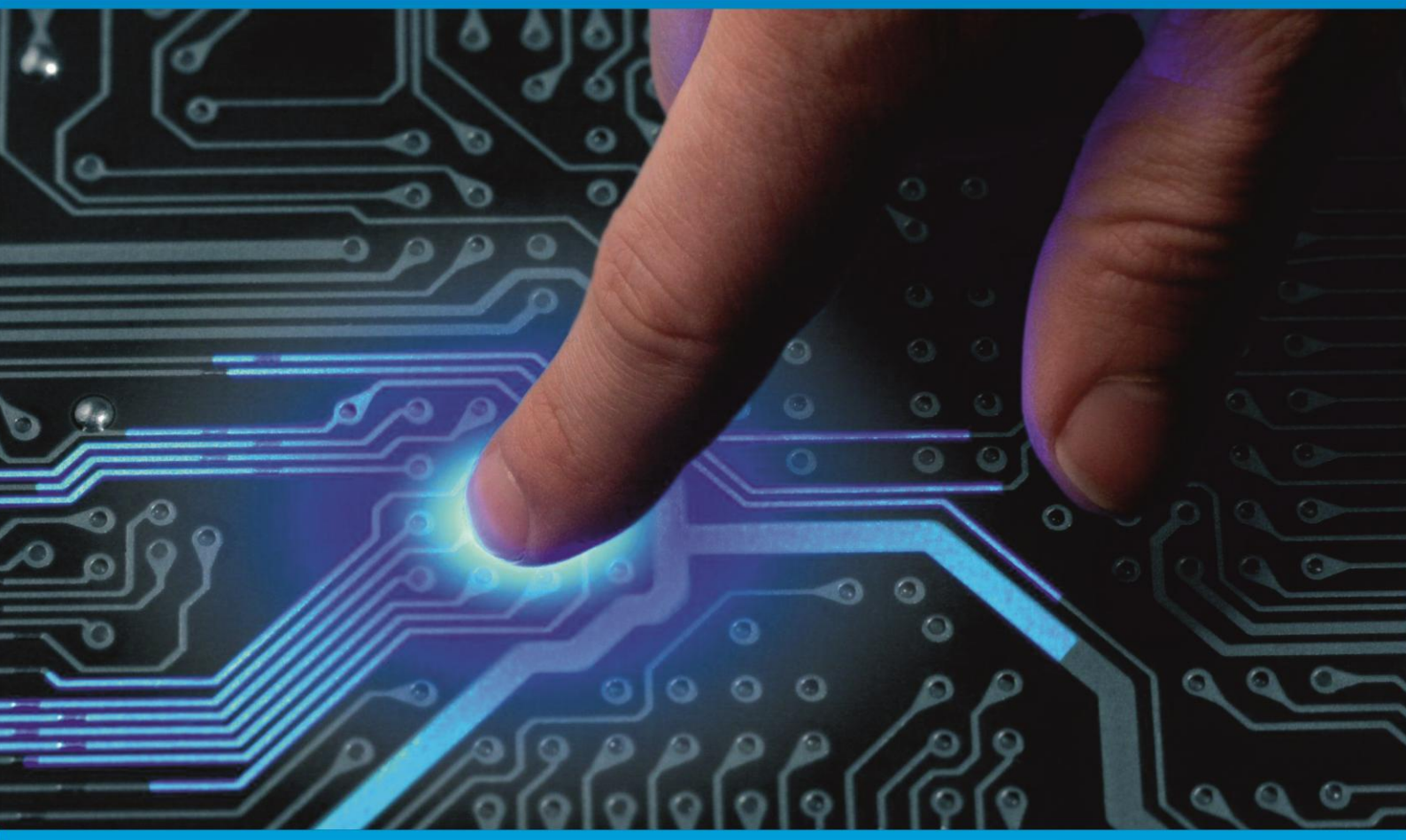
IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798



INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 9, Issue 5, May 2021

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 7.488

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.488 |

|| Volume 9, Issue 5, May 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0905033 |

A Novel Review on Prevention Methods for Malware Attacks Based on Android Devices

Nikhil Soni[1] , Raj Gandhi[2] , Vivek Shaji [3], Prof. Rajeshwari Gundla [4]

Student, School of Engineering, Ajeenkya D Y Patil University, Pune, Maharashtra, India [1,2,3]

