## INTRODUCTION:

Android malware is malicious software created specifically to affect devices running the Android operating system and its users. Malware designed particularly to infect Android devices and the people who use them is known as Android malware. It is a problem that is growing more prevalent in the realm of mobile devices, and it can cause physical damage to the devices as well as violate the privacy of the users.

Malware that targets Android devices can be disseminated through a variety of tactics, such as phishing and visiting websites that have been compromised, among others. Android devices are susceptible to a wide variety of malware attacks, including adware, spyware, ransomware, banking Trojans, and rootkits, to name a few. Every variety of malicious software serves its own unique function and operates in its own unique way.

You will need to take specific preventative measures in order to keep harmful malware from harming your Android smartphone. Sticking to apps that come from the official Google Play store, upgrading your smartphone on a regular basis, utilising a reputable security programme, and exercising common sense while downloading and installing new apps are all good ways to avoid falling victim to phishing scams and other forms of online fraud.

## EVOLUTION OF ANDROID MALWARE



<https://news.sophos.com/wp-content/uploads/2015/04/sophos-mobile-malware-infographic-700.png>

Since the beginning of the Android operating system, malicious software for Android has been a source of concern. Malware designed to infect Android devices has undergone significant development throughout the course of its existence, reflecting shifts in the Android platform, the technology industry, and the strategies employed by cybercriminals. The following is a concise outline of the history and development of malicious software on Android:

## **Infancy of Anroid Malware:**

Between 2004 and 2010, malicious software for Android was very uncommon and frequently of a primitive nature. Early examples of malicious software for Android included trojans that might steal personal information; however, these dangers were typically simple to identify and eliminate.

Cabir, identified in June 2004, was one of the first known mobile phone viruses. It was a proof-of-concept virus that infected Symbian-based mobile phones. Cabir infected phones via Bluetooth and propagated from one infected device to another without any user intervention.

The virus was called from the words "Cabir" found in the virus's code. When a device became infected, the virus showed a message on the screen informing the user that the device had been infected and pushing the user to spread the infection to other devices.

While Cabir did not cause major harm to compromised devices, it was a watershed point in the growth of mobile malware. It proved that mobile devices were susceptible to malware and that these risks may be transmitted via wireless networks such as Bluetooth.

Cabir's finding raised concerns about the security of mobile devices, prompting the creation of security measures and solutions to combat mobile malware.

Between 2004 and 2010, several significant mobile malware threats were discovered and several of them are highlighted below:

Cabir (2004) - Cabir was one of the first known mobile phone viruses, discovered in June 2004. It was a proof-of-concept virus that affected mobile phones running the Symbian operating system and was able to infect devices via Bluetooth.

Commwarrior (2005) - Commwarrior was a worm that affected Symbian OS-powered mobile phones. It spread via MMS and Bluetooth, and once a device was infected, the worm was able to replicate itself and spread to other devices.

Skulls (2006) - Skulls was a Trojan that affected Symbian OS-powered mobile phones. It was disguised as a legitimate application and was able to steal sensitive information from infected devices.

Vegas (2006) - Vegas was a Trojan that affected Windows Mobile-powered devices. It was disguised as a legitimate application and was able to steal sensitive information from infected devices.

Commjacking (2007) - Commjacking was a proof-of-concept attack that exploited vulnerabilities in Bluetooth-enabled devices. It allowed attackers to gain unauthorized access to devices and steal sensitive information.

CoreeBot (2007) - CoreeBot was a worm that affected Symbian OS-powered mobile phones. It was able to spread via MMS and Bluetooth and was able to steal sensitive information from infected devices.

Cabass (2008) - Cabass was a worm that affected Symbian OS-powered mobile phones. It was able to spread via Bluetooth and was able to steal sensitive information from infected devices.

## The Emergence of sophisticated threats (2011-2012):

By 2011, attackers had begun to develop increasingly sophisticated Android malware that was designed to steal sensitive information and control infected devices. In 2012, this type of threat continued to evolve.

Geinimi (2011): Geinimi was one of the first advanced Android malware strains. Geinimi was developed by the Japanese company Geinimi. It was developed with the purpose of stealing sensitive information and exerting control over devices that it infected. It was identified in 2011, and it had spread through Android app marketplaces that were not affiliated with Google. This event represented a turning point in the development of malicious software for Android, as cybercriminals began to concentrate their efforts more on malicious software that could steal private information.

