CYBER CRIME THREADS ON MOBILE DEVICES

Dr. M. Mohankumar [1] K.Banuroopa [2], M.Vanitha [3]

ABSTRACT

India emerged as the third most vulnerable country in terms of risk of cyber threats, such as malware, spam and ransomware, in 2017 moving up one place over the previous year according to solutions provider Symantec. Nowadays, smart devices with advanced capabilities like those of Tablets and Mobile phones are becoming more and more vulnerable to cyberattacks . The device is usually connected with Internet most of the time. This creates well-known, but not well-understood, threads from cyber criminals. The global threat ranking is based on eight metrics: malware, spam, phishing, bots, network attack, web attacks, ransomware and crypto miners. In this paper, we tried to identify threads on mobile devices and also discuss the solution for above the problem.

[***Key words:*** Ransomware, Malware, Crypto-jacking, Coin-miners, spam, phishing]

I. INTRODUCTION

In today's world with the rise of smart phones there is virtually no difference between computers and mobile phones. These devices are usually network connected including smart buildings e.g. restaurants, homes, shops, and working places. The traditional mobile devices have security and privacy concerns. People are use mobile phones for a number of activities and store all the personal details, such as contact information, email, documents, bank information etc. Attackers are devising new approaches of attack and try to discover their tracks and execute the attacks. India ranks second as most impacted by spam and bots, third as most impacted by network attack and fourth as most impacted by ransomware. Digital security intimidation can come from expected and unexpected sources in the web. Ransomware detection, by country wise in table 1 gives a clear idea about crypto-jacking.

Ransomware detections by country

Typically, ransomware has been more dominant in countries with higher numbers of internet-connected populations.

Rank	Country	Percent
1	United States	18.2
2	China	12.2
3	Japan	10.7
4	India	8.9
5	Italy	4.1
6	Germany	3.4
7	Brazil	3.1
8	Mexico	2.5
9	United Kingdom	2.3
10	Canada	2.1

Table: 1 Ransomware Detection, by County wise

Crypto-jacking is a rising threat to cyber and personal security Tarun-kaura [5]. A massive profit incentive puts people, devices and organizations at risk of

[1]Assistant Professor, Department of CS, CA & IT, Karpagam Academy of Higher Education.

[2] Assistant Professor, Department of CS, CA & IT, Karpagam Academy of Higher Education.

[3] Student, MSc (CS), Department of CS, CA & IT, Karpagam Academy of Higher Education

unauthorized Coin-miners siphoning resources from their systems, further motivating criminals to infiltrate everything from home PCs to giant data centers. This coin mining gold rush resulted in an 8,500% increase in detections of Coin-miners on endpoint computers during the final quarter of 2017. Coin-mining has an immediate impact on performance related slow down process, like overheating batteries in some cases, rendering depiction devices unusable and having a broader implication, specifically, for IT industry.

2. MOBILE THREAD

Mobile threads are like viruses and spyware that can spread to the mobile phones or PCs. [1] [2] There are a variety security threads that can affect the mobile devices. Mobile threads are divided into four categories:

- Mobile Application-based Threads
- Website- based Threads
- Network-Based Threads
- Physical Threads

2.1 Mobile Application-based Threads :

Nowadays many mobile-based applications are downloadable from play stores creating many types of security problems for mobile devices. Some of the 'Malicious apps' may act fine, but they are specifically designed to commit threads for the downloader's [3][4]. Application-based threads generally fit into one or more of the following categories:

Malware :

This malicious software performs [7] actions when it is installed on the phone without the knowledge of the user. For example, it sends unwanted messages to the user's contact list. Table 2 gives details about the new mobile malware variants from 2016 to 2017.

Mobile threats continue to rise

The number of new mobile malware variants grew by 54 percent in 2017, compared to 2016.

Mobile malware variants by year

The number of new mobile malware variants grew by 54 percent in 2017, compared to 2016.

	2016	2017	Change
Mobile Malware Variants	17,214	26,579	54%

Number of malware blocked per day on mobile devices

An average of 23,795 malicious mobile applications blocked on mobile devices each day.

	2016	2017
Total Mobile Malware Blocked	7,193,927	8,684,993
Average per Day	19,709	23,795

Table: 2 Mobile Threats from 2016 to 2017

Spyware :

These threads [4] would try to collect or use private data without the user's knowledge. The data commonly targeted by spyware include phone call history, email, location, private photos and browser history. The stolen information could be used for identity theft or financial fraud. Figure 1 shows the attack via malver-tisement in four steps.

Figure: 1 Shows the Flash Zero Day Attack

Privacy Threads :

A privacy thread is the result of malicious applications that are downloaded by the user for his requirement, but the app gathers user sensitive information like location, contact list, personally identifiable information and threads.

Vulnerable Applications :

Vulnerable applications is an application that helps the attackers try to access sensitive information of an organization-; It mostly happens during unwanted actions or downloading of applications without the user's knowledge.

2.2 Web-site -based Threads :

In this case the user is continuously connected to internet and regularly accesses web-based services, [7].Website-based threads create persistent issues for mobile devices: Figure 3 shows the website-based attacks' blocking details for the year 2017.