Assistant Professor, School of Engineering, Ajeenkya D Y Patil University, Pune, Maharashtra, India [4]

ABSTRACT: This paper explores about the android malware attacks, its types and attacks. There are infinite sources out there. Malware attacks can come from anywhere throughout the system. This research paper gives you information about the malware attacks and its types and how to prevent and save your data from his attacks. These attacks can penetrate and steal the data and access every android device like phones, printers, monitors and cameras of laptops. This paper also gives information about prevention methods, high risk permission, android antivirus, cons of malware attacks and its future scope. This paper also discusses about the risk and danger about the malware attacks. This paper also discussed in brief in this topic. More about the malware and android attacks in all types of android devices in the daily life.

KEYWORDS: Types of malwares, Goal of malware attacks, Prevention methods, High-risk permissions, Cons of malware, Android antivirus.

I. INTRODUCTION

Android malware is malicious software that targets android phones, by causing the collapse of the system and loss or leakage of confidential information.it has become increasingly difficult to ensure their safety and security against android attacks in the form of viruses or other malware. The evolution of mobile devices has certainly improved our lives, but yet, security threats are rising. Although malware can affect any mobile operating system (OS), in this article I'm going to look at Android malware specifically, since Android is the most targeted OS. Actually, you may have already read a bunch of headlines around Android malware attacks. Long gone are the days when cyber criminals were only targeting computers. Now, they are likely to infect any piece of tech equipment you can imagine, starting from smart home ecosystems, to self-driving cars, drones, and AR/VR devices. And of course, your Android device is no exception. Malware is any software intentionally designed to cause damage to a computer, server, client, or computer network.A wide variety of malware types exist, including computer viruses, worms, Trojan horses, ransomware, spyware, adware, rogue software, wiper and scareware [1].

Android smartphones were not being targeted by malware since their popularity was growing gradually and attackers were mainly focusing on other widespread mobile operating systems of the time, such as Symbian. But as soon as its user base started developing more and more, by 2010, the platform was becoming a suitable environment for malware infections [1].

II. LITERATURE SURVEY

Android security Architecture

Let's scrutinize the Android OS Security in a bit of depth. Android is a privilege-separated operating system. Each app runs through a unique Linux user ID. Linux helps in isolating applications from each other.And, through additional permission mechanisms, restrictions are enforced on particular operations which may steal data from the device. Speaking in terms of layman language, the central architecture of Android security ensures that no application has permission to impact other applications, the operating system or the user (which includes the user's private data such as contacts & e-mails). They also cannot access the network or keep the device awake without prior consent [6].

A very important anf compulsory file present in every Android App is "AndroidManifest.xml". Let's have a look at what this manifest file does (from the security point of view):

- It primarily describes the application's activities, services and broadcast receivers.
- Some declarations in it let the Android OS know what components the app has and when there is a need to launch them.
- It declares which permissions the application needs for accessing the protected parts.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.488 |

|| Volume 9, Issue 5, May 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0905033 |

-It also declares the permissions that other apps require to have in order to interact with the application's components.
The xml file in the app requires <user-permission> tags for making use of protected features on the device. When installing an application, the user is requested by the application package installer to grant permission(s). But, before or while running the application, it is never checked again by the user. If the permission was granted, the app can then use the desired features without prompting the user [6].
Moreover, another feature for all the .apk Android Applications is the signing of a certificate. The developer is identified by this signature and the private key is also held by him only. The purpose of this certificate is to distinguish the authors and allow the system to grant or deny signature-level permissions [6].
Thankfully, there have been significant security enhancements in the latest development of Android – Gingerbread 2.3. It's said to prevent clickjacking attacks from cyber criminals. Clickjacking is basically an attack which tricks user into clicking rogue links disguised as legitimate page features. The Gingerbread platform is built with a touch filtering mechanism called "FilterTouchesWhenObscured" for the prevention from these types of attacks. This will alert users when their devices are obscuring or concealing sensitive functionality[6].
This was coders insight into the security design of our beloved Android OS. Now, it's time to have a look at the loophole's friends! And, obviously in this competitive world, we are bound to compare the rivals. So, in our next post we will present the iOS Security design. And, we will also point out the gaps in Android OS by comparison[7].