Obad (2012) is the year when the sophisticated trojan known as Obad was found. It had the ability to collect personal information as well as install further malicious software on systems that it infected. It was one of the earliest instances of Android malware that was used to construct botnets and perpetrate mobile ad fraud. It was propagated by malicious apps, and it was one of the first instances of Android malware that was able to use a device as a bot in a botnet.

DroidDream (2011) - DroidDream was an Android malware family that was found in 2011. The infection was distributed through third-party app shops while masquerading as legal programmes. Once installed, the malware might steal sensitive information such as device IDs and user data and download further infections onto targeted devices.

GingerMaster (2012) - GingerMaster was an Android malware family detected in 2012. The infection was distributed through third-party app shops while masquerading as legal programmes. Once installed, the malware might steal sensitive information such as device IDs and user data and download further infections onto targeted devices.

ZeuS (2011) - ZeuS was a financial Trojan family that targeted both desktop and mobile computers. It was capable of stealing important information from infected machines, such as login passwords and financial information.

SpyEye (2011 film) - SpyEye was a banking Trojan that was designed to attack both desktop and mobile computers. It was capable of stealing important information from infected machines, such as login passwords and financial information.

Flashback (2012) - In 2012, a family of Mac OS X malware known as Flashback was found. The software spread via malicious websites and was capable of stealing important information from infected machines, such as login passwords and financial information.

## Era of botnets and fraudulent activity in mobile advertising

In the years that followed, malicious software for Android continued to advance, with cybercriminals utilizing infected devices to build botnets and perform mobile advertising fraud. The "Obad" trojan, which was found in 2012, is a good illustration of this category of malicious software. In 2013, The "FakeID" vulnerability was discovered, which allowed attackers to create malicious apps that could access sensitive information on an Android device. This vulnerability was particularly concerning because it could be used to steal sensitive information such as login credentials, credit card details, and other personal information. The "Stagefright" vulnerability was discovered, which affected a large number of Android devices and allowed attackers to remotely execute code on the infected device. This vulnerability highlighted the importance of keeping Android devices up-to-date with the latest security patches.

In 2015 and 2016, attackers began to focus more on exploiting vulnerabilities in the Android operating system and other components of Android devices. This shift in attention on exploiting flaws was a result of the growing focus on vulnerabilities that occurred in 2015 and 2016. The "AdUps" malware was discovered, which was found pre-installed on a number of Android devices and used to collect sensitive information such as text messages and location data.

In 2016, The "Gooligan" malware was discovered, which infected over a million Android devices and used them to steal sensitive information and generate revenue through fraudulent advertising. HummingBad (2016): HummingBad was a strain of malicious software that was found in the year 2016. It was developed with the purpose of stealing sensitive information and exerting control over devices that it infected. It was distributed through malicious applications and was used to construct botnets and perform mobile ad fraud.

## Present day status of Android Malware

In the years that have passed since then, a malicious software designed for Android has continued to progress, with cybercriminals adopting new strategies and making use of newly discovered vulnerabilities in order to transmit malware to Android devices. Malware that is transmitted via malicious apps, malware that exploits weaknesses in the internet of things, and malware that uses cloud-based services to store and disseminate malware are some of the most recent dangers.

Agent Smith (2019): Agent Smith was a strain of malicious software that was found in the year 2019. It was designed to replace legal apps on Android smartphones with malicious versions, which would then be used to display adverts that the user did not wish to see. The malicious software was distributed over unofficial Android app marketplaces and has the potential to infect a significant number of different devices.

Joker (2019): Joker was a strain of malicious software that was found in the year 2019. It was developed with the purpose of stealing sensitive information and exerting control over devices that it infected. It was capable of infecting a significant number of devices and was distributed using apps that were designed to do harm.

xHelper (2020): xHelper was a strain of malicious software that was found in the year 2020. It was developed with the purpose of stealing sensitive information and exerting control over devices that it infected. It was disseminated via malicious applications, and the fact that it was so difficult to eradicate from a device once it had already done so was a major cause for concern.

Anubis (2020): Anubis was the name of a strain of malware that was found in the year 2020. It was developed with the purpose of stealing sensitive information and exerting control over devices that it infected. It was disseminated using malicious apps and was utilized to steal bank information as well as commit mobile ad fraud.

