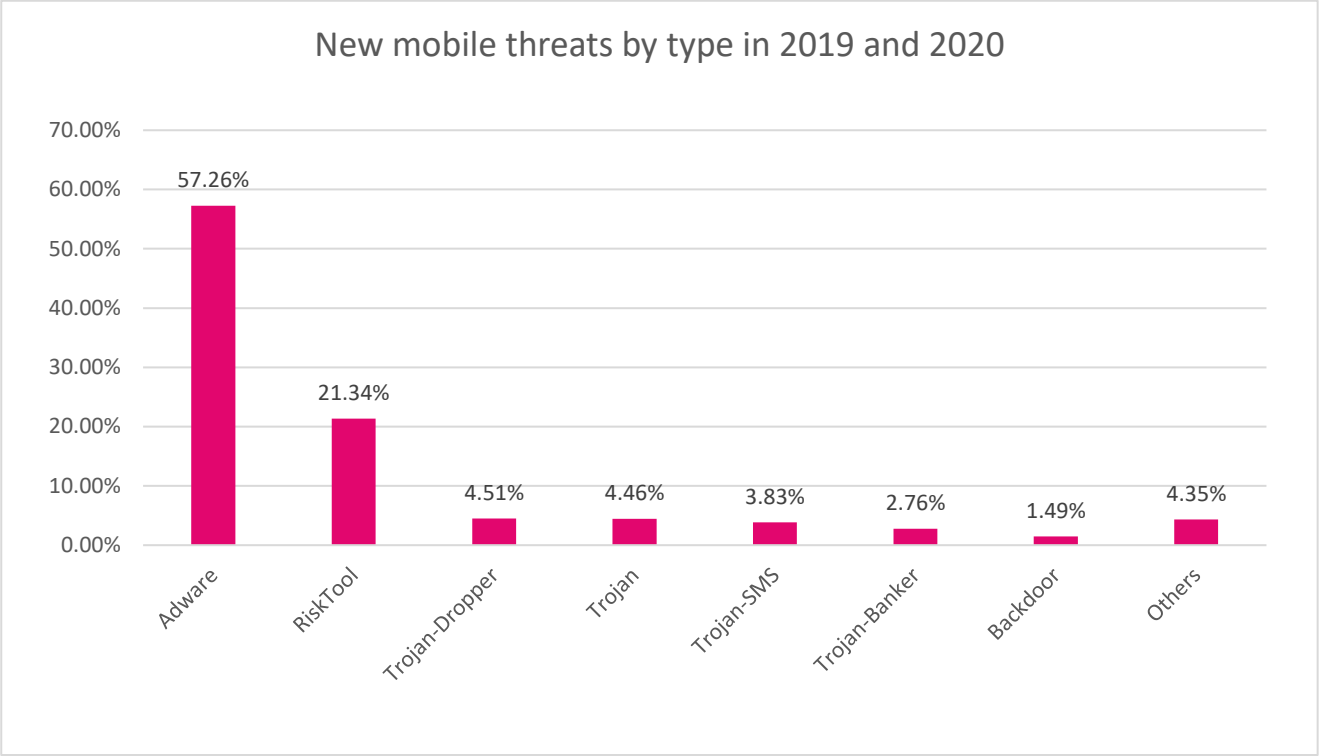


Figure 6. Distribution of new mobile threats by type in 2019 and 2020 (Chebyshev, 2020).

Some of key events of the period include the following:

**Pegasus (2016):** 2016 saw the development of the highly sophisticated spyware called the Pegasus by the Israeli cyberarms company NSO Group. It was intended to break into iOS and Android smartphones in order to collect a variety of information, such as text messages, emails, calls, location data, and even data from encrypted messaging services like Signal and WhatsApp. Pegasus is a very powerful spying tool since it can turn on a device's camera and microphone to monitor the environment.

Pegasus has been connected to multiple global events involving the monitoring of dissidents, journalists, activists, and political figures. It is well known for its capacity to take advantage of zero-day vulnerabilities, which are essentially undiscovered security flaws in operating systems or software that let it install itself on a target's device without the target having to do anything. Concerns regarding privacy, surveillance, and the possibility of abuse by state actors against political opponents and civil society have been highlighted by its use. The Pegasus revelations have sparked worldwide discussion on the morality of surveillance technology and the necessity of strict regulations and openness around governments' use of these instruments. In order to shield people from

state-sponsored cyber spying, it has also generated calls for stronger cybersecurity measures (Greengard, 2024).

**Judy Malware (2017):** The Judy malware, an auto-clicking adware, was discovered in 41 Google Play Store applications developed by a Korean business. When it was found in May 2017, an estimated 36.5 million Android devices had been compromised. Judy's primary objective was to fool people into clicking on fictitious advertisements so that the attackers could profit from their deception. The malicious apps, some of which had been published on the Google Play Store for a period of years, gave the impression of being legitimate games, but instead, they contained dangerous adware. Once installed, the virus would communicate with its command and control server (C&C) to acquire instructions, simulating clicking on adverts and accessing secret websites, all without the owner of the device's knowledge or consent (Check Point Mobile Research Team, 2017).

Judy's discovery sparked a much longer discussion about app store security and the procedures in place to detect and remove malicious apps. Google and other platform operators were also compelled to tighten up their app review processes and employ more advanced algorithms and detection techniques in order to prevent such incidents in the future.