II. TYPES OF MALWARES

The list of malware types (or the range of cybersecurity threats in general) is growing every day. As recently as July 2020, reports emerged about a new variant called "shadow attack," which forges key documents. In this type of security attack, threat actors can alter the contents of a digitally signed PDF document and lull users into a sense of security. Let's look at the different types of malware[2][3].

1. Ransomware
Ransomware blocks a user's access into a system or data file and refuses to open it until payment in the form of a ransom is made by the user or organization where the user is employed. It might block a computer's sign-on screen, or go to the extent of encrypting large volumes of important information and hold it "hostage." The WannaCry ransomware attack of 2017 brought this particular malware type to the forefront of global conversations [2].

2. Virus
While the terms "virus" and "malware" are often used interchangeably, a virus is actually a highly specific type of malware. A virus refers to any application that alters the code or structure of a target file or software. Like a biological virus, it attaches itself to a legitimate software (called the host) and slowly disarms its functionality [2].

3. Trojans
Like the Trojan horse from Homer's Odyssey, a computer Trojan is a malware masquerading as a legitimate app. This type of malware has become surprisingly popular over the last few years owing to the rising online traffic and interest in downloading applications (safe or otherwise). In Q1 of 2019 alone, Kaspersky detected over 29,000 installation packages for mobile banking Trojans [2].

4. Adware
Adware is among the most common malware types. Its goal is to route a user to an unwanted piece of advertising, hoping to gain some revenues. Adware often comes bundled with legitimate software programs that are downloadable off the internet. A stealthier variant would be an adware that directs you to a familiar-looking website (e.g., an Amazon shopping window) but contains a series of unwanted ads [2].

5. Worm
Just as the name suggests, worm refers to a self-replicating type of malware, which quickly spreads across your system and to other computers via a connected network. Unlike a virus that needs someone to use the host application, a worm has very little dependence on human action. This makes it more effective and dangerous than a typical virus. Worm attacks usually work in the background, slowly spread across the network, and make its presence felt only when it's too late [3].
6. Mobile malware
Mobile malware is different in structure, as it targets a different operating environment. For example, banking Trojans are a common malware type for mobile phones, as users are likely to trust a bank provider without conducting due

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.488 |

|| Volume 9, Issue 5, May 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0905033 |

diligence. A new mobile malware called LeifAccess was discovered last year. This malware installs itself on your smartphone, creates multiple accounts, downloads apps, and posts reviews, turning your smartphone into a review farm [3].

7. Spyware
Spyware comes in different shapes and sizes. Some spyware falls into the category of keyloggers, which monitor your keystrokes to gather sensitive intel like passwords, pin numbers, proprietary information, etc. Others can take over computer peripherals like a webcam to record videos of the user's surroundings or listen-in using the mic. Some spyware can record your browsing history and online behavior to push more targeted adware [3].

8. Malicious bots
A bot is a highly flexible type of malware that can auto-execute commands at a certain date or time. They are also called botnets, and interestingly, they aren't always malicious in nature. In the computing world, bots perform several legitimate activities, such as automatically indexing websites for search engine results. However, a threat actor could use this in a malicious way. For example, it could install the same bot in thousands of systems and program them to log into a specific website at the same time. This floods the website beyond capacity, ultimately crashing it. Bots can turn a computer system into an attack accessory, not necessarily the target [3].

9. Rootkit
A rootkit is designed to give a remote threat actor unauthorized access to privileged systems/restricted software. Typically, a rootkit doesn't work as a standalone malware. Instead, it enters your system as a suite of different tools, including keyloggers, spyware, bots, etc., all working towards a single goal [3].

10. Malvertising
Often, a legitimate ad platform is used to direct users to a fraudulent/malicious website. Let's say that you have downloaded a new, freely available PDF reader. If the app is ad-sponsored, there is a good chance that you will see unverified and untargeted advertising content. Clicking on these will lead you to a harmful website, where any activity will further expose your system[3].

III. PREVENTION METHODS

Android has the biggest smartphone market share in the world in 2020. 85.4% of smartphone users have an Android device, with only 14.6% falling to iOS. As a result, malware designed for Android will have a wide reach, necessitating appropriate defense mechanisms. Here are the steps to remove malware on Android:

Look out for signs of infection
It's relatively easy to understand if malware has entered an Android phone – the battery will deplete faster than usual, RAM will be occupied despite no apps being open, data usage shoots up, and carrier bills could also rise. If you spot any of these symptoms, don't put them on the backburner [4].

