Survey on Mobile Device Cyber Crime

Dr. M. Mohankumar[1], K.Banuroopa [2], K.Sreevidhya [3]
[12]*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*

Abstract- India has been the most liable country in terms of the risk of cyber threats, such as malware, spam and ransomware, in 2017, moving up one place over previous year, according to a report by security solutions provider Symantec. In 2017, 5.09% of global threats detected were in India, slightly less than 5.11% in 2016.The U.S (26.61%) was most vulnerable to such attacks, followed by china. Threats in the mobile space are increasing day by day. The number of cyber mobile crime increased 54% in 2017, which is high when compared to last year. On an average of 24,000 malicious mobile applications were blocked each day. In this paper we are going to look about what is meant by mobile device crime and what are the attacks that have taken place.

Keywords- malware, ransomware, grayware,vishing, smishing.

I. INTRODUCTION

A mobile device is uttermost widely used by people worldwide. Nowadays people can't be afforded to stay without a mobile device. There are many different types of devices people may tend to use, such as cell phone, pc, laptop etc. which are connected to Internet. But most people prefer a hand held device which easy to carry everywhere.
In this technologically advanced era, the devices are also grows advanced day by day. People eagerly look forward to the newly upcoming advanced mobile phones. There is diverse of different crimes in mobile phone.

II. MOBILE DEVICE CRIME

Cyber-crime is the most complicated problem in the cyber word. In this cyber world mobile crime is one of part it. Most of the peoples were affected by mobile crime in every one's life one way or other. However, the technology advanced newly produced mobile devices is very weak in security, so that criminal may easily hack such a device. Criminals fighting for their cause would want their goal to be achieved at any cost. The global threat ranking is based on eight metrics that is malware, spam, phishing, bots, network attacks, web attacks, ransom ware and crypto miners as per the report given by security solutions provider Symantec. India is in a second position in spam and bots attack, third in network attack and fourth in ransomware.
Most of the time the device will be switched on and the people won't preserve their data and any other backup for the data. So, criminals can easily access the device and hack it. People may have no idea that knowingly or unknowingly they are affected cyber-crime

A. MOBILES WITH HUMAN LIFE

Mobile operating system is usually an open source system. Unauthorized persons can enter with ease and can hack the device. People were easily addicted to mobile device by newly upcoming advanced one. By Year by year passing the device would be more technically developed and will be more attractive. So, people were dump to buy newly ones.

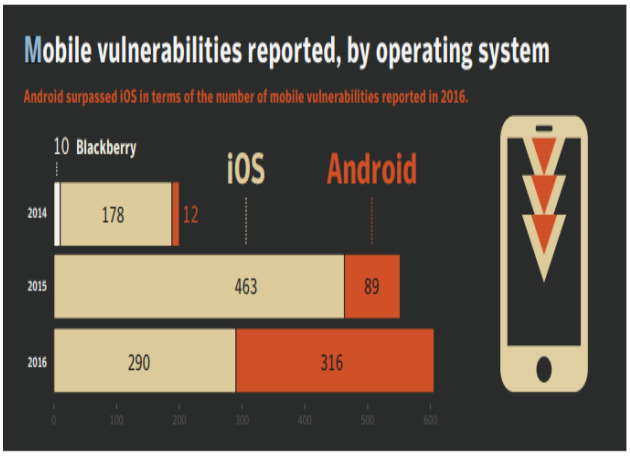

Fig.1: Mobile Vulnerabilities by operating system

In every day mobile is the one of main part in every one's life. With using like alarm, communication, calls, calculator, calendar and etc. this are may use in regular days. They can't be stay without using. McAfee, in its survey pointed out that of the Indian children active on social media, 69% have published photos, 58% have posted their email address and 44% would meet or have met someone in person that they first met online.

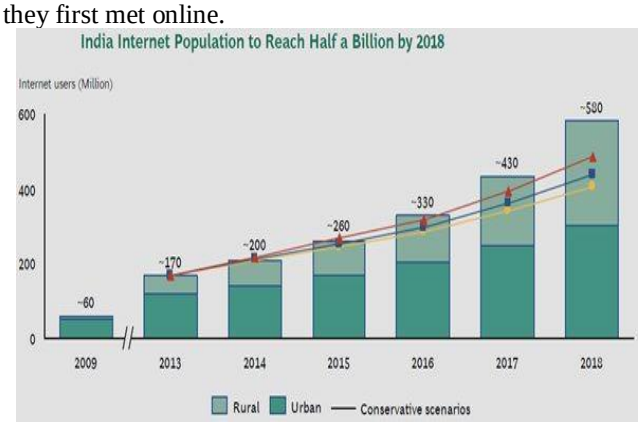

Fig.2: Survey on Indian internet usage

Malware continues to be a threat with more than 357 million new variants observed in 2016. However, for the first time,

the rate of new malware seen on the endpoint has remained largely stagnant in 2016 – increasing by only a half a percent.