**Agent Smith Malware (2019):** Malicious software that targeted Android smartphones was discovered in 2019 and was known as the Agent Smith malware. About 25 million devices were infected by Agent Smith worldwide, with a large number of infections occurring in Bangladesh, Pakistan, India, and other regions of Asia before the infection spread to other nations. It’s the nickname, which references to the antagonist of the "The Matrix" film series, captures its ability to pose as legitimate programs while covertly downloading hazardous ones. The majority of Agent Smith's distribution occurred through unofficial app stores, emphasizing the risks associated with downloading software from unreliable sources.

By utilizing known vulnerabilities in Android, the malware replaced installed apps on the smartphone with malicious ones without the user's intervention. The fake adverts that these compromised apps ultimately showed were profitable for the attackers. Agent Smith may be used in more serious scenarios to steal sensitive data from the user's device, such as email passwords and banking credentials, even if its primary function appeared to be adware-related actions (Check Point Research Team, 2019).

**COVID-19 Related Malware (2020):** In the year 2020, many different malware attacks were launched by cybercriminals who took advantage of the global crises that were caused by the COVID-19 epidemic. Individuals, businesses, and even government organizations were the targets of these attacks, which took advantage of the fear, uncertainty, and increased reliance on digital communications that were characteristic of the pandemic. There were many different kinds of malware that were associated with COVID-19, but they all shared a single characteristic: they pretended to be trustworthy sources of information or essential services that were related to the coronavirus. Here are some examples how attackers tried to benefit from COVID-19:

1. **Phishing Emails and Websites:** Cybercriminals sent out phishing emails pretending to be from health organizations like the World Health Organization (WHO) or the Centers for Disease Control and Prevention (CDC). These emails frequently included links or attachments that, if clicked, may infect a user's device with malware.
2. **Malicious COVID-19 Tracking Apps:** Profiting from the increased demand for COVID-19 information, hackers created and distributed malicious apps that claimed to monitor the virus's progress. After installation, these apps run the risk of infecting devices with malware, which could result in adware, spying, or data theft.
3. **Ransomware Attacks:** Attacks used ransomware that targeted research centers and healthcare organizations. Attackers encrypted valuable research data and demanded ransom payments to unlock it, hoping to profit from the epidemic. These attacks posed a serious risk to public health responses because of the pandemic's urgent need for access to research data and medical records.
4. **Fake COVID-19 Information and Donation Websites**: Cybercriminals created fake websites pretending to provide COVID-19 information or to ask for donations for the virus’s victims. These websites frequently tricked users into donating money that went straight to the criminals or spread malware when they were accessed. These websites might be especially misleading because some of them resemble trustworthy news or charity websites.

From the statistics and key events, it can be seen that apart from some advanced attacks and attacks that targeted politics and society, the vast majority of mobile cybercriminals appear to be interested in the simplest and fastest way to get financial gain from mobile malware. Click fraud,

adware, fake reviews, and ransomware seem to be the trend of the era, after criminals tried a number of other ways to make money from their efforts over the past few years for example the banking trojans during 2010-2015. Due to the fact that advertisers only pay a small amount for each clickthrough or ad display, the objective is to induce as many fraudulent behaviors as possible before being found. These malicious apps used to operate swiftly and early, but now they're slowing down in an effort to go undetected.

# 7 Modern Day Landscape (2021-2024)

## 7.1 Current State of Mobile Devices

Over the course of the current timeline, which spans from 2021 to 2024, there have been significant shifts in the landscape of mobile devices and operating systems. Not only do these changes reflect technology developments, but they also reflect a shift in user expectations and the ways in which user's engage devices. A higher emphasis has been placed on user-centric features, privacy, and security in this age as a result of the demands of a world population that is becoming more mobile and always connected.

The world of mobile devices has witnessed a breakthrough that is both revolutionary and rapid in its innovation. As a result of the introduction of foldable screens, users now have new possibilities for interacting with their smartphones and consuming content. This is because foldable screens have radically revolutionised the appearance and functionality of smartphones. By offering a versatile user interface that can be utilised for a variety of activities, such as gaming, watching movies, and reading, these foldable devices have successfully bridged the gap that existed between traditional smartphones and tablets.

Another important aspect of this time period has been the proliferation of 5G connectivity, which has resulted in increased mobile internet speeds and a reduction in latency to levels that were previously unreachable. Not only have technological improvements such as these made mobile internet more dependable and faster for users, but they have also made it possible for new services and applications to be developed, such as virtual reality (VR) and augmented reality (AR), which require connections with a high bandwidth and a low latency.

The operating systems that serve as the basis for mobile devices have also undergone significant transformations. Both Android and iOS, which are the two most popular platforms, have increased their security measures in response to the increasing threats that are posed by mobile malware. New permissions models that give users more control over the data that apps may access are included in these, as are frequent updates and patches that are designed to fix problems. In addition, modern operating systems have taken advantage of the capabilities of artificial intelligence in order to provide users with experiences that are more effective and personalised. The usability

and simplicity of mobile devices have been significantly enhanced by artificial intelligence, which has enabled the development of features such as predictive text and email suggestions, adaptive battery life management, and app usage estimates of mobile applications. Beyond the context of user interface, the addition of artificial intelligence has expanded to play a significant part in the enhancement of device security. In the present day, sophisticated machine learning algorithms have the ability to rapidly identify and eliminate dangers, providing a proactive approach to mobile security. This is a significant advancement in comparison to the reactive security measures that were implemented in the past, and it is a significant step in the right direction for securing the data and privacy of users.