Download Google Play Protect
Recognizing the growing threat of Android malware, Google has come out with a dedicated app to tackle the problem. Simply open the Play Store on your smartphone or tablet, and run a device status check. Google Play Protect comes built-in with your Android device and is turned on by default. This is an easy way to check for and remove Android malware [8].

Use your smartphone in safe mode
Just like a Windows PC, Android systems also come with a safe – or emergency – mode. To turn it on, press the power button (or the power icon on the top of your notifications screen) until you see the Power Off and Restart options. The emergency mode is turned off by default – you can switch it on after accepting the terms and conditions. Using a smartphone in safe mode prevents the malware from causing any further damage [9].

Report suspicious app activity
Unlike iOS, Android doesn't prevent users from downloading apps from outside the Play Store. It offers a useful feature that lets you report any suspicious apps you might have downloaded to Google. Activate this from the Play

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.488 |

|| Volume 9, Issue 5, May 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0905033 |

Store – Go to Play Protect on the left menu, open the Settings menu on the top right, and turn the "Improve harmful app detection" toggle on [9].

Top permissions asked by malware:

- Internet
- Access network state
- Read/write external storage
- Read phone state
- Access WIFI state
- Access location
- Read/write contacts
- Camera access
- Microphone access

Hackers are taking advantage of a flaw in the OS that can trick you into giving up access to your phone. A vulnerability that can exploit the permission pop-up windows on Android. Ironically, the permission pop-ups are meant to be a safety feature; if an app wants access to your phone's SMS messages, camera or contacts, it first needs to get your approval. The feature is a handy tool to prevent apps from automatically accessing any sensitive data or functions on your phone. Unfortunately, the same safeguard has a flaw. The security firm Promon has uncovered hackers using malicious Android software to overlay fake permission pop-ups on top of legitimate ones[10].

An attacker can ask for access to any permission, including SMS, photos, microphone, and GPS, allowing them to read messages, view photos, eavesdrop, and track the victim's movements, Promon said in the company's report. "The attack can be designed to request permissions which would be natural for different targeted apps to request, in turn lowering suspicion from victims [10].

The same flaw can hijack the permission pop-up for any Android app. In addition, it can also overlay look-alike login windows on top of a social media or banking app to dupe you into handing over your passwords[11].
The vulnerability exists thanks to multitasking system in Android called "task Affinity," which can inadvertently let a malicious app assume the identity of another app on board the OS, Promon said. The security firm uncovered the threat after customers of several banks in the Czech Republic reported their money mysteriously disappearing from their accounts. A company partner then supplied Promon with a live sample of the Android malware that exploited the flaw [11].

To deliver the attack, the hackers have been secretly using "dropper apps" and "hostile downloaders" over the Google Play Store. These apps can be harmless at first, but will secretly download the Strandhogg-based malware to the vicitm's phone at a later time[12].

In response to the threat, Google said it's removed the harmful apps from the Play Store. The company's built-in malware protection software for Android, Google Play Protect, has also been updated to block apps from using the Strandhogg attack. "Additionally, we're continuing to investigate in order to improve Google Play Protect's ability to protect users against similar issues," a company spokesperson added [12].

Nevertheless, Promon claims Google hasn't patched the Android OS itself from the Strandhogg attack. In total, 36 malicious apps —some sourced back to 2017— have been found using the vulnerability, according to Promon's partner on the investigation, Lookout. Oddly, none of the companies involved named which apps were affected, making it unclear the scale of the threat[13].

So how can you protect yourself? The attack comes from malicious apps. So, it's best to avoid third-party app stores outside of Google Play and to refrain from downloading apps from little-known developers [13].

Promon also advises users to be on guard against apps requesting permissions they don't need. For example, a calculator app asking for GPS permission. If you suspect something shady is occuring, uninstall the app immediately[14].

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.488 |

|| Volume 9, Issue 5, May 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0905033 |

IV. GOOD APPS DON'T REQUEST 'RISKY' PERMISSIONS, RIGHT?

There are millions of apps available to users, and while some are in fact 'safe' and treating your personal data with the utmost care, the vast majority are not. This includes apps that make App Stores. While seemingly harmless, these apps can easily be compromised. This can be done either by developers themselves, or by malicious third parties through vulnerabilities the app's code.
That's why it's so important to pay attention to the permissions you're granting apps (and not just to those apps you would consider to be risky). Regardless of where you find them or how innocent you.
As a consumer or a business enabling your employees with corporate mobile devices, you must be proactive and monitor app permissions before they become problematic[16].

