Sri Lanka Institute of Information Technology

MOBILE MALWARE

Individual Assignment

IE2022 - Introduction to Cyber Security

Submitted by: Ekanayake E.M.I.R

Student Registration Number	Student Name
[redacted]	Ekanayake E.M.I.R

Date of submission : 29.04.2020

Table of Contents

ABSTRACT

Mobile Malware is rapidly becoming a major and also a serious threat to the mobile device's user. In this report, I considered a simple review of mobile malware. I have discussed several areas of mobile malware through this report. First in this report includes what is the mobile malware and history of the mobile malware. Mobile malware has an interesting and also important history. Then I considered symptoms of mobile malware and how it install to the devices. After this report considered a simple description of the current state of mobile malware. Then I consider the types of mobile malware and a small description of some modern mobile malware. In this section, I considered how it comes to devices, what happened after infected this malware and how to protect in this malware. The content of the latter part of this report includes the future in mobile malware and prevention methods. Users have many responsibilities to protect their devices from this mobile malware.

Overall, I gave a simple idea of mobile malware in this report.

INTRODUCTION

Nowadays people are using mobile devices for many of the same purposes as desktop computers in the past. Mobile devices also provide many features for users to get easily their work more than desktop computers. Modern days people use social networking, online banking, browsing the internet, access to their private account and also official accounts, playing games, get online information. Mobile devices are the main part of our daily life. With the result of this popularity rapidly increasing malicious activities in these mobile devices because attackers also moving to this mobile section. Hence even rapidly increasing mobile malware the same as mobile devices usage. It's growing serious and also as a huge threat in the cyber world. Mobile malware has various types and also it has various methods to spread among devices. Operating systems of devices are implementing. So attackers also develop their malware program against this sophisticated operating system. As much as the operating systems are improving, mobile malware are also improving and goes to the users' devices. Hence mobile malware gets much attention in society.

Malicious software especially targets mobile devices, simply it's known as mobile malware. Users of mobile malware doing various irrelevant activities or visit the suspicious web site, link and open suspicious email, text and doing various kinds of activities. These activities are a great opportunity for hackers to launch their malware. If some malware installed to the devices, it maybe trouble users' data and information as well as the device. Because of most of the mobile malware target is users' data. When installed malware to the devices, hackers can get access devices and also they can steal, modify or damage users' data and information.

Today's era moving to mobile devices from desktop. Because mobile devices can bring wherever users go. Also, mobile devices grow each year with sophisticated technologies and methods that

not only store data but also some private information such as GPS, camera and password. Therefore mobile devices create a good platform for mobile malware. So these mobile devices bring with them a risk of some attack from mobile malware. Not only users but also hackers are moved to this mobile section because they want to spread their malware among the most famous section and then they can to steal, modify or whatever to a lot of data and information. Mobile malware were initially demonstrated by Brazilian software engineer Marcos Velasco. Old mobile malware were not very harmful malware but today malware are harmful and also dangerous.

What is mobile malware?

Today Mobile devices such as mobile phones, tablets, laptops are playing a major role in our society because most people are used to store their sensitive data on their mobile devices and also many people doing their work with their mobile devices. So today society wants to consider Mobile Security. Most of our sensitive data are stored in our mobile devices. Why we want to consider mobile security, what is the effect of it, how it's working, what are the types likewise so many points have to consider when we are talking about mobile security.

Attackers usually try to exploit their attack through the vulnerabilities and steal our sensitive data, modify our data and doing various illegal things. So many people work with mobile devices but they do not consider or do not know about security. Hence attackers use this chance and they launch their attacks on our mobile devices. Attackers are using various malware to exploit their attacks on our devices.

So what is MOBILE MALWARE?

"Mobile malware is malicious software that targets mobile phones or wireless-enabled Personal digital assistants (PDA), by causing the collapse of the system and loss or leakage of confidential information." [1]

The above definition gives a very simple idea of what is mobile malware. Mobile malware is malicious software specially designed to attack our mobile devices such as smartphones, laptops, tablets. It is grabbing opportunities at the moment and playing a major role and also a great threat to mobile devices. With more people and more companies than ever before work with mobile devices, criminals are also have spotted the great opportunity to exploit this for their work. Mobile malware can result in providing mechanisms for attackers to gain access to the system, loss of our sensitive data and also sometimes loss of our money in the illegal transaction. Mobile malware is the main cause to break down our mobile security. Mobile malware has many types. It is not only one cause but also it has various types. Attackers try to gain control or steal our

data or modify our data through this mobile malware hence mobile malware is an emerging topic in the cyber world at the moment. The most common malware attacks are

- Viruses
- Worms
- Mobile bots
- Mobile phishing attack
- Ransomware
- Trojans

But some mobile malware combines more than one type of attack. Developers of this mobile malware known as cybercriminals.