In this year 2018 internet population has increased than previous years. In future this trend will tend to increase and more people will start using the Internet through mobile devices.

There were major growth spikes in both malware and grayware apps between the years 2014 and 2015, but in 2016 both areas leveled off. In the year 2016 grayware increased only by less than 4% but malware increased around 30% compared to year 2015. The levels of grayware and malware identified in 2016 are now almost equal.

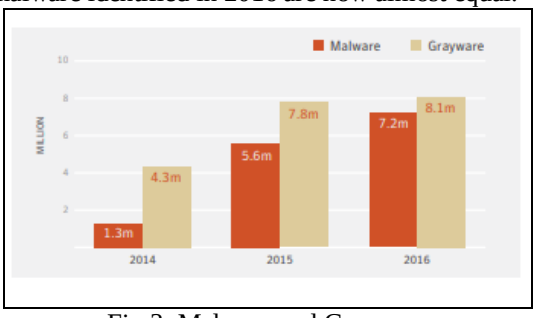

Fig.3: Malware and Grayware

III. TYPES OF CRIMES

These are the some of the cyber-crimes on mobile device activities.

- Vishing
- Smishing
- Blue bugging
- Blue jacking
- Blue snarfing

A. VISHING

Vishing is the criminal act of using voice email, landline or mobile to gain access to personal financial information. In this the criminals may achieve their goal by collecting their needed.

Fig.4: Vishing

B. SMISHING

Smishing is a criminal activity that may act as a like send sms text and calls. Phishing is related to smishing. Phishing is when someone tries to give them your private information. Smishing depends on fooling the people by sending a text message and that may contain a URL and by clicking on the link the user's device is hacked for information.

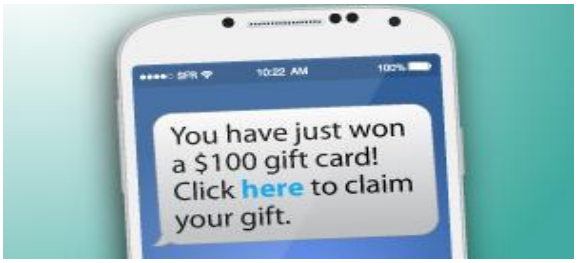

Fig.5: Smishing

C. BLUE BUGGING

Blue bugging is activity that accesses the mobile through Bluetooth device. This may act on wireless device. Within Bluetooth they may try to inter act with users.

Fig.6: Blue bugging

D. BLUE JACKING

Blue jacking is a sending of unwanted message from Bluetooth to Bluetooth device such as mobile, computer. People using Bluetooth in mobile phones and PDAs can send messages, including pictures, to any other user within a 10-meter or so range. While connecting to a Bluetooth the hacker may act on user device, by stealing pictures, documents and personal information.

Fig.7: Blue jacking

E. BLUE SNARFING

Blue snarfing is the unauthorized access of information from a wireless device through a Bluetooth connection on mobile device, computer, and laptop. Bluetooth is of high-speed but very short-range wireless technologies to share a data are other documents.

IV. SECURING CELL PHONE

Given below are certain pointers to secure a cell phone.

- Keep your mobile phone safe and secure.
- Use strong password.
- Backup your data regularly.
- Keep your anti-virus up to date
- Install only secure apps.
- After using data and other wireless connection, turn them off.
- Don't store and share any personal information and any bank details in mobile phones.

V. CONCLUSION

A mobile phone is just a way to communicate and make call through network connection. These devices are wireless so they can be carried where ever we want. The device is a danger to this generation, more so for children. Year by year the usage of mobile are increasing and also the crime associated with it. While people get involved more on mobile devices then they are prone to cyber crimes. Not all the crimes can be identified. People may get affected personally or financially by these crimes. Even some of applications and files downloaded may assist in hacking. While using Internet there the hacker may enter the device due to lack of security. The rate of cyber crime will not reduce unless the security of devices is increased.

VI. REFERENCES

[1]. http://www.cialfor.com/2016/02/15/
[2]. https://www.ft.com/content
[3]. https://www.researchgate.net/publication
[4]. http://www.cialfor.com/2016/02/15/
[5]. http://racolblegal.com/crimes-committed-through- mobile-phones
[6]. http://cyberlaws.net/cyber-law-books/mobile-crime-mobile-law