## 7.2 Advanced Technologies Mobile Devices

Artificial intelligence and the Internet of Things are two examples of cutting-edge technologies that have been incorporated into mobile devices. These technologies have not only gained popularity, but they have also fundamentally altered the way mobile devices are used and how they function. During this period, there has been a convergence of technology and everyday life. Mobile devices have been at the center of this integration, serving as the primary interface for a wide variety of digital activities and services.

Artificial Intelligence has overtime become an effective tool in mobile technology, beyond its basic functions and becoming an essential part of mobile device architecture. Its capabilities have been used to enhance mobile computing in a variety of ways, including the enhancement of security protocols by means of anomaly detection algorithms and the enhancement of battery economy by means of adaptive power management. Voice-controlled assistants and suggestions that are aware of the context are two examples of how artificial intelligence has fundamentally transformed user interfaces, resulting in digital interactions that are more natural and distinct. The user experience has been enhanced as a result of these improvements, which have also made technology more accessible and customizable to fit unique requirements. Additionally, mobile devices have become more time and energy efficient.

The Internet of Things technology that has been integrated into mobile devices has simultaneously brought out a new era of being connected. Mobile phones are the key center for a wide variety of

connected devices in today's world. These devices include wearables, smart home appliances, automotive systems, and healthcare monitoring gadgets. The increasing number of "smart environments," in which individuals are able to monitor and control their surroundings with a level of simplicity and precision that has never been seen before, has been made possible by the connectivity that has been established. As a result of the mutual dependence of mobile devices and Internet of Things gadgets, new opportunities have been opened up in the areas of home automation, energy management, and remote healthcare. This demonstrates the transformative power of linked technology in everyday life.

Furthermore, during this period, there has been a great emphasis placed on the confidentiality and safety of Internet of Things integrations. Due to the fact that mobile devices are responsible for managing more sensitive data and are in charge of crucial tasks in linked ecosystems, manufacturers and developers have placed a larger emphasis on the construction of strong security frameworks for mobile devices. The purpose of these efforts is to safeguard users against potential vulnerabilities that could be exploited in a world that is highly connected. This is done to ensure that advancements in convenience and usefulness do not come at the expense of users' safety and privacy.

## 7.3 Impact of Mobile Malware in the Modern Era

Between the years 2021 and 2024, the dynamic threat environment of mobile malware had a significant influence on the condition of mobile technology, which revealed a wider trend in cybersecurity challenges. Attackers are more likely to target mobile devices because of their growing significance in both personal and professional lives. This has made mobile devices increasingly appealing targets for threats. In addition to the malware itself, the methods that are utilized to distribute and deploy these harmful apps have also become more sophisticated, which indicates that the level of complexity of these threats has increased.

One of the most notable changes that has occurred over this time period is the increase in the number of phishing attempts that are conducted against mobile users. Advanced social engineering tactics have been utilized by cybercriminals, who frequently create messages that are convincing in order to convince people to divulge personal information or download malicious software by

utilizing personalized information. Furthermore, during this period of time, there has been an apparent increase in the level of sophistication of spyware operations that are directed towards mobile devices. The user may not even be aware that these campaigns are gathering sensitive data, tracking user behavior, and even taking control of their devices without their permission. Violations of privacy of this nature have consequences that extend beyond the persons who are directly impacted, they also constitute major risks to the safety of both the nation and businesses.

The mobile environment has also seen a rise in ransomware attacks, whereby hackers encrypt users' data on their phones and demand payment in order to unlock it. In contrast to traditional ransomware assaults on personal computers, mobile ransomware frequently takes use of the sentimental value of the data stored on mobile devices, such as contacts, messages, and photographs. This makes the attack highly personal and increases the likelihood that the victim will be willing to pay the ransom.

The strategies employed by attackers to distribute mobile malware have also evolved. More and more malicious actors are taking use of genuine app stores by either disguising malicious software as harmless applications or taking advantage of weaknesses in legitimate applications in order to distribute malware to users who are unaware of the underlying threat. In addition, the usage of exploit kits, which are software programs that take advantage of vulnerabilities in mobile operating systems or applications in order to automatically install malware, has grown more and more common. These methods demonstrate how adaptable criminals may be and how hard they work to circumvent the stricter security controls that platform providers and app developers have established in place.

The impact of mobile malware during this period has been significant and diverse. Beyond the obvious losses in money and data that individuals and organizations have suffered, the growing number of mobile malwares has decreased confidence in digital ecosystems. This is in addition to the fact that these losses have been experienced. In addition to this, it has resulted in a re-evaluation of mobile security strategies, with an increased awareness of the requirement for complete security solutions that incorporate user awareness and education in addition to technological safeguards.

## 7.4 Statistics and Key Events from 2021 to 2024

In the history of mobile malware, the years 2021–2024 marked notable advancements in attack complexity and defense mechanisms. The use of mobile devices has increased drastically in this era, primarily because of the COVID-19 epidemic and the ongoing worldwide trend towards remote work and digital transformation. As mobile devices grew increasingly integrated into people's personal and professional life, they became a primary target for cybercriminals.