HISTORY OF MOBILE MALWARE

Mobile devices, bring with them many risks of attacks from malware that continues to increase each year. One of the research by Symantec represents in 2017, new mobile malware increased by 54 percent an average of 24,000 malicious mobile applications were blocked every single day. So this mobile malware had to begin somewhere. Now let's see where and how was the birth of this mobile malware.

Mobile malware was initially created by a Brazilian software engineer who is known as Marcos Velasco. Why he was created first mobile malware because of informed and educated this public threat.

In June 2004, cybercriminals were sent very first mobile malware. It's known as **Cabir**. It's a worm. The vendor of this very first mobile malware is the Symbian operating system which was the operating system used on mobile phones at that time. This malware was created by a group of hackers known as 29A. Cabir was harmless mobile malware relatively today's mobile malware. It drains the battery power of the mobile device. The main goal of this malware was to spread to the Bluetooth enabled devices. The first version of Cabir was not much considering a threat.but later versions of Cabir able to attack our mobile devices. So this Cabir showed to the world, Mobile malware can launch great issues for our mobile devices and also it should be taken seriously. Cabir is the very first mobile malware in the world and now improving and more in advanced malware comes to our mobile devices.

There are some more mobile malware used in the past too.

- ✓ **Mosquitos**

  "Mosquitos" is the world's first mobile Trojan. It is a harmless mobile phone game. This game work as a legal game but the difference is it has some malicious code. Send numerous SMS messages when the game was played**.**

- ✓ **Skuller**

  The Skuller was one of the well known mobile malware in history. An affected after this malware on to the devices it replaced icons with a skull and crossbones logo. This malware was designed to damage usage. Also, overwrite the application files and making the phone unusable. This Skuller malware also used code from Cabir which is the first mobile malware.

- ✓ **Comm Warrior**

  The Comm Warrior is a worm type of malware. It was a relatively harmless worm that used the Symbian operating system. This is the first mobile threat to spread through the multimedia message. This comm warrior malware was more successful than Cabir malware.

- ✓ **Red Browser**

  Red Browser is the first multiplatform mobile malware. It was established in 2006. It could work on phones which running java 2 mobile edition software. At this time most of the mobile phones running this java 2 mobile edition software such as Samsung, Nokia, Motorola. Hence this malware was spread widely. The malware pretended to be a WPA browser but it sent out the message from the victim's devices instead of browsing the internet.

- ✓ **Flexi Spy**

  This is the first spyware in mobile devices. It established in 2007. This malware could collect messages and also record calls and send the information that collected and recorded to the attacker. This malware was introduced as a spy tool.

- ✓ **Ikee**

  This is also worm malware. It's special in malware iPhone. Although this malware problem for devices up until 2015. However, the worm spread when people decided to removed apple software restriction from their iPhone. When the malware was the start on the phone, stole the apple id, password, changed the default password and also changed the phone's wallpaper.

- ✓ **Zitmo**

  This malware was some dangerous malware because it's stolen our internet banking transaction authorization numbers. Zitmo was targeted to the Symbian operating system but it was spread on Windows mobile, Blackberry and also Android operating system.

- ✓ **Droid Dream**

  This mobile malware was established in 2011. Droid dream is an android threat. Users were downloaded this droid dream malicious software thousand of times on play store. This malware could steal our sensitive data on our mobile devices and also install other applications.

- ✓ **Fake Defender**

  Fake defender is the first mobile ransomware in mobile malware history. It was established in 2013. It's mainly focused on Android devices. Fake defender is also changed operating system setting and users were unable to do a hard reset on their mobile. While this malware was affected lock some device's features and attackers get some money from users to get access back.

- ✓ **Simplocker**

  Simplocker was the first ransomware to encrypt files and hold for ransom. It was established in 2014. This ransomware also focused on the Android operating system. This malware encrypted user's documents, photos, videos stored on the device's SD card. Then the displayed message device had been locked for the presence of child pornography and that the only way to unlock the device was by paying some money. Also, this message was displayed whenever open an app.