These are only some of the most significant moments in the development of malicious software for Android throughout its history. The Android platform and the technology sector have made great progress over the years in enhancing the security of Android devices. Despite these advancements, the danger of malware continues to pose a serious risk to users of Android devices. It is likely that the hazards posed by Android malware will continue to evolve as the technology continues to evolve as well. As a result, the technology sector, governments, and users will need to be vigilant in order to prevent and respond to these threats.

## TYPES OF ANDROID MALWARE

There are a number of different forms of malware for Android, each of which has the potential to compromise a user's device, their personal data, or their privacy. The following are some of the most prevalent types:

Adware is a form of malware that causes unwanted advertisements and pop-up windows to appear on the device. It can slow down the device or possibly cause it to crash, and it is frequently exploited by the attacker to make income for themselves.

Spyware is a form of malware that is designed to monitor and gather sensitive information such as user passwords and financial information. Spyware is used to monitor and collect sensitive information. In addition to that, it is able to monitor the location of the device and record both phone calls and text messages.

Ransomware is a sort of malicious software that encrypts user data on a device and then demands payment from the user in order to decrypt the data. Additionally, it has the capability to encrypt files and bar access to them until the ransom is paid.

Trojan horses that pretend to be legitimate banking applications are a form of malware that steals financial information and is known as banking Trojans. It is possible for it to steal login credentials as well as financial information, which could lead to fraudulent activities.

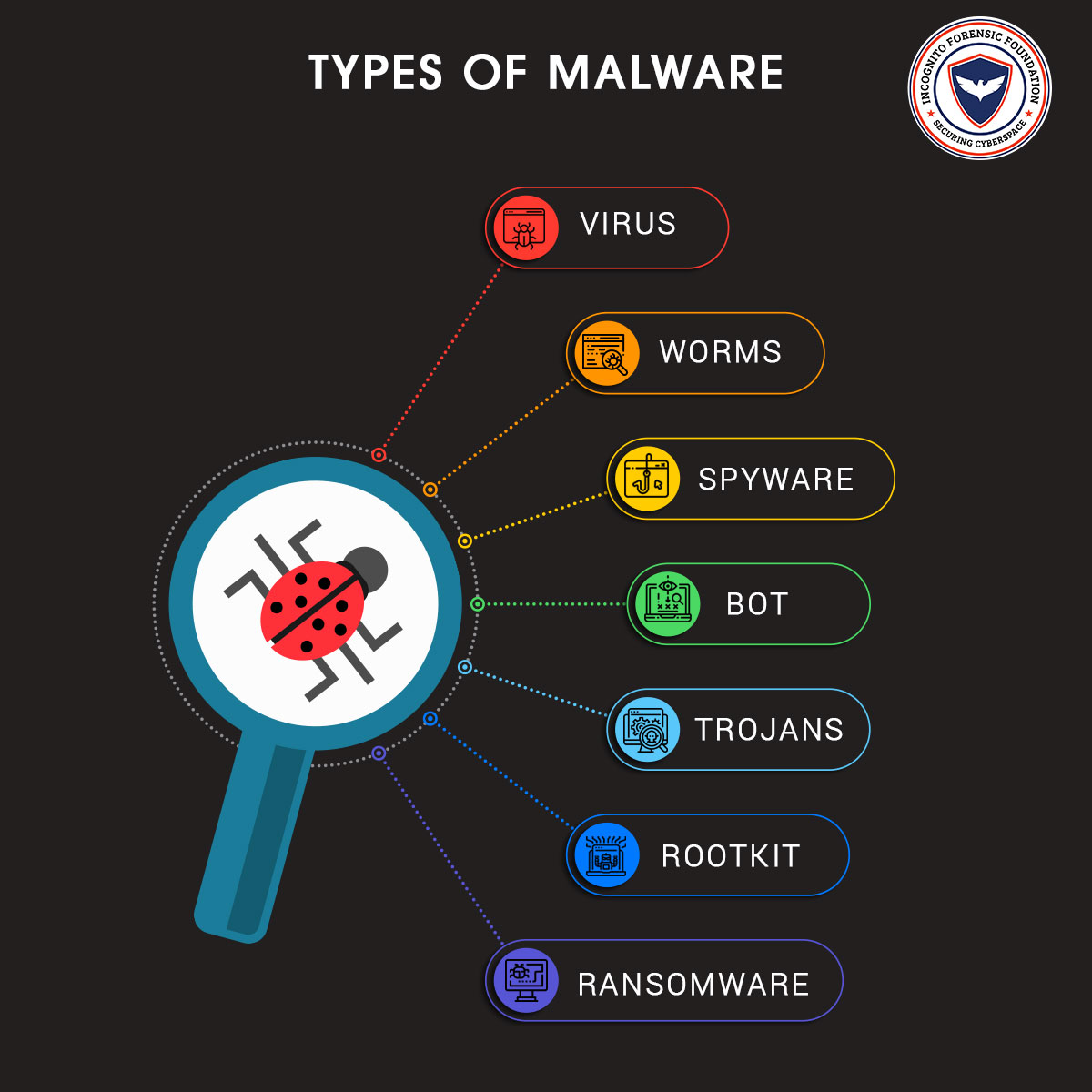
Rootkits are a sort of malicious software that, once installed, grants the attacker full control over the infected device and conceals the malware's presence on the device, making it difficult to find and eliminate.