According to data conducted by Kaspersky Security Network, there was a once again increase in the number of adware attacks in the year 2023. Of all the threats detected 63.66% was mobile device adware reaching again number 1 position from overall malware types discovered. Between 300 000 and 500 000 of new mobile malware samples are discovered in ever quarter. The figure 7 illustrates how new mobile malware found were divided by their type in 2023.

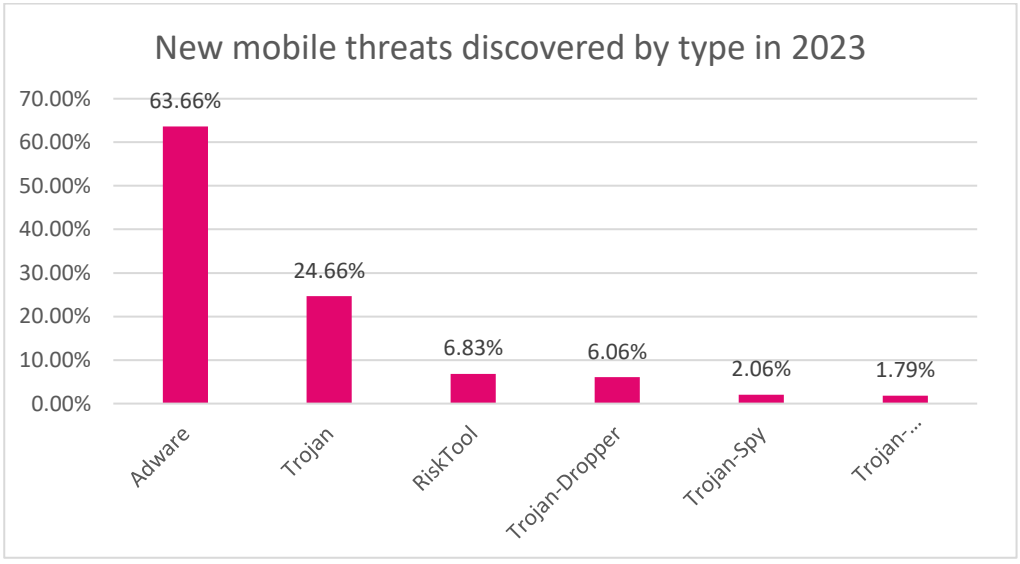


Figure 7. Distribution of detected installation packages by type (Kivva, IT threat evolution in Q3 2023. Mobile statistics, 2023)

According to Kaspersky Labs, 33 790 599 attacks were prevented by their products overall in 2023. The number of mobile device attacks decreased to 2,000 000 cases per month in January 2023 between the years 2021 and 2023, but it began to rise again in the latter half of 2023, reaching over 5,000 000 recorded incidents per month. Figure 8 shows the number of attacks targeting users of Kaspersky mobile solutions.