- ✓ **YI specter**

  YI specter is a first ios malware for non-jailbroken devices. This malware could allow attackers to install and also uninstall apps, download files, and display advertisements. Yi specter mainly focused on devices in China and Taiwan. The malware was spread through third-party apps stores, social media and also forum posts.

So, mobile malware has a big history. Also, mobile malware authors continuously improve and implement their techniques for the attack on our mobile devices. [2]

Symptoms of Mobile Malware

When a mobile device installed malware, it can cause several problems including allowing to attackers steal, modify or damage data. So understanding how to know if a mobile device has installed any malware is an important step for all mobile devices users'. There are several ways to have know are users' mobile devices in risk. [3]

Daily data usage of the mobile device is the increase

One of the best indicates is the sudden increase in data usage. Some games or applications in mobile devices can use the amounts of data heavily. But without any reason heavily use data in daily it may be a sign that the mobile device has been installed any malware. Most of the mobile devices have the option to see how data are using daily.

Mobile devices' battery is draining faster than other days

This is also one of the well-known symptoms of shows malware was installed into mobile devices. If installed malware to the device, it uses the phone's resources to fulfill its goals without the user's permission. Hence the device's battery is draining faster than other days.

The sudden appearance of Pop-ups Ads

When pop-ups ads will usually show even after the user has left software or applications and remain on the homepage of their mobile devices. Sometimes, these ads will show inappropriate advertisements. Most of the time these pop-ups ads are disturbing to mobile devices users.

Perform poor performance of the device

Most of the latest mobile devices have powerful processors and enough RAM to deal easily with applications, software and also games. As these mobile devices when showing poor performance or lack of performance, it may be one of the symptoms of installed malware into a mobile device. If installed malware to the device it performs very slowly for simple tasks as getting a call or maybe send some text.

Overheating

Overheating is another sign to know installed malware to the devices. Importantly, this is an uncommon issue for most of the smartphones. Hence users have overheating issue, the best thing is to do a virus scan for their device.

Wifi and mobile data switching automatically

Sometimes, users connect to their wifi connection and work through the wifi network but after its switch to mobile data from wifi. This is also sign for know to installed malware into their device.

Download unfamiliar new application

Sometimes, unfamiliar new applications are download into the device automatically. If new and also unfamiliar apps appear unexpectedly on the device, have to chance some malicious app can

be downloaded and installed into the device. Hence users want to check the app is verified app or not before downloaded.

How to install Mobile Malware to devices?

Mobile devices can not secure the same as the computer. Hence mobile devices have a huge chance to affect malicious software in various ways.

Downloading malicious applications

This method is the most common method to spread malware. Users can get apps in the official app store safely. But some users of mobile devices get apps in the third-party software market. These apps can include various types of malware because it comes from a less legitimate source. Sometimes developers use unofficial tools. Everything developed using these tools will include malicious code. Therefore these applications or maybe some software can damage or steal user's data and information easily.

Using mobile devices with operating system vulnerabilities

Sometimes the operating system has vulnerabilities that attackers can exploit Users are not regularly updating the software on their mobile devices, it can be vulnerable.

Open suspicious Emails

Most of the people in today's world use emails. They use email for their official work and also communicate with each other. So email is one of the ways to attackers use to install malware to mobile devices. Sometimes users receive email display something won or have to chance to win something and then users also click to it and open the emails. Then users have been dummy site or maybe nothing happen but meantime downloaded malware and installed it into user's mobile

devices. After hackers can steal, modify or damage to data and information which are store in mobile devices. Most of the users are easily interfere with this suspicious email because of users are trusting email and good suspicious emails are look official.

Using non-secure WiFi or URL

If users are accessing an insecure website, they have to chance to install malware into their mobile devices. If users are using these insecure websites, they can be susceptible to malware and also man-in-the-middle attacks. While we are browsing the internet, show websites URL in HTTPS is secure websites. Others are not secure that show in HTTP. HTTP stands for HyperText Transfer Protocol and HTTPS stands for HyperText Transfer Protocol Secure. Until users using URL in HTTPS, their data is secure than using HTTP otherwise their data at risk. But it does not mean users' data in 100% secure. Attention and responsibility are inevitable when users use mobile devices.

Receiving voicemail or text message

Sometimes users can be receiving text messages or voicemails that asking legitimate information either user or device from anonymous. Reply to these texts or voicemails can be dangerous. In these messages or voicemails have to ability to install malware into mobile devices.