SMS Trojans are a form of virus that, without the knowledge of the user, sends text messages to premium-rate numbers. This results in the user being charged a premium rate for each message.

Trojans that open backdoors on devices are a form of malware that enables an adversary to gain remote access and control over a device. Backdoor Trojans open a backdoor on the device.

Trojans that allow remote access, also known as Remote Access Trojans (RATs), are a type of malware that allows an attacker to get remote access and control over a device. This gives the attacker the ability to steal sensitive information and modify the device.

Malware known as cryptojacking takes use of the device's processing power to mine bitcoin. This type of malware significantly reduces the device's performance and consumes important resources.



<https://ifflab.org/wp-content/uploads/2020/01/Types-of-Malware-IFF.jpg>

## HOW DOES ANDROID MALWARE SPREAD?

Android malware can spread in a number of different methods, each of which poses a distinct risk to the confidentiality and safety of the device. The following are some of the most often-used methods:

**Downloading Malicious Apps**: The downloading of malicious apps is one of the most prevalent methods that malicious software can propagate on Android devices. Fake applications that are intended to fool users into downloading them can be manufactured by adversaries, who then either distribute them through social engineering methods like phishing or publish them to third-party app stores. After being installed, the malicious app has the potential to infect the smartphone with malware, which can then either steal private information or cause the device to malfunction.

**Visits to Harmful Websites**: Malware for Android can also propagate when users navigate to websites that include malicious code. Simply going to one of these websites can infect the user's device with malware if it contains any of the aforementioned threats. They are also able to deceive the user into downloading a malicious application or installing malware by presenting them with an infected advertisement or download link.

**Scams That Look Like Phishing**: Scams that look like fishing can be used to spread malware on Android by tricking users into supplying sensitive information like login credentials or financial information. Phishing scams are one type of phishing scam. After obtaining this information, the attacker can utilise it for their own nefarious reasons or spread malware onto the device.

**Attachments to Emails**: Malware can also be distributed by infected files or URLs that are attached to emails and sent to recipients. An adversary may craft phoney emails that give the impression of coming from a reliable source in order to deceive users into installing malicious software on their devices by having them open an attached file or clicking on a link in the email.

**Drive-by Downloads**: Another method for disseminating Android malware is through the use of drive-by downloads. It happens when the user accesses a website that has malware, which instantly infects the device without the user's knowledge or agreement. These infections are known as drive-by downloads.

**SMS Spam**: Malware that targets Android devices can also spread through the use of the SMS spam technique, in which cybercriminals send text messages with links that, when clicked, download malware to the device.

**Bluetooth**: Bluetooth can also be used to distribute Android malware, as cybercriminals can produce infected files and send them to neighbouring devices using Bluetooth connections. This allows them to infect multiple devices simultaneously.

## HOW TO PROTECT OURSELVES FROM ANDROID MALWARE:

It is essential to adhere to the following best practices if you want to safeguard your Android device from malicious software:

Only Download Apps from the Google Play Store One of the most effective ways to shield an Android device against malicious software is to restrict app installation to the Google Play Store. Because the Google Play Store is equipped with safeguards that can identify and eliminate potentially harmful applications, it is a more reliable place to download software.