V. WHAT ARE APP PERMISSIONS?

Have you ever asked yourself, 'what are app permissions?' Chances are you have when different mobile apps ask to "access your personal info" or something similar. It's vital to understand exactly what app permissions are, when you are notified of them, how you can manage them, and what app permissions to avoid.App permissions determine what exactly the app you are attempting to download has access to on your device [32].

For the purposes of this article, we will be focusing on Android app permissions. The most important thing to understand about these app permissions is that they aren't optional. Unless you make the choice not to download the app, the SDK will receive all of the permissions it requires once it is installed on your device[32].

In the process of installing an app from the Google Play Store, for example, you will receive a popup on your screen of all the permissions the app will require. It's becoming increasingly important that you both read through and understand these permissions to know exactly what the app will have access to [17].

As a business, it's very difficult to monitor every single permission every app on every device within your mobile estate has access to. In fact, it's nearly impossible unless you have full visibility into mobile device traffic[17].

VI. OTHER HIGH-RISK PERMISSIONS REQUESTED

There are others, not as frequently requested permissions that are essential to keep in mind as a user or a business. Here at Wandera, we consider them to be both highly risky and oftentimes unnecessary to the app's purpose [31].

Name: android.permission.CALL_PHONE
Title: "Directly call phone numbers"
Description: Allows the app to call phone numbers without your intervention. This may result in unexpected charges. Note that this doesn't allow the app to call emergency numbers [31].
% of apps: 9%

Name: android.permission.RECEIVE_SMS
Title: "Receive text messages"
Description: Allows the app to receive and process SMS messages. This means the app could monitor or delete messages sent to your device without showing them to you [31].
% of apps: 5%

Name: android.permission.WRITE_CONTACTS
Title: "Modify your contacts"
Description: Allows the app to modify the data about your contacts stored on your phone, including the frequency with which you've called, emailed, or communicated in other ways with them. This permission allows apps to delete contact data[31].
% of apps: 5%

Name: android.permission.READ_SMS
Title: "Read your text messages"

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.488 |

|| Volume 9, Issue 5, May 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0905033 |

Description: Allows the app to read SMS messages stored on your phone or SIM card. This allows the app to read all messages, regardless of content or confidentiality [31].
% of apps: 5%

Name: android.permission.READ_CALENDAR
Title: "Read calendar events"
Description: Allows the app to read all calendar events stored on your phone, including those of friends or co-workers. This may allow the app to share or save your calendar data, regardless of confidentiality or sensitivity[18].
% of apps: 4%

Name: android.permission.SEND_SMS
Title: "Send SMS messages"
Description: Allows the app to send SMS messages. This may result in unexpected charges. Malicious apps may cost you money by sending messages without your confirmation [18].
% of apps: 4%

VII. ANDROID ANTIVIRUS

There are dozens of free antivirus apps available on Google Play today. However, in order to get optimum Android security, what you need is the best free antivirus app for Android. By downloading one, you'll get a top-quality Android virus scanner that doesn't break the bank [19].

-Here are some qualities of the best free antivirus apps for Android:
-High-standard Android virus scan feature
For obvious reasons, the best free antivirus for android is one that gives you access to an actually efficient Android virus scanner. Android security must be on 24/7; it is crucial that your free android antivirus must provide your phone with always-on protection[19].

Through this feature, you will be able to detect infectious malware and other security risks threatening your Android phone. After every Android virus scan, the app will direct you to initiate a virus removal process. This guarantees that every potential threat will be removed from your Android phone [19].

The best free antivirus apps for Android also allow you to schedule recurring Android virus scans. By enabling such function, the free antivirus app will scan your entire phone on a regular basis. This further assures that your Android phone will remain virus-free[30].

User-friendly interface
The best free antivirus apps for Android are the ones that offer easy usability. A high-grade Android virus scanner is not going to be useful if you don't know how to use it properly [30].
With an easy-to-use interface, you will be able to easily familiarize how to use and control your free antivirus app. This will allow you to access its Android virus scanner easily, and perform every security function with no hassle [30].
A user-friendly interface is also one determining factor of a free antivirus app's efficiency. With a user interface that you can understand and navigate easily, you can quickly initiate Android virus scans regularly, or when necessary. This allows you to maximize the usage of the best free antivirus for Android[20].

