CYBER SECURITY ISSUES
&
CHALLENGES FACED IN HANDLING CYBERCRIMES

Pranav C
Sir MV Institute of Technology, Department of Electronics & Communications

Abstract: With rapid computerisation of all walks of life, cyber security has become a major challenge to the mankind. Cyber security is all about security of anything in cyber realm, while information security is all about security of information regardless of the realm. Cybercrimes are perpetrated by using computers and related devices / networks by individuals with sophisticated knowledge in the field of computers. Cybercrime is an evil having its origin in the growing dependence on computers in modern life. In a day and age when everything from microwave ovens and refrigerators to nuclear power plants is being run on computers, cybercrime has assumed rather sinister implications. Cybercrime perpetrators are keeping pace with innovations in technology and are way ahead of security measures taken to curb them. With huge money involved in cybercrimes, it has become a major concern. This research paper briefly defines cyber security and deals in detail with cybercrime and five major cyber security threats currently plaguing the world.

Keywords: Cyber Security, Information Security, Cybercrime, major cyber security threats

I. Cyber Security

As per the NIST (National Institute of Standard and Technology) definition [1] Cybersecurity means, ability to protect or defend the use of cyberspace from cyber attacks.

On the other hand, Information Security is Protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide —

1) **integrity**, which means guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity;

2) **confidentiality**, which means preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information; and

3) **availability**, which means ensuring timely and reliable access to and use of information.

II. Cybercrime – An Introduction

As per National Cyber Crime Reporting Portal [2], an initiative of Government of India, cybercrime is defined as "Any unlawful act where computer or communication device or computer network is used to commit or facilitate the commission of crime".

Merriam-Webster defines cybercrime as: ": criminal activity (such as fraud, theft, or distribution of child pornography) committed using a computer especially

to illegally access, transmit, or manipulate data." [3] "Cybercrime" is very broad term and represents a wide variety of criminal activities that are conducted by using and/or targeting any type of electronic devices such as computers, cell phones, databases and IoT devices.

Any criminal activity that uses a computer either as an instrumentality, target or a means for perpetuating further crimes comes within the ambit of cyber crime [4].

A generalised definition of cybercrime may be 'unlawful acts wherein the computer is either a tool or target or both [5]. The computer may be used as a tool in the following kinds of activity – financial crimes, sale of illegal articles, pornography, online gambling, intellectual property crime, e-mail spoofing, forgery, cyber defamation, cyber stalking. The computer may however be target for unlawful acts in the following cases – unauthorised access to computer / computer system / computer networks, theft of information contained in the electronic form, e-mail bombing, data diddling, salami attacks, logic bombs, Trojan attacks, internet time thefts, web jacking, physically damaging the computer system [6].

Cybercrime can begin wherever there is digital data, opportunity, and motive.

The peculiar characteristics of cybercrime are:

a. The weapon with which cybercrime is committed is technology. Cybercrimes are the work of technology and thus cyber criminals are technocrats who have deep understanding of the internet and computers.

b. Cybercrime is extremely efficient i.e., it takes place in real time. It may take seconds or a few minutes to hack websites or do cyber frauds.

c. Cybercrime knows no geographical limitations, boundaries or distances. A cyber criminal in the one corner of the world can commit hacking on a system in the other corner of the world for example a hacker in the US can in real time hack in the system placed in Japan.

d. The act of cybercrime takes place in cyberspace which makes the cybercriminal being physically outside cyberspace. All the components of cyber criminality from preparation to execution, take place in the cyberspace.

e. Cybercrime has the potential of causing harm and injury which is of an unimaginable magnitude. It can easily destroy websites created and maintained with huge investments or hack into websites of Banks and the defence department's websites. The amount of loss which may cause is easy to be imagined.

f. It is extremely difficult to collect evidence of cybercrime and prove the same in the Court of law, due to the anonymity and invisibility of cybercriminal and its potential to affect in several countries at the same time, which are different from the place of operation of the cybercriminal.

The upward progression in technology is also helping in the rise of hackers and other cybersecurity threats. Further, the risks for cyber frauds are also heightened with the increased awareness and knowledge of technology, from consumers and hackers alike. Cybercrime's sophistication and scope tend to grow right along with the technologies that enable it. Two such technologies are cryptocurrencies (e.g., Bitcoin) and anonymous browsers, which promote the continued expansion of cybercrime by protecting criminals' identities. Consequently, they allow hackers to extort money without leaving any personally identifying information.

The amount involved in cybercrimes is huge. According to a report by Cybersecurity Ventures, the cost of cybercrime is slated to reach an astounding $6 trillion globally by 2021. This is particularly worrisome given the massive recent increase in ransomware, in which cybercriminals demand payment or will lock users or companies out of their data or systems. According to the Cisco's "2017 Annual Cybersecurity Report," ransomware is growing 350 percent each year.