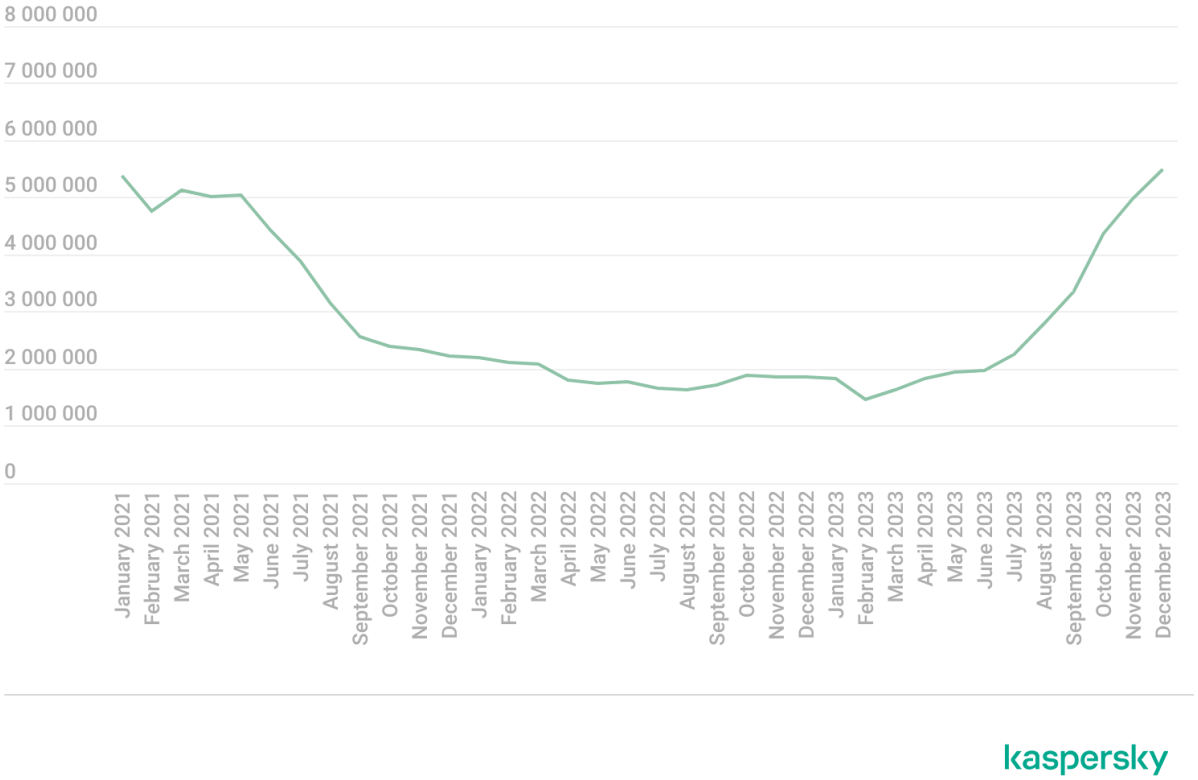


Figure 8. Number of attacks targeting users of Kaspersky mobile solutions, 2021–2023 (Kivva, The mobile malware threat landscape in 2023, 2024)

Some of key events of the period include the following:

**Flubot (2021):** The Flubot virus was a mobile malware that mostly targeted Android mobile devices. However, there were concerns that it might spread to other platforms as well given its widespread distribution. Malware was spread using smishing attacks, which consisted of sending text messages that contained links to malicious websites. In the phishing text message, clients were directed to download a piece of software that was actually malware disguised as a legitimate program when they clicked on the link. Theft of banking and financial information was one of the primary goals of the Flubot program. It was able to accomplish this by placing fake login panels on top of real banking applications whenever customers sought to access their financial accounts, thereby collecting login information in the process. In addition to their ability to steal information,

Flubot might also provide attackers with remote control over the machines that have been infected, which would allow for a wide variety of destructive operations (Europol, 2022).

**BrazKing (2022):** Specifically aimed targeting Android smartphones, the mobile banking Trojan known as BrazKing was primarily seen in Brazil. BrazKing is often disguised as a real banking application, and after it was installed, it had the ability to display fake log-in panels on top of actual banking apps. This occurred when the user attempted to access their accounts, and it collected login information as well as other sensitive information in the process. Fake websites, SMS phishing, and third-party app stores were the methods that were used to spread the BrazKing malware. By sending users fake notifications that suggested they needed to update or confirm their banking information, or by employing other social engineering techniques, users were tricked into installing the Trojan without their knowledge.

The primary objective of BrazKing was to always steal money from the bank accounts of the victims. It is possible for attackers to carry out unauthorized operations such as fund transfers and purchases if they gain the passwords in order to log in to their banking accounts and credit card details. The cybercriminals who were responsible for BrazKing were continually making changes to the virus in order to prevent it from being detected by security software and to accommodate the new security measures that banking institutions had implemented. This included alterations to its coding, distribution processes, and the fake applications that it copied (KL, 2021).

# 8 Research Findings and Future Trends

## 8.1 Key Findings

Between the years 2000 and 2024, a review of the development of mobile malware provides a comprehensive overview of the ways in which mobile threats have advanced in parallel with technological advancements in mobile devices, networks, and mobile services. Among the many important discoveries that are highlighted by this research are the adaptability and growing complexity of mobile malware, the development of attack vectors based on trends in mobile device and mobile service development, and the ongoing battle that exists between cybercriminals and cybersecurity defenses. Expanding on the main research findings in the following chapters.

### 8.1.1 Financially Motivated Malware

A noticeable trend towards threats that are motivated by financial gain has taken place in the field of mobile malware. Malware such as adware, banking Trojans, ransomware, and cryptojacking has become increasingly widespread, and it is being used to steal financial information and turn the mobile platform into a platform for attackers to use for their own benefit. This shift is indicative of a general upward trend in cybercrime, in which attackers are attracted to targets that represent their biggest opportunity for financial gain. Due to the fact that mobile devices contain a wide range of personal and financial information, they have become an appealing target for unlawful activities.

It is possible to come to the conclusion that between the years 2010 and 2015, banking trojans were the dominant attack vector for criminals who were aiming to earn financially from mobile malware. This conclusion is based on several statistics and key events that were described in the chapters. From the year 2015 till the present day, there has been a widespread movement towards adware and ransomware attacks. Before the year 2010 most of the mobile malware variants were not intended to cause much actual harm to infected devices other than slight inconvenience and very minor financial loss.

### 8.1.2 Increased Sophistication and Evasion Techniques

The evolution of mobile malware demonstrates a significant rise in the sophistication of attack methods and evasion strategies. The earliest forms of mobile malware were straightforward, and they were developed primarily for the goal of annoying users rather than for any criminal purposes. Malware, on the other hand, evolved to become stealthier and more complicated as mobile devices became more common and users became more dependent on these devices and the services that they offer in their private as well as their professional lives. Mobile malware is currently using sophisticated techniques such as polymorphism and metamorphism in order to avoid detection by standard antivirus solutions. These advancements are a reflection of the improved understanding that attackers have about mobile operating systems, which enables them to exploit vulnerabilities with greater precision.

### 8.1.3 State-Sponsored and Politically Motivated Malware

In addition, the research data indicates that since 2015, there has been a rise in mobile malware operations that are politically motivated and supported by states. These operations are distinguished by their restricted focus and high level of skill in execution. Many of these operations are centered on monitoring, spying, and political manipulation by the very nature of them. The tactical importance of mobile devices as vectors for gathering information and cyber warfare is highlighted by the fact that state actors are using mobile malware to carry out their operations.