Keep the Device and Its Operating System Up to Date Keeping the device and its operating system as up-to-date as possible can help protect against Android malware. A common component of updates is the addition of security patches, which close loopholes that could be exploited by malicious software.

Utilize a Reputable Security Program Installing a security app with a good reputation might provide further protection against malicious software designed for Android. These applications are able to monitor network traffic, scan for harmful applications, and block malicious websites and phishing scams.

**Be Wary of Unknown or Dubious Apps**: You should try to avoid downloading apps from unknown or suspicious sources. Additionally, you should be wary of apps that have a low number of downloads, a poor rating, or unfavorable reviews.

Rooted devices should be avoided at all costs because the process grants hackers more access to the device's operating system, which in turn increases the likelihood that the device will become infected with malware.

**Be Wary of Phishing Scams**: To prevent falling victim to a phishing scam, you should avoid clicking on links or downloading attachments from sites that you are not familiar with. Be extremely cautious when responding to emails or text messages that request personal information or login passwords.

Steer clear of using public Wi-Fi because these networks are frequently insecure and can be exploited by cybercriminals to transmit malware. Stay away from connecting to public Wi-Fi networks and instead use a virtual private network (VPN) to encrypt your access to the internet.

Enable Two-Factor Authentication in order to add an additional layer of protection to crucial accounts, such as financial or email accounts, and enable two-factor authentication for those accounts.

Back-Up Your Data On a Regular Basis Backing up your data on a regular basis will help protect you from malware that deletes or encrypts files. It is possible to safeguard oneself from malware by storing data in a safe location, such as on an external hard drive or through the use of a cloud storage service.

Users can secure their devices, personal data, and privacy by following these recommended practices, which will lower the danger of Android malware infecting their devices and protect their privacy. In addition, users who are knowledgeable of the many forms of Android malware as well as the methods that are used to spread the virus are better able to defend themselves against the threats that they face.

## IMPACT OF ANDROID MALWARE ON ITS USERS:

Malware that infects Android devices can have substantial repercussions for users, which can vary from relatively minor inconveniences to major security vulnerabilities. The following is a list of the more prevalent impacts:

Malware that infects Android devices can take private information such as login credentials, credit card details, and other sensitive data. After that, this information might be put to use for identity theft or some other kind of criminal activity.

Android malware has the potential to add unwanted costs to a user's phone bill by inadvertently subscribing the user to premium services without their knowledge or approval. These charges can be considered unapproved.

Deterioration of performance Malware has the potential to waste a substantial amount of system resources, which will in turn slow down the device and make it more difficult for the user to carry out their duties.

The user's location can be tracked, their contacts can be accessed, and their online activity can be monitored if the user has Android malware on their device, which results in a loss of privacy.

Malware can utilize an infected device to send spam or phishing messages to the user's contacts. This not only helps to spread the malware but also damages the user's reputation.

Malware that infects Android devices can offer the attackers control from a distance over the device that has been infected, enabling them to access and change data, install other malware, or carry out other harmful operations.

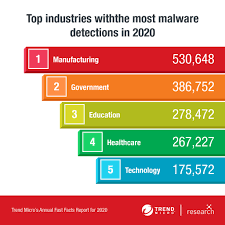
## LATEST STATISTICAL REPORT ON ANDROID MALWARE:

The number of new Android malware variants is expected to increase by 27% in 2020 compared to 2019 when it was estimated that there were over 20 million different Android malware variants. This information comes from a report published by Symantec. Adware was the most prevalent kind of Android malware in the year 2020, accounting for 56% of all malicious software found on Android devices. Trojans and backdoors rounded out the top three forms of Android malware. According to the findings of the report, another big source of dangerous software for Android is third-party app shops. The report indicated that many harmful apps are disseminated through these stores.

(Reference:<https://www.symantec.com/content/dam/symantec/docs/reports/istr-2021-en.pdf>)

According to a report published by Trend Micro, the amount of malicious software targeting Android devices saw a 47% year-over-year growth in 2020, reaching a total of 6.4 million newly discovered Android malware variants. According to the findings of the survey, the countries most impacted by malware on Android devices are India, the United States of America, and Brazil.