Origin of cybercrimes can be traced to 1970s when computer virus was invented. Those were days when internet was not much popular and there was not much technological sophistication. However, with the rapid growth in technology, cybercrimes also started evolving with new threats being introduced as a result of a new product / technology. For example, cryptojacking threat was introduced with bitcoins.

III. Top 5 Risks

While currently, we are facing many types of cybercrimes, we may classify the following as top 5 risks: 1) Ransomware attacks 2) Cryptojacking attacks 3) phishing 4) farmjacking and 5) IoT attacks. Brief details of these 5 threats are provided in the following paras.

1) Ransomware attacks

Ransomware is a computer malware that takes control of system and demands payment for regaining control. Ransomware is a serious malware infection. It typically propagates as a conventional computer worm, entering through vulnerability in a network service or an E-mail attachment. It may then disable an essential system service or lock the display at system start-up and encrypt some of the user's personal files. In both cases, the malware may prompt the user to enter a code obtainable only after making payment to the attacker [7].

Working of Ransomware

Ransomware is spread through links and downloads that trick people into allowing access to their computer and network system. In most of the cases, the ransomware is sent via an email that appears to come from a legitimate source. The link within the email is clicked or attachment is downloaded which contains the malicious ransomware code. Ransomware also can get into our systems through social media messages or by clicking links on compromised websites and plugging in an unfamiliar USB drive, etc.

There are several things the malware might do once it's taken over the victim's computer, but by far the most common action is to encrypt some or all of the user's files. But the most important thing to know is that at the end of the process, the files cannot be decrypted without a mathematical key known only to the attacker. The user is presented with a message explaining that their files are now inaccessible and will only be decrypted if the victim sends an untraceable Bitcoin payment to the attacker.

Examples of Ransomware attacks

Bad Rabbit: Target of bad rabbit are insecure websites. User visits these websites, which are actually legitimate websites, without knowing that these are compromised. Bad rabbit is spread through a method called "drive-by attack".

Wannacry: it is a wormable ransomware and spreads like a virus. It affected lakhs of computers and crippled banks, law enforcement agencies and other infrastructure. It used EternalBlue developed by NASA and stolen by hackers.

NotPetya: it started as a fake Ukranian tax software update. It also used EternalBlue. It hit a number of firms in the US and caused major financial damage.

Locky: It was released in the year 2016 by hackers. Locky spreads via fake emails with infected attachments. It has the ability to encrypt files.

CryptoLocker: Cryptolocker again is spread through infected email attachments. Once transmitted to computer, it searches for valuable files to encrypt and hold to ransom. Though it was first seen in 2007, large scale attack on systems started in 2013.

2) Cryptojacking

Cryptojacking is the unauthorized use of a computer, tablet, mobile phone, or connected home device by cybercriminals to mine for cryptocurrency.

Meaning of Cryptocurrency

Cryptocurrency is a form of digital currency that can be used in exchange for goods, services, and even real money. Users can "mine" it on their computer by using special programs to solve complex, encrypted math equations in order to gain a piece of the currency.

It's hard to explain how cryptocurrencies gain monetary value; however, it is based in part on the principle of supply and demand, and the difficulty of obtaining the cryptocurrency. For example, there are only a finite number of Bitcoins that have not been completely mined. There are other variables such as how easy the currency is to use, the energy and equipment put into mining it, and more.

For these reasons and others, cryptocurrency has fluctuated in value in the past several years. In 2010, a Bitcoin was set at less than 1 cent. Cryptojacking also skyrocketed in 2017.

In a sense, cryptojacking is a way for cybercriminals to make free money with minimal effort. Cybercriminals can simply hijack someone else's machine with just a few lines of code. This leaves the victim bearing the cost of the computations and electricity that are necessary to mine cryptocurrency. The criminals get away with the tokens.

Toward the end of 2017, when the value of cryptocurrency was at its peak, there were about 8 million coin-mining events blocked by Symantec in December alone. Because cryptojacking can yield lucrative results, coin-mining activity increased by 34,000 percent over the course of the year.

Working of cryptojacking

Coin mining on your own can be a long, costly endeavor. Elevated electricity bills and expensive computer equipment are major investments and key challenges to coin mining. The more devices you have working for you, the faster you can "mine" coins. Because of the time and resources that go into coin mining, cryptojacking is attractive to cybercriminals.

There are a few ways cryptojacking can occur. One of the more popular ways is to use malicious emails that can install cryptomining code on a computer. This is done through phishing tactics. The victim receives a seemingly harmless email with a link or an attachment. Upon clicking on the link or downloading the attachment, it runs a code that downloads the cryptomining script on the computer. The script then works in the background without the victim's knowledge.