### 8.1.4 The Impact of Emerging Technologies

The increase in the amount of mobile malware has been significantly influenced by a number of emerging technologies, including machine learning, artificial intelligence, and the Internet of Things, amongst others. At the same time that these technologies have introduced new vulnerabilities and attack vectors, they have also increased the attack surface that hackers have access to. With the increasing integration of these technologies into mobile devices and networks, it is projected that they will have a significant impact on the future landscape of mobile malware.

## 8.2 Predictions Regarding the Future of Mobile Malware

Predicting the future trend of mobile malware is a difficult challenge because of the continuously changing landscape of mobile technology, which when combined with the changing strategies of hackers, means that the industry is constantly developing. By analyzing the findings of the research, technological advancements, and changes in the behavior of cybercriminals, it is possible to make predictions that are fairly accurate on the route that mobile malware threats will take in the future and the types of dangers they will represent.

It is quite clear from the research findings that attackers always follow the most recent developments in mobile technology. It can be determined that the mobile ecosystem will see a significant increase in malware that makes use of artificial intelligence and machine learning technologies for malicious purposes as these technologies advance in capability. With the help of artificial intelligence and machine learning, malicious software may be taught to learn from its surroundings and alter its behavior in order to avoid detection, automatically identify recently identified vulnerabilities, and carry out attacks with no user interaction. Additionally, artificial intelligence might be utilized to generate phishing assaults in large quantities, so rendering them more convincing and difficult for users to recognize.

In addition, it is possible to draw the conclusion that mobile wallets and payment systems will grow more vulnerable to mobile malware attacks as their use becomes increasingly common. More advanced malware that is intended to intercept transactions or steal cryptocurrencies by taking advantage of vulnerabilities in these programs is probably going to be developed by cybercriminals. It is possible that attacks of this sort might have serious effects on the financial health of both individuals and businesses. Attackers are currently gathering all the ransomware payments in Bitcoin, which allows attackers to receive payments from victims into private Bitcoin wallets that are not held at regulated organizations.

5G networks are being deployed globally, offering the capacity to connect more devices at once and higher internet speeds. However, there are additional security challenges brought up by 5G. The increased bandwidth and capabilities of edge computing will make it possible to launch new kinds of attacks that were previously impossible due to the limitations of prior generations of mo-

bile networks. Hackers, for example, may make use of the speedier connections and reduced latency in order to carry out distributed denial-of-service attacks with more success or to take control of infected devices and steal their data in a more rapid approach.

Supply chain attacks are made possible by the complex nature of the mobile ecosystem, which includes third-party libraries, app stores, and creators of apps. There is a possibility that malicious actors who are attempting to spread malware around the world could breach this supply chain at any point in time. An example of this would be the hacking of a well-known library that is utilised by mobile app developers, which might result in malicious software being automatically incorporated into otherwise legitimate applications. While it is true that attacks of this kind have been around ever since the introduction of app stores and application development, the characteristics of these attacks and the mobile environment in which they are carried out have evolved over the course of time.

The Internet of Things is expanding at a rapid rate as a result of the increasing number of devices that are connected to the internet and are often operated by applications on smartphones. Mobile malware could be exploited by attackers as a means of gaining access to Internet of Things devices or mobile devices. Attackers may find this expanding network to be an interesting target. As a result of the wide range of Internet of Things devices and the numerous security configurations they employ, these devices are susceptible to attacks that can rapidly spread over several networks and devices.

Phishing attackers that target mobile devices now have access to a new tool that has the potential to be extremely powerful thanks to the development of deepfake technology and synthetic media techniques. Deepfakes have the ability to produce incredibly realistic audio or video recordings of recognisable people, such public personalities or company executives, in order to trick victims into revealing private information or doing acts that risk security. In the future, when this technology becomes more generally available and advanced, it will be extremely challenging to recognise and defend against attacks that are both personalised and targeted at specific individuals.

## 8.3 Future of Mobile Security

The development of mobile malware has had a major impact on the landscape of mobile security, which has resulted in significant advancements in defensive technology and techniques. Considering the growing importance of mobile devices in both personal and professional areas, it is essential to understand the impact of this development in order to create effective security measures.

The ongoing arms race between cybersecurity experts and cybercriminals has accelerated the creation of more advanced defensive systems. Leading the way in this technological advancement are machine learning and artificial intelligence, which provide the ability to predict hazards and take action with excellent accuracy and speed. When these technologies are integrated into mobile security systems, it enables automatic responses and the identification of threats in real time, which in turn reduces the window of opportunity for attackers.

Furthermore, the development of mobile malware has accelerated the progress of secure communication protocols and encryption technology. Because hackers are always developing new ways to intercept and alter data, there is an increasing demand for secure encryption methods. This requirement is becoming more and more visible. Regarding upcoming mobile security protocols, it is quite likely that end-to-end encryption for data both while it is in transit and while it is at rest would be given priority. This will ensure that data cannot be decoded by unauthorized parties.