Additional Android security features
To provide better Android security, the best free antivirus apps for Android offer additional security functions other than just a reliable Android virus scan feature. These additional functionalities guarantee all-around Android protection [20].

Comodo antivirus
An Android virus scanner can help detect and neutralize mobile malware. But if you want to guarantee that your Android phone will be able to block mobile malware, you need complementary security functions. Some of these functions are safe browsing features and Android VPN [20].

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.488 |

|| Volume 9, Issue 5, May 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0905033 |

One virus removal app you can use is Comodo Free Antivirus for Android. It is one of the leading antivirus applications for Android phones. Comodo Free Antivirus for Android gives you access to a high-grade Android virus scanner that protects your phone against viruses, unsafe apps, potentially risky settings[29].

How to remove a virus from an Android phone?

Removing a virus from an Android phone doesn't really require installing an antivirus app. There is actually a way that you can try to manually remove Android viruses. However, doing this requires effort and high-technical knowledge. This is not a convenient choice, especially to less tech-savvy Android users. Installing a free antivirus app from the Google Play Store is a way better option [29].

As mentioned before, there are many free antivirus apps for Android available. Downloading one will give you access to fast and efficient virus removal [21].

After successfully downloading a free antivirus, you can now get complete access to its Android virus scanner. What you need to do is to tap the "scan" button and the app will then search your phone for malware and other security risks [21].

After the Android virus scan is completed, it will display all the detected security risks on your phone. Your free antivirus app will then ask you to perform necessary steps in order to resolve any risks that was detected by the scan[28].

If you want to know how to tell if your Android phone was infected by a virus, we listed some common signs:

-Your phone's battery drains faster.

-A sudden spike in internet data usage.

-Applications keep on crashing from time to time.

-Unfamiliar apps start to appear on your Android phone

If you have noticed any of these signs, you must download a free antivirus app immediately. This will allow you to confirm your hunch that a virus has infected your Android. A free antivirus enables to immediately address risks before they lead to worse security issues. To ensure top-notch virus protection, you can use Comodo Free Antivirus for Android [28].

To get access to Comodo Free Antivirus for Android, you need to download Comodo Mobile Security. It is a remarkable Android security application that protects your phone against a range of known and unknown Android security risks. By installing Comodo Mobile Security, you can guarantee that your Android phone will remain healthy and virus-free[23].

VIII. CONS OF MALWARE ATTACKS

Visibility is the most important thing when it comes to evaluating the safety of apps and what exactly you're giving up when you hit accept. Sometimes, however, that new app just isn't worth the potential cost.For businesses, however, visibility isn't as easy. You can't monitor every app your employees are downloading every day. That's where Wandera's App Insights feature comes into play.The App Insights report from Wandera presents admins with a 360-degree view of apps installed across the mobile fleet. Not only that, but it also gives a detailed view of the permissions required by each of these apps, which will help you determine which app permissions to avoid. As an admin, this makes easy to evaluate what high-risk permissions exist on what devices and take the necessary action required to ensure mobile app security [6].

Scaring you with a popup message that might tell you that your computer is in danger or other false information[6].

- Reformat the hard drive of your computer…show more content…

If you keep your browser's default security settings it will minimize "drive-by" or bundled downloads.

- Pay attention to your browser's security warnings. Many browsers come with built-in security tool that scans and warn you before you visit an infected webpage or download a malicious file.
- Type the URL of a trusted site directly into your browser, Criminals send emails clicking on them could download malware or send you to a scam site.
- Do not open attachments in emails unless you know who sent it and what it is. Opening the wrong attachment even if it seems to be from your friends, family or work can install malware on your computer without you knowing.
- Download well-known software directly from the source. Sites that offer lots of different kinds of programs like (browsers, PDF readers, and other popular programs) for free are more likely to include malware.

We hope this look into Android app permissions helped to answer what app permissions are. More importantly than what app permissions are, is which you should avoid and which are simply there to enhance your experience using the app[24].

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.488 |

|| Volume 9, Issue 5, May 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0905033 |

IX. FUTURE SCOPE

In the future, the android system will be used in all sorts of devices from Smartphone, TVs to Car navigation system. As the system updates the malware attacks will also be more updated to prevent this the users and android developers will have to strengthen their security and privacy. Number of malware attacks will be more in future that's why it important that we will be careful with our device's privacy[26].