The current state of the Mobile Malware

Today's era rapidly increasing use of mobile devices. Most people are using these mobile devices for mobile banking, store their day to day work, information and also downloading videos, documents for their essential work. Therefore mobile devices are known as a place full of our sensitive data and information in today's world. Hence mobile devices are playing a major role in nowadays society. This is the main reason for Mobile Malware to become an emerging topic in the cybersecurity field. Some people know about what is mobile malware but they can not understand what is the type and how it infected to their mobile devices.
Now plenty of mobile malware are also develop and implement the same as mobile devices. Cybercriminals use various tactics to infect their malware with this developing technology. Mobile malware developers are also doing various things to spread mobile malware among mobile devices.

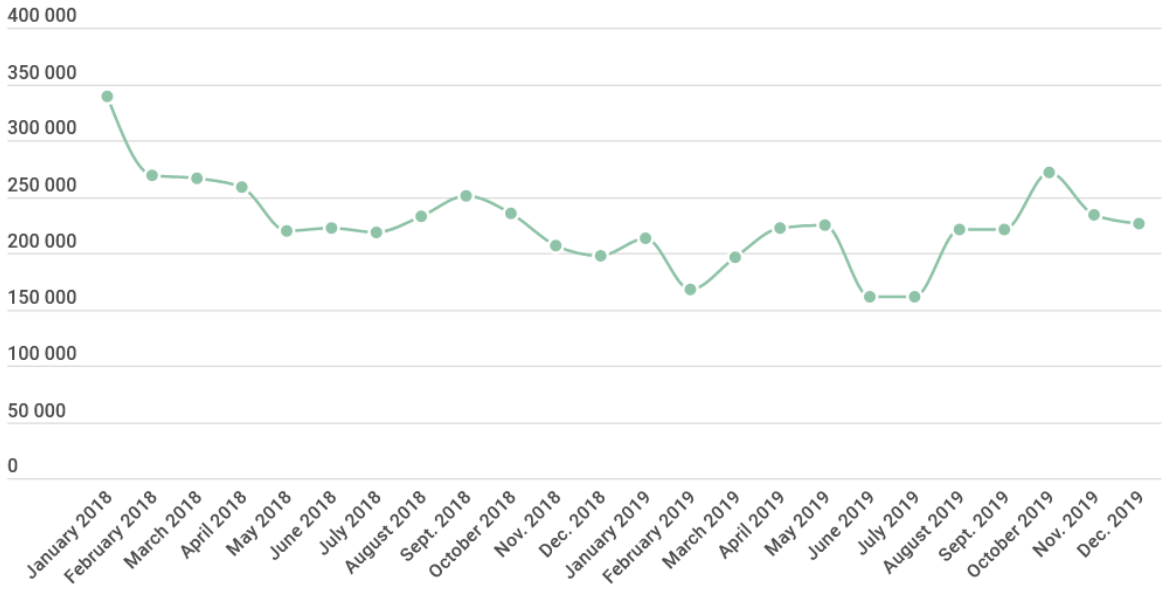
Nowadays most attackers use the *infected applications* method for the launch of their malware among mobile devices for various purposes. Applications are repackaged or include some malicious code into the original code and uploaded to the third-party app store. Recently have a huge trend to the upload infected application to the play store which is an applications market in the Android operating system.

Another trend of used attacker known as *Malvertising.* This is a technique used to spread malware through online advertisements. Online advertisements have a large audience. These online advertisements are dealing with many users through the internet. This situation is used by hackers to launch their malware.

Direct to device is another using technique for spread malware among mobile devices. In this method, hackers want to touch mobile devices to install malware.

The *phishing attack* is also a famous method among cybercriminals in these days. When using this method, redirected to a malware web page through a web redirect or pop-up screen. Sometimes, a link to the infected page is sent to email or text directly. Also, users motivate to the install fake application and then begin collecting our sensitive data across the fake applications.