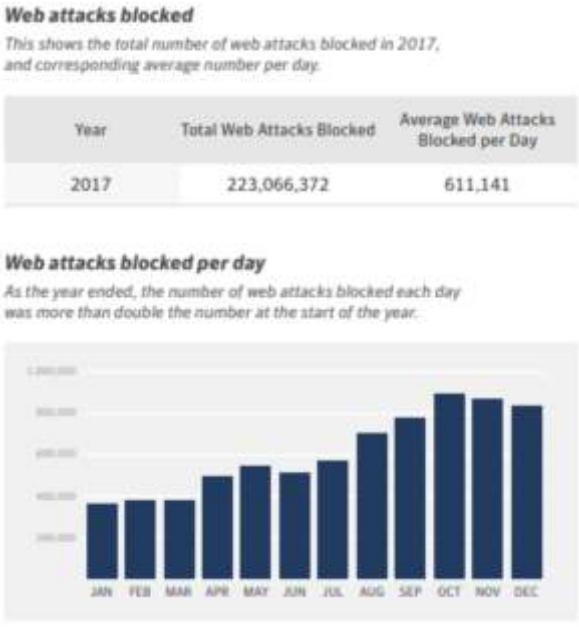

Figure: 3 Web Attacked Blocked in 2017

Phishing Scams: Use of email, text messages, face book and twitter to send links to websites that are designed to trick the user into providing information like passwords and or account numbers. Figure 4 shows the attack execution by bad guys

Figure: 4 Shows the Bad Guys Attack

Drive-By Downloads: When the user visits a webpage without the user permission it can automatically download an application and execute the threads to the user.

2.3 Network Threads:

Smart phones typically support cellular networks and wireless networks such as Wi-Fi, and Bluetooth

Network exploits: It can take chance of defect in the smart phones operating system on local or cellular networks. Once connections are established, they can set up malware on user's Smartphone without his knowledge.

Wi-Fi Sniffing: It is a technology travel through the waves between the mobile device and the Wi-Fi contact point. Many mobile apps and websites which do not take appropriate security measures, while transferring encrypted data from a Wi-Fi network can be simply accessed by someone who can grab the data as they travel. Figure 5 shows the Wi-Fi sniffing methodology in diagrammatic representation.

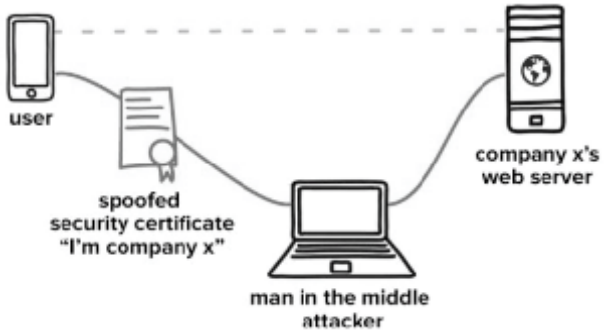

Figure: 5 Shows the Man in The Middle Attack

Network threats [7] analyzed network devices that were exposed to insecure networks over a longer period of time. For example, figure 6 shows that 21.2% of new devices were exposed to network threats in their first month of use. But this rose to 43.7% after four months. In this model, a network threat arises because of there may be a chance for malicious man-in-the-middle (MitM) style attack.

Percentage of Android devices running newest version of OS

	2016	2017
Android Devices on Newest Major Version	15.0%	20.0%
Android Devices on Newest Minor Version	11.8%	2.3%

Percentage of iOS devices running newest version of OS

	2016	2017
iOS Devices on Newest Major Version	79.4%	77.3%
iOS Devices on Newest Minor Version	24.0%	26.5%

Figure: 6 Android devices and iOS versions

2.4 Physical Thread :

Lost or stolen devices are one of the most prevalent mobile threads. The mobile device is valuable not only for the hardware itself as it can be re-sold on the black market, but also for the sensitive personal and organization information it may contain.

3. STEPS FOR PROTECT YOUR MOBILE DEVICES :

1. Download Apps Only from Trusted Sources: If you download apps on your mobile, if it's not from a company you recognize, then do some research before installing the app on your device.

2. Protect Your Phone with a Password: It is the easiest thing you can do to protect your phone from attack. Using a fingerprint lock would be even better.

3. Use an Antivirus or security Software: There are numerous apps available for all phones which can help to protect them. Look out mobile security is a good one with free and paid version for Android and i-phone.

4. Install and maintain a firewall: Firewall is especially important when using different networks. It can help to prevent outsiders from gaining unwanted access.

5. Don't Connect to Public Wi-Fi Without a VPN: Using public Wi-Fi connection can offer more chances for cyber criminals. Many of the VPN (virtual Private Network) providers are now developing mobile apps. Handy clients can be tried to connect to secure VPN server, thereby encrypting your traffic as it leaves your device.

The opportunity :

Globally, about 4 billion people are projected to be online by 2020. [6] Gartner estimates worldwide enterprise spending on information security (including advanced network and security analytics, machine learning technologies, training and user behavior) will touch about $113 billion by 2020.

Cyber as a war zone is becoming increasingly real and everything from social media to mobile phones now have a cyber impact that we cannot be shrugged off. A seismic shift to smarter cybersecurity is the need of the hour

4. CONCLUSION :

The value of data is slowly increasing. Nowadays mobile users and enterprises are facing many kinds of mobile attacks such as malware, theft, and loss. This paper discusses the attacks against on mobile phones and PCs. It focuses on how the attack is carried out and what the goal of the attacker is. Finally, current security solutions for mobile phones or smart phones are reviewed.

REFERENCES

1. http://www.cs-cert.gov/reading_room/TIP10-105-01.pdf
2. http://www.cs-cert.gov/cas/tips/ST04-017.html
3. https://www.pwc.co.uk/issues/cyber-security-data-privacy.html
4. https://www.lookout.com/resources/reports/mobile-threat-report
5. https://www.deccanchronicle.com/technology/in-other-news/050418/cryptojacking-skyrockets-massive-threat-to-cyber-personal-security.html
6. https://www.csoonline.com/article/
7. https://www.symantec.com/blogs/threat.../istr-23-cyber-security-threat-landscape