The widespread infection of both computer worms, viruses or Trojan horses spammed to millions are generally no longer considered a serious security threat, and instead, especially for organizations and corporations, targeted Trojan horses have become the highest concern[26].

Vincent Weafer, a senior director at Symantec Security Response, said, "Targeted Trojan horses are still a tiny amount of the overall threat landscape, but it is what the top corporations worry about most." With the aid of carefully placed keyloggers or screen-scraping software, cybercriminals can more easily access specific computers. This method is used primarily in industrial espionage and other financially motivated crimes. Common attacks are more easily detected and halted by most security technology, but targeted attacks such as these can easily remain hidden. This is due to traditional products being unable to recognize the threat [26].

New methods and variants continue to be implemented, allowing these lesser-known and uncommon malware packages to keep their attacks going for a longer period of time, even if this means blatantly attacking the people who are trying to study them. There have been many new and improved attacks discovered in recent reports [26].

There was one piece of malware found during a forensics investigation on a desktop computer. This particular piece of malicious software had actually been pre-coded to steal specific information from the victim's organization. It was also noted as being disposable so that it could vanish without a trace after performing its tasks[25].

In another instance, there was a malware written specifically to steal intellectual property. What was unusual about this malware, however, was that it could crawl different file types (Excel, PDF, etc.) for intellectual property to steal. Then it would encrypt and send the stolen data to a remote server[25].

X. DISCUSSION

In this digital era after computer and internet Smartphone is the third revolution and making ubiquitous computing possible. Android led the smartphone market as most used operating system. This popularity of Android also makes it primary targets of cyber attackers and hackers. There are many different types of cyberattacks targeted towards Andorid environment. In this review paper, we have investigated various attacks reported with respect to Android and have also gathered different type of defenses available to protect users from these attacks[34]. This work is focus on accumulating various literature works available in this domain and provide a comprehensive representation of these works. The various works are grouped into two broad categories i.e., signature and non-signature based, and techniques mentioned in each work is studied and technical observations are made against them which help to understand the usability of these techniques. Such organized and details review work is required to study the problem in depth and works towards solution. The literature works are summarized and organized in proper table which help to visualized and easy comparison the information[35].

XI. CONCLUSION

To summarize the past year, we can say with confidence that it was one of the most critical so far for the evolution of mobile threats. First of all, this was because of the steady growth in the number of malicious programs targeting mobile devices. Second, because malicious users moved to Android as their main targeted platform. Finally, because 2011 was the year in which malicious users essentially automated the production and proliferation of mobile threats. And till the date of 2021 this malware attacks have been increased in big numbers so the solutions should be effective and reliable for long time and also protective for the future attacks of malware upon the system. The updates of devices also have to face the updated malware for the updated system.so conclusion of this topic is to prevent malware from the android devices and minimize and neglect the danger fromthe android system and devices.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.488 |

|| Volume 9, Issue 5, May 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0905033 |