(Reference:<https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/trend-micros-mobile-threat-report-for-2020>)



<https://encrypted-tbn0.gstatic.com/images?q=tbn:ANd9GcQMbnqPwERaFrsbdyLN8ZESs98_sN5NGtMjAQ&usqp=CAU>

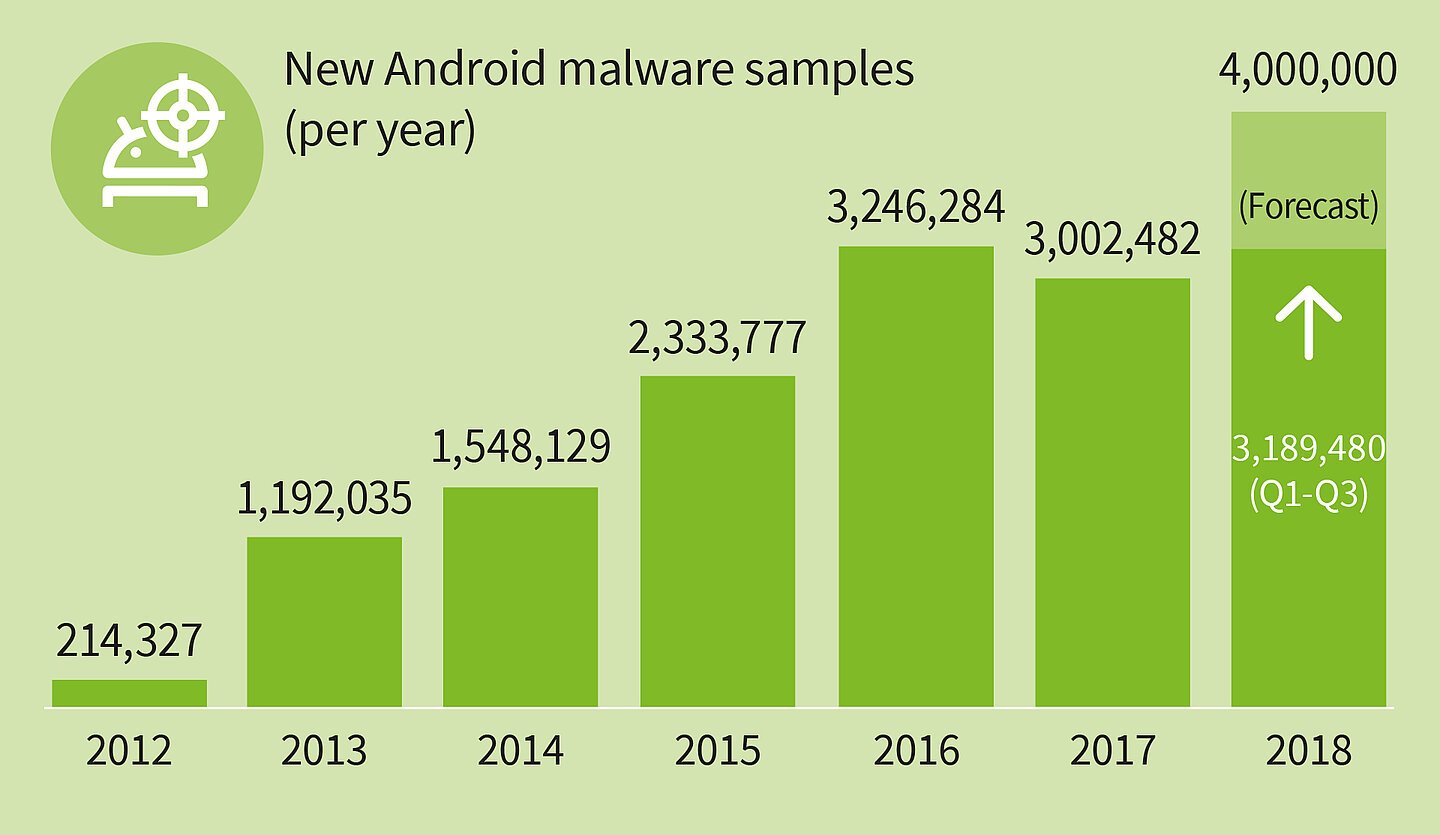
According to the findings of a study conducted by Kaspersky, the percentage of Android users who were infected with malicious software that targeted their mobile banking accounts rose by thirty percent between 2019 and 2020. In addition, the survey discovered that Russia, India, and Brazil were the top three countries where mobile banking malware was most prevalent. (Reference:https://securelist.com/mobile-malware-evolution-2020/101552/)

According to the findings of a study conducted by the University of Cambridge, a malicious software designed for Android devices is becoming increasingly complex and evasive. Attackers are employing methods such as code obfuscation and dynamic analysis evasion in order to avoid being discovered. According to the findings of the study, third-party app shops are also a key source of harmful software for Android devices. The study indicated that many malicious apps are disseminated through these stores.