The relevance of privacy and data protection has increased due to the increasing complexity of mobile viruses, especially with regard to spying and data theft. It is because of this knowledge that technological advancements and changes in regulations are being made with the objective of securing user data. As an example, mobile operating systems are introducing more detailed permission limitations, which enables users to take greater control over the data that each application has permission to access. In addition, the legal environment that has been developed as a result of the introduction of privacy-focused laws, such as the General Data Protection Regulation (GDPR) in Europe, requires app developers and service providers to place the user's privacy as their top priority.

The evolution of mobile malware highlights the limitations of reactive security measures that focus just on identifying and neutralizing recognized threats. In the future, mobile security will probably

take a more proactive position. In order to avoid, detect, respond to, and recover from threats, security frameworks with interconnected components must be created. Furthermore, a greater emphasis will be made on safe software development processes, which will ensure that applications and services are developed with security in mind from the very beginning of the development process.

# 9 Conclusion

The Research of the evolution of mobile malware from 2004 to the present day has provided insight into the always evolving landscape of cybersecurity in the age of smartphones. Early mobile viruses like Cabir and Commwarrior, which took advantage of the weaknesses in the expanding mobile ecosystem, marked the beginning of the mobile malware and mobile threats. The growing popularity of mobile technology has led to an increase in the sophistication and depth of mobile malware, which has resulted in a variety of threats to the users' privacy and the security of their data. Malware such as Trojan horses, spyware, ransomware, and adware were among these threats.

Based on the findings of the research, it is clear that malware that is motivated by financial gain has been the most prevalent type of malware in the field of mobile malware. Malicious actors have been attempting to make a financial advantage from the development of mobile malware ever since the introduction of app stores and mobile banking services in the late 2000s. Since the year 2015, adware has been the type of malware that is being produced the most. This demonstrates the motivation of malicious actors in seeking quick financial gain.

One of the most important discoveries made by the researchers is the connection between mobile virus developers and the progression of technology in mobile devices. As a result of the extensive deployment of 4G and 5G networks, as well as the fast adoption of smartphones, the diversity of assaults has increased, making mobile devices an appealing target for hostile actors. The increase in mobile malware related incidents shows that this connected era has brought major threats along with previously unheard-of access to information and services.

The research findings also highlighted how the expanding mobile ecosystem, defined by the Internet of Things, has expanded the attack surface for cybercriminals. Despite the fact that it has increased both productivity and convenience, this new type of connection has also brought forth significant security concerns. Although there are many advantages to mobile technology advancements, it has also accidentally contributed to the growth of mobile malware development. Increasing computer power, greater connection, machine learning and artificial intelligence, and the increasing number of mobile applications are some of the elements that cybercriminals have taken

advantage of in order to develop variations of malware that are more efficient and harder to detect. Rather than putting security concerns off to a later stage in the development lifecycle, this demonstrates how critical it is to put security concerns at the forefront of technological innovation from the very beginning. Even though the attack surface has significantly grown overtime due to these factors, the review of the key events indicates that social engineering, phishing, and app stores have been the primary attack vectors for the majority of mobile malware history.

The research findings highlight the importance of resilience and adaptation in facing the challenges of evolving malware threats. Constant monitoring, regular updates to security processes, and the development of new countermeasures are all necessary in order to keep up with the dynamic world of mobile malware. Collaboration between cybersecurity professionals, developers of mobile devices, developers of mobile applications, as well as end users is required in order to build an effective defense system against the threat posed by mobile malware.

In conclusion, a study of the evolution of mobile malware demonstrates an environment that is characterized by increasing complexity, vulnerabilities that are cross-platform, and a continuous need for innovative cybersecurity solutions. The knowledge gained from this study increases our understanding of the difficulties and possibilities involved in protecting mobile landscape from harmful actors.

# 10 References

Apvrille, A. (2014). The evolution of mobile malware. *Computer Fraud & Security, Volume 2014, Issue 8*, 18-20.

Brewster, T. (2011, March 7). *Google promises better Android security after DroidDream*. Retrieved from itpro: https://www.itpro.com/631657/google-promises-better-android-security-after-droiddream

Castle, W. (2019, October 2019). *4G vs 5G Security, The Key Differences*. Retrieved from wraycastle: https://wraycastle.com/blogs/news/4g-vs-5g-security-the-key-differences

Chebyshev, V. (2020, February 25). *Mobile malware evolution 2019*. Retrieved from securelist: https://securelist.com/mobile-malware-evolution-2019/96280/

Check Point Mobile Research Team. (2017, May 25). *The Judy Malware: Possibly the largest malware campaign found on Google Play*. Retrieved from checkpoint: https://blog.checkpoint.com/securing-user-and-access/judy-malware-possibly-largest-malware-campaign-found-google-play/

Check Point Research Team. (2019, July 19). *"Agent Smith": The New Virus to Hit Mobile Devices*. Retrieved from checkpoint: https://blog.checkpoint.com/security/agent-smith-android-malware-mobile-phone-hack-virus-google/

digicontentexperts. (2023, 10 26). *Android Operating System: Advantages And Disadvantages*. Retrieved from digicontentexperts: https://www.digicontentexperts.com/blog-detail/android-os-pros-and-cons

Ettinger, G. (2023, August 18). *What Happened To Nokia? The Rise And Fall Of A Tech Giant*. Retrieved from slashgear: https://www.slashgear.com/1369622/what-happened-to-nokia-explained/