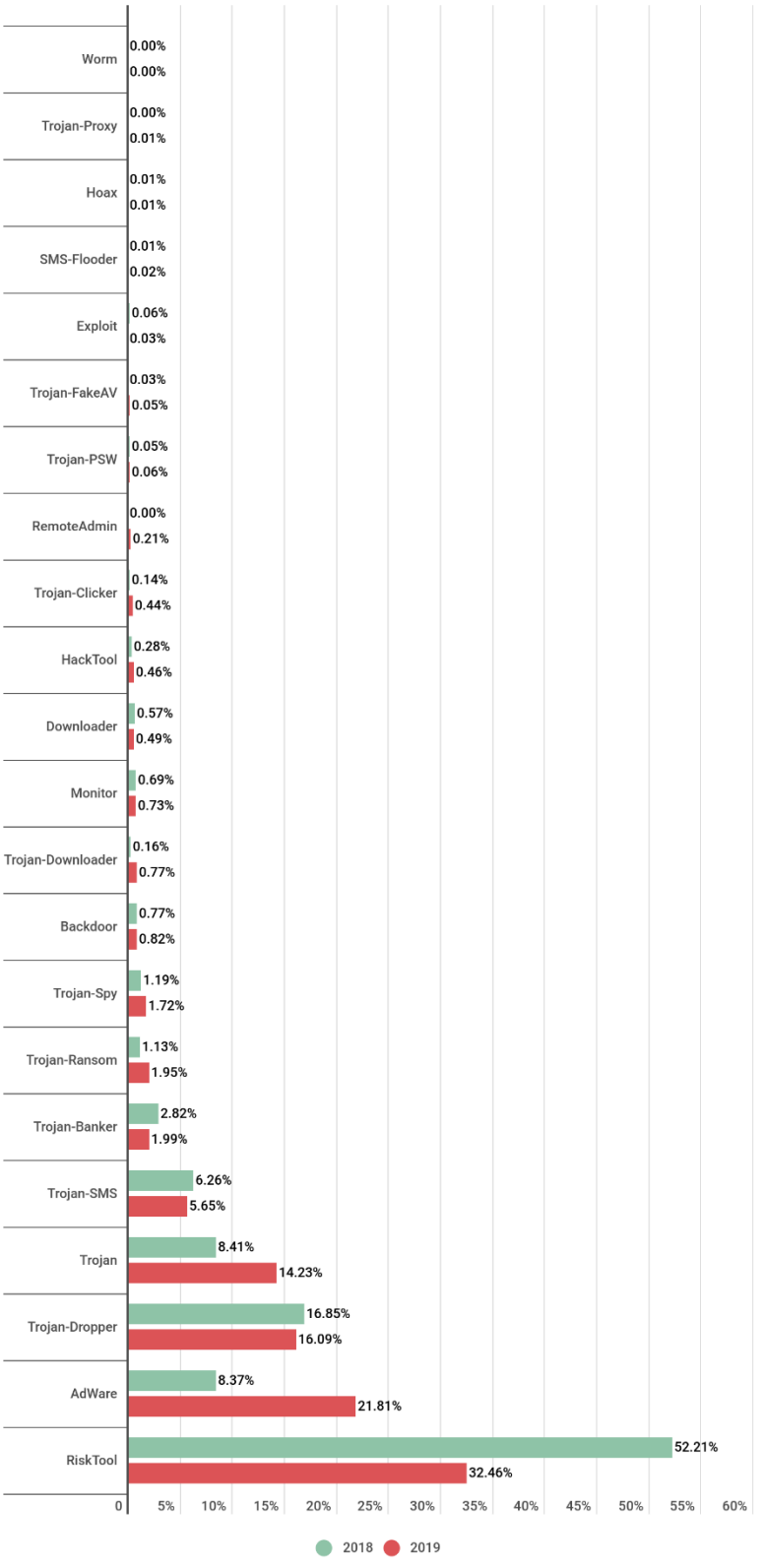
This graph shows the number of attacks by *Adware* [4]



Mobile banking malware is famous malware in these years. Nowadays so many people are doing there transaction or any other banking work with their mobile devices. So hackers see this trend and they also move to the launch of banking malware. They use various methods such as by stealing online banking credentials, stealing and manipulating banking application. Attackers pushed the fake notification and then users tapping this fake notification and open banking application and they fill out their sensitive data like password, account number. After attackers can gain full control of the victim's bank account and they access it.

So mobile malware perform a major role in various ways in today's era and a great threat to mobile devices user's day to day life.