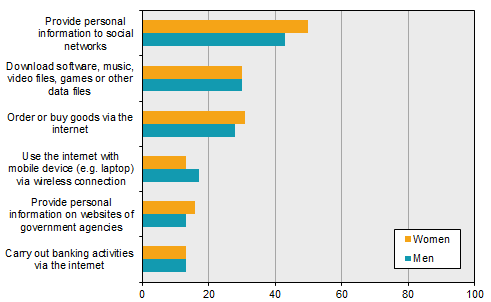
(Reference:<https://www.cam.ac.uk/research/news/android-malware-becomes-more-sophisticated-and-evasive>)

According to the findings of the Report on Research Conducted by Check Point, the amount of malicious software designed to target Android devices increased by 11% in 2020 compared to 2019. According to the findings of the study, trojans make up 59% of all Android malware that was discovered. This percentage accounts for the fact that trojans are the most prevalent form of Android malware. According to the findings of the survey, the most impacted countries by malware on Android devices were India, Russia, and the United States of America.

(Reference: <https://research.checkpoint.com/2020/2020-mobile-malware-report/>)



<https://www.gdatasoftware.com/fileadmin/_processed_/a/1/G_DATA_Infographic_MMWR_2019_Q3_New-Malware-Samples-Years_EN_a0eb4eca09.jpg>



<https://www.scb.se/contentassets/bae555ab532a430a9550c5172b6dcb47/di_en.png>

## FUTURE TRENDS OF ANDROID MALWARE

There are a number of factors that are likely to have an impact on the future of Android malware. These factors include the continued expansion of the Android operating system, the progression of technology, and the measures taken by the technology industry, governments, and users to prevent and respond to threats posed by malicious software. The following is a list of some of the trends that are expected to affect the future of malicious software for Android:

As the level of expertise of those who launch attacks rises, it is possible that they will come up with new and more efficient techniques for distributing malware to Android devices. This may include the use of social engineering techniques to fool users into installing apps that contain malware, or the exploitation of vulnerabilities in the Android operating system or other components of the device. Both of these methods can be used to install malware.

Assaults that are more specifically targeted It is probable that in the future, attackers will place a greater emphasis on launching attacks that are specifically meant to steal sensitive information from certain persons or organizations. This could involve the use of malware that is specifically designed to target certain devices or operating systems, or it could involve the use of social engineering techniques to deceive people into installing apps that are infected with malware.

As technology advances, cybercriminals are likely to find new entry points via which they might infect Android devices with malware. This could involve taking advantage of security flaws in Internet of Things (IoT) devices that are connected to Android devices, or it could involve utilizing cloud-based services in order to store and transmit malware.

Larger emphasis on security It is expected that the technology sector, governments, and users will place a greater emphasis on security in response to the growing threat posed by Android malware. This is because Android malware is becoming more sophisticated. This could involve the creation of new operating systems that are more secure, the deployment of software that can detect and remove malware, and an increased understanding of the risks that are posed by malware.

In the future, it is expected that the technology industry and the government will collaborate to avoid and respond to dangers posed by malware. This will be possible because of the likely increased level of collaboration between the two. This may include the exchange of information and specialized knowledge, the establishment of coordinated responses to outbreaks of malware, and the construction of legislative frameworks that promote the use of secure software development methods.

These are only a handful of the developments that are expected to have a significant impact on the future of malicious software for Android. Even though it is impossible to predict the future with absolute certainty, it is abundantly clear that malware will continue to pose a significant threat to the security of Android devices. Additionally, it is clear that the technology industry, governments, and users must collaborate in order to prevent and respond to these threats.

## STEPS TAKEN BY THE GOVERNMENT TO TACKLE ANDROID MALWARE:

The governments of several countries are taking measures to safeguard their citizens from the negative effects of Android malware and to reduce the risk that it poses. The following are some of the measures that are now being taken:

Regulation: Governments are currently in the process of enacting rules and regulations that require businesses to take preventative measures against malware attacks and to implement security protocols.