Europol. (2022, June 1). *Takedown of SMS-based FluBot spyware infecting Android phones*. Retrieved from Europol: https://www.europol.europa.eu/media-press/newsroom/news/takedown-of-sms-based-flubot-spyware-infecting-android-phones

Galazzo, R. (2020, Septemper 21). *Timeline from 1G to 5G: A Brief History on Cell Phones*. Retrieved from cengna: https://www.cengn.ca/information-centre/innovation/timeline-from-1g-to-5g-a-brief-history-on-cell-phones/

Glazova, J. (2021, March 19). *Stalkerware in 2020 is still a burning issue*. Retrieved from kaspersky: https://www.kaspersky.com/blog/stalkerware-in-2020/39102/

Gostev, A. (2008, May 07). *Malware evolution: January – March 2008*. Retrieved from securelist: https://securelist.com/malware-evolution-january-march-2008/36208/

Greengard, S. (2024, March 9). *Pegasus (spyware)*. Retrieved from britannica: https://www.britannica.com/topic/Pegasus-spyware

Guardsquare. (2019, May 20). *Fake Mobile Apps: A Growing Threat*. Retrieved from Guardsquare: https://www.guardsquare.com/blog/fake-mobile-apps-growing-threat-2019

Henry, J. (2022, March 09). *Mobile Malware Cyberattacks Rise to 500% on the First Few Months of 2022*. Retrieved from Techtimes: https://www.techtimes.com/articles/272773/20220309/mobile-malware-cyberattacks-rise-500-first-few-months-2022-heres.htm

Hernandez, J. (2023). *What is the actual cost of cybercrime?* Retrieved from Evolvesecurity: https://www.evolvesecurity.com/blog-posts/actual-cost-of-cybercrime

Kaspersky. (2011, October 06). *Teamwork: How the ZitMo Trojan Bypasses Online Banking Security*. Retrieved from kaspersky: https://www.kaspersky.com/about/press-releases/2011_teamwork-how-the-zitmo-trojan-bypasses-online-banking-security

Kivva, A. (2023, December 1). *IT threat evolution in Q3 2023. Mobile statistics*. Retrieved from securelist: https://securelist.com/it-threat-evolution-q3-2023-mobile-statistics/111224/

Kivva, A. (2024, February 26). *The mobile malware threat landscape in 2023*. Retrieved from securelist: https://securelist.com/mobile-malware-report-2023/111964/

KL, A. (2021, November 24). *How To Protect Your Android Device From The New BrazKing Android Malware?* Retrieved from thesecmaster: https://thesecmaster.com/blog/how-to-protect-your-android-device-from-the-new-brazking-android-malware

Kolmar, C. (2023, March 2). *25+ INCREDIBLE US SMARTPHONE INDUSTRY STATISTICS [2023]: HOW MANY AMERICANS HAVE SMARTPHONESS*. Retrieved from Zippia: https://www.zippia.com/advice/us-smartphone-industry-statistics/

Lab, K. (2014, February 24). *Mobile malware evolution: 3 infection attempts per user in 2013*. Retrieved from kaspersky: https://www.kaspersky.com/about/press-releases/2014_mobile-malware-evolution-3-infection-attempts-per-user-in-2013

Malware. (2021, February 10). *What Are Banking Trojans, and How Worried Should You Be About Them?* Retrieved from sitelock: https://www.sitelock.com/blog/what-are-banking-trojans/

Maslennikov, D. (2011, May 22). *Mobile Malware Evolution: An Overview, Part 4*. Retrieved from securelist: https://securelist.com/mobile-malware-evolution-an-overview-part-4/36350/

Maslennikov, D. (2011, October 06). *ZeuS-in-the-Mobile – Facts and Theories*. Retrieved from securelist: https://securelist.com/zeus-in-the-mobile-facts-and-theories/36424/

McAfee. (2018). *McAfee Labs Threats Report.*

McAfee. (2020). *McAfee Mobile Threat Report.*

Meyer, C. (2010, 11 14). *Apple Business Strategy 2011:*. Retrieved from workingwider: https://www.workingwider.com/strategic_innovation/apple-business-strategy-2011-milk-the-icow-for-growth-cash/

Neil Bergman, M. S. (2013). *Hacking Exposed Mobile Security Secrets & Solutions.* McGraw-Hill/Osborne.

Osborne, C. (2023, October 18). *9 top mobile security threats and how you can avoid them*. Retrieved from zdnet: https://www.zdnet.com/article/9-top-mobile-security-threats-and-how-you-can-avoid-them/

Santosh K. Smmarwar, G. P. (2024). Android malware detection and identification frameworks by leveraging the machine and deep learning techniques: A comprehensive review. *Telematics and Informatics Reports, Volyme 14*.

Shankland, S. (2022, July 19). *Pegasus Spyware and Citizen Surveillance: Here's What You Should Know*. Retrieved from Cnet: https://www.cnet.com/tech/mobile/pegasus-spyware-and-citizen-surveillance-what-you-need-to-know/

Snyder, J. (2019, February 21). *The evolution of mobile security solutions*. Retrieved from https://insights.samsung: https://insights.samsung.com/2019/02/21/the-evolution-of-mobile-security-solutions/

Speed, T. (n.d.). *Mobile security : how to secure, privatize, and recover your devices : keep your data secure on the go.* Packt Publishing.