Distribution of mobile malware types in 2018 Vs 2019


Worm
0.00%
0.00%
Trojan-Proxy
0.00%
0.01%
Hoax
0.01%
0.01%
SMS-Flooder
0.01%
0.02%
Exploit
0.06%
0.03%
Trojan-FakeAV
0.03%
0.05%
Trojan-PSW
0.05%
0.06%
RemoteAdmin
0.00%
0.21%
Trojan-Clicker
0.14%
0.44%
HackTool
0.28%
0.46%
Downloader
0.57%
0.49%
Monitor
0.69%
0.73%
Trojan-Downloader
0.16%
0.77%
Backdoor
0.77%
0.82%
Trojan-Spy
1.19%
1.72%
Trojan-Ransom
1.13%
1.95%
Trojan-Banker
2.82%
1.99%
Trojan-SMS
6.26%
5.65%
Trojan
8.41%
14.23%
Trojan-Dropper
16.85%
16.09%
AdWare
8.37%
21.81%
RiskTool
52.21%
32.46%
0
5%
10%
15%
20%
25%
30%
35%
40%
45%
50%
55%
60%
2018
2019

kaspersky

Types of Mobile Malware

Mobile malware are becoming a great challenge to the cybersecurity world. Because today's generation mostly use mobile devices to fulfill their works in day to day life and hackers also moved to this mobile section to launch their attack because most of the people interfere with mobile devices. Hackers using various malware for the attack on these mobile devices. So mobile malware has several types. Such as,

- ✓ Viruses
- ✓ Worms
- ✓ Mobile phishing attacks
- ✓ Mobile bots
- ✓ Mobile Spyware
- ✓ Trojans
- ✓ Ransomware

Some of the mobile malware combines more than one type of attack. Cybercriminals have one or several objectives including steal data, modify data, damage to sensitive data, lock the devices. So they are launching these various types of malware to archive their goals. [5]

Mobile Bots

Mobile Bots are a type of mobile malware. It is a type of botnets that specially targets mobile devices. it's run automatically once installed into mobile devices. if our smartphone or any other devices not protected by antivirus software, it can get the mobile bot. It can gain access to the device and also it's contents include user's data and information. Also, it can make phone calls and access user's media files, contact, document and more. Every device that infected this, it added to the network of mobile bots. Most of the mobile botnets can't be detected and they can spread copies by sending as a text message or emails.

How can bots install into the devices?

- By Email
- While surfing the web
- In drive-by downloads

Also, it can spread through viruses, worms or Trojans with capabilities.

What can happen after successful bot infection?

After successfully bot injection, hackers can access the victim's device with full control.

- Install or uninstall apps
- Make a call
- Send messages or block messages
- Steal sensitive data such as credit card number, passwords
- Copy contacts, messages and send to the server
- Disrupt gain access to networks
- Open any web pages
- Launch a DOS attack

Sometimes botnet identifications are can be a difficulty because a bot can work without user permissions. However, have several basic characteristics to have botnet infection.

- Slow users' system
- Increasing pop-ups ads
- Some issues with internet access

How to prevent mobile bot?

- Download apps only official and trusted app store.
- Be careful with emails.
- Maintain proper antivirus protection.
- Enable pop-up blocker.
- Regularly update the device.

Users can prevent and protect in this mobile bot malware, following and doing these prevention methods and keep safely device and also data.

If users' devices are already infected by a bot, they will have to do something to protect users' data against a bot.

First, try to disconnect the infected device from the network. This step can stop theft user's sensitive data and also prevent to attack other networks.

After, move all data in infected devices to external hard disk or another device

And then the clean infected device with security tools for free of malware.

Even though, follow prevention methods are better than protect. [6]

Mobile phishing

This is identity theft malware. Hackers try to steal personal data and information through this phishing attack. It can be financial loss of individuals as well as organizations because of this phishing attack. A Mobile phishing attack comes in the text messages or email. SMS phishing malware has increased in the new era because of most users open and read messages, they don't expect some malicious message. It has known as "smishing". The main target of this phishing malware usually to get access to users' financial information in the device. Also call phishing known as "vishing" is a type of mobile phishing used to launch malware. If users fell to a text or phishing, make sure to block the number and also inform to the related organizations.

How to protect from Mobile Phishing?

The better thing is to be vigilant.

Installed apps from the official app market.

Turn on caller id and related services.

Also, users can simply take a few steps to protect their devices after clicking a phishing link

- Disconnect devices
- Backup data
- Scan system for malware
- Change password
- Setup fraud alert
- Proceed with be careful

But, already if users are victims of phishing, they also have to do something.

Firstly, users want to disconnect the wifi connection and then want to remember what data or information like username, password user entered. Meantime users want to change their accounts passwords. After try to collect information such as email address or mobile number or whatever things that you receive the malicious email, call or message. Then the user can report to the organization that related to cybersecurity. [7]

Mobile Banking Trojans

Most of the people in the new generation are using their mobile devices for online banking. That is the reason for the rapidly increasing mobile banking Trojans as a kind of mobile malware. This is the most dangerous malware in the malware world because it causes to users' banking information and also transaction. Through this malware, attackers steal sensitive data also same as money. Android users have the highest risk to exposure to Banking Trojans.