Education: Governments are initiating awareness efforts to educate the public about the dangers of malware for Android devices. This includes offering advice on how to recognize and avoid downloading harmful applications, how to maintain software up to date, and how to use anti-malware software properly.

Cooperation with industry: Governments throughout the world are collaborating with the technology industry to devise and put into practice security measures that will lower the likelihood of being infected by malicious software (malware). This involves encouraging the use of safe software development processes and working with app stores and other distribution channels to screen for and remove dangerous apps. Additionally, this includes promoting the use of secure software development techniques.

Law enforcement: Governments are employing their law enforcement agencies to track down and prosecute individuals and organizations responsible for generating and distributing Android malware. These individuals and groups are being tracked down using Android malware.

Research and development: Governments are investing in research and development to develop new technologies and techniques for detecting and removing malware, as well as to identify new vulnerabilities that malware can exploit. In addition, these governments are conducting research and development to find new vulnerabilities that malware can exploit.

## FEW EXAMPLES OF ACTIONS TAKEN BY GOVERNMENTS ACROSS THE GLOBE:

Some examples of efforts that have been made by governments include the following:

The Federal Trade Commission (FTC) in the United States has adopted a variety of precautionary measures to reduce the possibility of malicious software being installed on Android devices. The Federal Trade Commission (FTC) has initiated a number of enforcement cases against businesses that have failed to install proper security measures, and it has provided the public with instructions on how to protect themselves from malware infestations.

The European Union Agency for Cybersecurity, also known as ENISA, is in charge of promoting and improving cybersecurity throughout the EU. ENISA collaborates with governments, businesses, and other stakeholders to develop and implement methods to prevent and respond to cyber threats, including Android malware. These steps include preventing the spread of malicious software.

The Indian government has taken a number of measures to control the risk of Android malware. These measures include launching awareness campaigns, collaborating with the technology industry to promote secure software development practices, and using law enforcement agencies to track down and prosecute individuals responsible for distributing malware.

The Australian government has launched several initiatives with the goal of reducing the risk of Android malware. These initiatives include working with the industry to develop secure software development practices, promoting the use of anti-malware software, and launching awareness campaigns to educate the public about the dangers of malware.

These are measures that governments all around the world are taking to control the risk posed by malicious software for Android devices. The particular steps that are taken may differ from nation to country and depend on the nature of the threat; nonetheless, the end goal remains the same: to safeguard citizens from the effects of malware and to ensure that the online environment is safe and reliable.

## TITLE SUGGESTIONS:

1. The Rise of Android Malware: Understanding its Evolution and Impact
2. From Simple Threats to Complex Attacks: The Transformation of Android Malware
3. How Android Malware Has Evolved Over the Years: A Comprehensive Study
4. The Growing Threat of Android Malware: Tracing its Evolution and Progress
5. The Changing Landscape of Android Malware: A Look at its Evolution and Advancements

## REFERENCES:

* Symantec. (n.d.). Mobile Threats: A Look Back. Retrieved from <https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/mobile-threats-a-look-back.pdf>
* McAfee. (n.d.). Mobile Threat Report: Second Quarter, 2010. Retrieved from <https://www.mcafee.com/enterprise/en-us/assets/reports/rp-mobile-threats-q2-2010.pdf>
* F-Secure. (n.d.). Mobile Threat Report: Q3 2010. Retrieved from <https://www.f-secure.com/documents/996508/1030738/Mobile_Threat_Report_Q3_2010.pdf>
* McAfee. (n.d.). Mobile Threat Report: Second Quarter, 2012. Retrieved from <https://www.mcafee.com/enterprise/en-us/assets/reports/rp-mobile-threats-q2-2012.pdf>
* Trend Micro. (n.d.). Mobile Threat Report: Q2 2012. Retrieved from <https://www.trendmicro.com/vinfo/us/security/research-and-analysis/threat-reports/roundup/mobile-threat-report-q2-2012>

<https://www.imperva.com/learn/application-security/penetration-testing/>

<https://www.synopsys.com/glossary/what-is-penetration-testing.html>

<https://www.contrastsecurity.com/glossary/penetration-testing>

<https://www.softwaretestinghelp.com/penetration-testing-guide/>