REFERENCES

[1] Android Malware: Your Mobile Device Isn't Safe from Hackers (heimdalsecurity.com)Accessed on 10 April, 2021.
[2] https://heimdalsecurity.com/blog/android-malware/ this blog on Accessed on 10 April, 2021.
[3]https://www.kaspersky.com/resource-center/threats/mobile accesed on Accessed on 10 April, 2021.
[4] Mobile Malware Attacks and Defense - Google BooksAccessed on 10 April, 2021.
[5] Future scopes are from https://www.enigmasoftware.com/the-future-of-malware-beware-of-new-trends-and-attacks/Accessed on 10 April, 2021.
[6] Cons of malware https://www.ipl.org/essay/Advantages-And-Disadvantages-Of-Malware-FJXCACW5SWGAccessed on 10 April, 2021.
[7]android antivirus from https://antivirus.comodo.com/blog/computer-safety/android-virus-/Kozaczynski, J.Q. Ning, and A.Engberts., Program Concept Recognition and Transformation,IEEE Transactions on Software Engineering,18(12), 1992, 1065-1075.
[9] I.D.Baxter.,Design Maintenance Systems. Communications of the ACM,35(4), 1992, 73-89.
[10]P.Tonella and R.Fiutem and G.Antoniol and E.Merlo.,Augmenting Pattern-Based ArchitecturalRecovery with Flow Analysis: Mosaic -A Case Study,Working Conference on RevereEngineering,1996,198-207.
[11]T.Munakata., Knowledgediscovery.Communications of the ACM,42(11), 1999, 26–29.
[12]M.Blaha.,Reverse Engineering of Vendor Databases,Working Conference on androidmalware (WCRE-98), Honolulu, Hawaii, USA, 1998,183–190.
[13]S.R. Tilley.,Coming attractions in program understanding II: Highlights of 1997 and opportunities for 1998.Technical Report CMU/SEI-98-TR-001, Carnegie MelloInstitute, 1998.
[14]R.Clayton, S.Rugaber, and L.Wills.,The knowledge required to understand a program,Proceedings of the 5thWorking Conferece on Reverse Engineering (WCRE-98), Honolulu, Hawaii, USA, 1998,69–78.
[15]J. Singer and T. Lethbridge.,Studying work practices to assist tool design in software engineering,Proceedings of the 6thInternational Workshop on Program Comprehension (WPC- 98), Ischia, Italy, 1998,173–179.[16]. A. Blackwell.,Questionable practices: The use of questionnaire in psychology of programming research,The Psychology of Programming Interest Group Newsletter, 1998.
[16]R. Kazman and S. Carrie,,re.,Playing detective: Reconstructing software architecture fromavailable evidence. Journal of Automated Software Engineering, 6(2),1999,107–138.
[17] Zhang D, Wang J and Yang Y 2014, Design 3D garments for scanned human bodies, Journal of Mechanical Science and Technology, 28 (7) 2479-2487.
[18]K.Wong.,Reverse Engineering Notebook,PhD thesis, Department of Computer Science,University of Victoria, 1999.
[19]B. Boehm.,Software Engineering Economics. (Prentice-Hall, New York,1981).
[20] C. Rich and R.C. Waters., The Programmer's Apprentice. (ACM Press,1990).
[21]H.A. Partsch., Specification and Transformation of Programs: A Formal Approach to Software Development. (Springe, 1990).
[22]J. Nielsen.,Usability Engineering. (Academic Press, New York, 1994).
[23]A. Umar.,Application (Re)Engineering: BuildingWeb-Based Applications and Dealing with Legacies. (Prentice Hall, New York, 1997).
[24]L. Bass, P. Clements, and R. Kazman., Software Architecture in Practice. (Addison-Wesley, 1997).
[25]B. Shneiderman.,: Designing the User Interface: Strategies for Effective Human-Computer Interaction. (Third Edition, Addison-Wesley, 1998).
[26]S. R. Tilley.,The Canonical Activities of Reverse Engineering. (Baltzer Science Publishers, The Netherlands.2000).
[27]Draghici G 1991, Ingineriaintegrata a produselor [Integrated product engineering], Ed. Eurobit, Timisoara, Romania.
[28] Raja V and Fernandes K 2008, Reverse Engineering an Industrial Perspective, Springer Series in Advanced Manufacturing, UK.
[29] Gibson I, Rosen D and Stucker B 2010, Additive Manufacturing Technologies. Rapid Prototyping to Direct Digital Manufacturing, Springer.
[30]Geomagic Available: http://www.geomagic.com/en/products/design/overview. Accessed 12 April 2015.
[31]Rapid Form Available: http://www.rapidform.com/products/xor/overview/ Accessed 12 January 2015.
[32] CATIA Available: http://www.3ds.com/products-services/catia/solutions-by-industry/ Accessed 1May 2015.
[33]Chang K and Chen C 2011, 3D Shape engineering and design parameterization, Computer - Aided Design and Applications. 8(5) 681-692.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.488 |

|| Volume 9, Issue 5, May 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0905033 |

[34]Durupt A, Remy S and Ducellier G 2010, Knowledge based Reverse Engineering – An approach for Reverse Engineering of a mechanical part. ASME Journal of Computing and Information Science in Engineering. 10(4) 044501-1-044501-4.
[35]Durupt A, Remy S and Ducellier G and Eynard B 2008, From a 3D point cloud to an engineering CAD model: a knowledge-product-based approach for reverse engineering. Virtual and Physical Prototyping, 3(2) 51-59.

INNO SPACE

SJIF Scientific Journal Impact Factor

Impact Factor:
7.488

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details