Cybercriminals are publishing apps including malicious code in the third-party app store. Then users download it into their device themselves. Mostly, this malicious app act as legitimate. Then users are deceiving and install malicious apps.

Some example of banking Trojans :

Backswap

Panda

Ramnit

Danabot

Didex

Trickbot

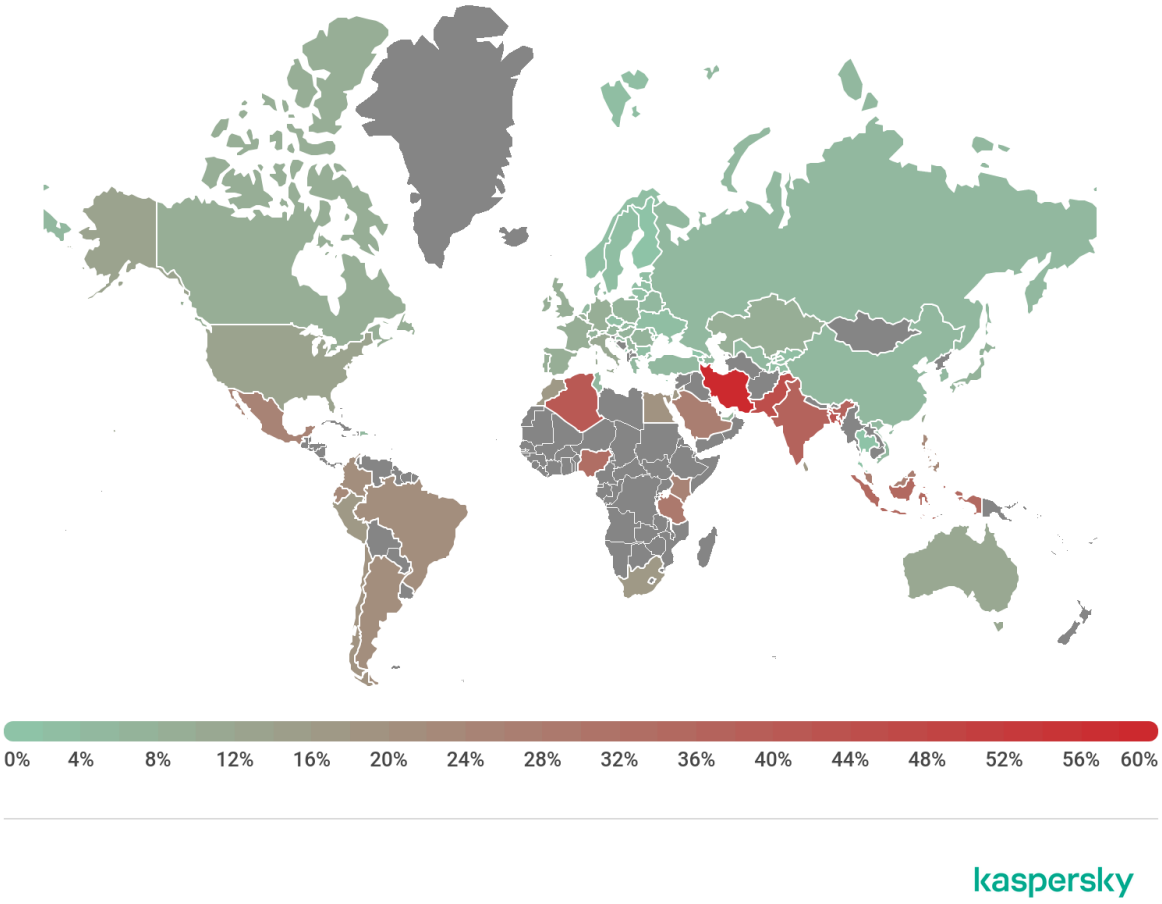
How user can protect from mobile banking Trojans?

- Only download the banking app in trusted app market.
- Use high-security features that bank offers.
- Keep updated software.
- Use a proper password manager because most banking Trojans are using log keystrokes.

- Don’t open any suspicious emails, messages or links.
- Use two-factor authentication.

[8]

Future of the Mobile Malware



This map shows the contribution of users attacked by mobile malware.

According to this map, Iran was coming top country for mobile malware. It is around more than 60%. And also Pakistan, Bangladesh increased mobile malware. Adware is the most common type of malware in these countries. Also, risk tools, types of Trojans are becoming increasing in the world. [4]

Most of the users normally open and read the received text and emails also click to the pop-up ads which the received. Hackers have known this matter and they are increasing to launch their malware through this text, emails or ads. Hence adware and Trojans are rapidly increasing today. This situation will come to the future because most users are less pay any attention to this malicious text, email or pop-up ads. They are open it and click some link in the content that they received email or text and install malware to the devices by themselves. Hackers using this opportunity for their activity. Now, rapidly increasing uses of mobile devices. It never goes down in today's era and also the future world. When increasing the uses of mobile devices, mobile malware also get the same opportunities for increasing unethical activities.

Now, mobile malware attack is an emerging topic in the cybersecurity world. In the future, it will take a major place in the cybersecurity section because attackers are also using some sophisticated techniques and implement mobile malware.

Mobile malware will create a great threat to the future. But users' responsibility is to prevent this mobile malware and do their work.

How to prevent from Mobile Malware

Continuously, attackers are developing more sophisticated mobile malware against mobile devices. They are finding new paths to launch their attack through mobile malware. Have some tips for preventing this malware attack.

Be careful while browsing

When users are browsing the internet, they have a higher risk of install malware on the device. Most of the fake websites and also the link of malware have in the internet. Hence users want to pay attention to this fake website and also links on the web. If users click on the links or visit the websites, it is the beginning of some attack. While users are clicking, malware is installing to the devices and get trouble to users' devices and also data and information. Hence users want to select or filtering legitimate websites or links and be careful when they are browsing the internet.

Install antimalware software

Install more reliable antimalware software is a good prevention method that uses the users. Because it detects malware before it installs to the device. Always antimalware software checks the connection and also helps to scan devices free of malware. Also, it can minimize the risk of malware.

Download apps in the official app market

Hackers include malicious code into the app and release it into the third-party app market. Hence users use the third-party app market, it's maybe a dangerous risk. User use their official app market, it helps to reduce risk from mobile malware.

Pay attention to the setting

This is also an important thing. Because, if malware installed to the device it's getting permission for some tasks without the user's permission. Devices have to enable some protection option in the device setting. If users enabled that option, can minimize the risk from malware. One of the examples is the WiFi auto-connect option. If the user enables it whenever wifi connection is available, device is connected to that. This is a very dangerous thing. Because malware can entry through public Wifi. If the user was disconnected this option, it can get some protection from malware.

Conclusion

To summarize the past few years, Mobile malware has become the most critical and major topic in the cybersecurity world. Because considering the above mention matters, rapidly increase mobile malware programs in the world. Attackers are using various sophisticated methods and implement the malicious program and release it among mobile phones or PDAs. The new generation mostly uses mobile devices such as smartphones, tablets, laptops to fulfill their day to day work as well as their officially works. Hence they store their sensitive and also information on mobile devices. So attackers are also launching their attack on these mobile devices through the newly implemented mobile malware.

Users can store their sensitive data on the server-side and not on mobile devices. It is a good practice. Because if installed any malware into the devices, users don't want to be scared about data. All data on the server-side system. Most of the mobile malware target users' data stored in the devices. If data on the server-side user can be safe.

Mobile devices will continuously grow and evolve. Therefore mobile malware also continuously grows. That's why mobile malware is becoming an emerging topic in the cybersecurity world. But users' responsibility is to prevent this mobile malware and use the mobile device. Some security experts and also companies implement some antimalware software against mobile malware.

Mobile devices users also have some responsibilites for protect from malware. Users recently upadate their system and want to pay attention recently to what happened in their device. Also never click to malicious link or never open suspicious received messages to the device. Users understand these things and use mobile devices correctly, we can do a successful battle against mobile malware.

References

[1] unknown, mobile malware, wikipedia, 2020.

[2] J.-P. power, A Brief History of Mobile Malware, Medium, Apr 12, 2018.

[3] U. Amir, How to identify malware on your phone with these 7 signs, HackRead, December 12th, 2019.

[4] V. Chebyshev, Mobile malware evolution 2019, SECURELIST, February 25, 2020.

[5] M. Rouse, mobile malware, TechTarget, December 2018.

[6] unknown, Mobile botnets taking over smartphones, BullGuard.

[7] C. Kerskie, 5 Steps to Take After Clicking on a Phishing Link, AgingCare, June 5, 2019.

[8] D. W. Remi Cohen, Banking Trojans, F5LABS, August 09, 2019.