3) Phishing

Phishing is a form of social engineering, characterised by attempts to fraudulently acquire sensitive information, such as passwords and credit card details, by masquerading as a trustworthy person or business in an apparently official electronic communication, such as an e-mail or an instant message [8]. The term phishing arises from the use of increasingly sophisticated lures to 'fish' for users' financial information and passwords [9]. The act of sending an e-mail to a user falsely claiming to be an established legitimate enterprise in an attempt to scam the user into surrendering private information that will be used for identity theft. The e-mail directs the user to visit a web site where they are asked to update personal information, such as passwords and credit card, social security, and bank account numbers, that the legitimate organisation already has. The web site, however, is bogus and set up only to steal the user's information [10]. By spamming large groups of people, the 'phisher' counts on the e-mail being read by a percentage of people. Phishing, also referred to as brand spoofing or carding, is a variation on 'fishing', the idea being that bait is thrown out with the hopes that while most will ignore the bait, some will be tempted into biting [11].

Types of Phishing Attacks

Spear phishing

"Spear Phishing" is a method of sending a Phishing message to a particular organization to gain organisational

information for more targeted social engineering. Spear phishers send e-mail that appears genuine to all the employees or members within a certain company, government agency, organisation or group. The message might look like as if it has come from the employer or from a colleague who might send an e-mail message to everyone in the company. It could include requests for usernames or passwords.

While traditional phishing scams are designed to steal information from individuals, spear phishing scams work to gain access to a company's entire computer system. If you respond with a user name or password, or if you click on the links or open the attachments in a spear phishing e-mail, pop-up window or website, then you might become a victim of ID theft and you might put your employer or group at risk.

Clone Phishing

In clone phishing an almost identical or cloned email is created from a legitimate, and previously delivered email containing an attachment or link which are then replaced with some thing malicious.

Whaling

It is also called as CEO fraud as under whaling attack, cybercriminals directly target senior or other important executives in an organization. The purpose of the attack is to steal money or sensitive information or gaining access to their computer systems for criminal purposes.

Some phishing scams

Hackers have stolen $46.7 million from Ubiquiti Networks, a U.S. computer networking company by using phishing emails. This amount account for nearly 10% of the company's cash position [12].

In 2014, phishers could swindle $50 million from Smith Laboratories, a U.S. drug company over a period of 3 weeks. The phishers instructed company's accounts payable coordinator to make nine fraudulent transfers by sending phishing emails impersonating the company's CEO.

4) Formjacking

Formjacking is when cybercriminals inject malicious JavaScript code to hack a website and take over the functionality of the site's form page to collect sensitive user information. Formjacking is designed to steal credit card details and other information from payment forms that can be captured on the checkout pages of websites.

Working of formjacking

Once a website user enters their payment card data on an e-commerce payment page and clicks "submit," the malicious JavaScript code collects the entered information. The malicious JavaScript code that has been installed by the cyber thieves can collect information such as payment card details, home and business addresses, phone numbers and more. Once the information has been collected, it is then transferred to the attacker's servers. The cyber thieves can then use this information for financial gain

themselves, or they can sell the information on the dark web.

5) IOT attacks

IOT is the interconnection of uniquely identifiable embedded computing devices. That means any device that can be connected – not just computers, but various types of sensors and monitors, too. Unlike in the case of internet of people where people access data and communicate with one another, in the case of Internet of Things, things access data and communicate with one another. While humans will continue to use the current internet, future internet will also be a pipeline for non-human devices [13].

The more devices you connect to the global network, the more points you have for hackers to enter and corrupt the system. Billions of new devices mean billions of new opportunities for the bad guys to exploit. That is challenge.

In addition, all the data collected by all these new IoT devices puts a lot of personal information out there just waiting to be stolen or legally abused by those in power. The IoT devices, when up and running, will know quite a lot about you and what you do; who will have access to that information, and how will they use it?

Then there is the issue that the more we rely on the IoT, the more vulnerable we will be if some or all of it is attacked or goes offline. If we rely on the smart grid to manage all our electricity use, what do we do when hackers hack into and takes control of the smart grid systems? How about if a malcontent hacks into your smart car's autonomous guiding system? Or terrorists take control of Domino's fleet of pizza delivery drones?

For these reasons and more, we need appropriate safeguards to ensure that our smart devices do not get hacked into and the IoT does not fall under malicious control. Otherwise, the consequences are frightening to consider.

Concerned about the dangers posed by the rapidly growing IoT attack surface, the FBI released a public service announcement, FBI Alert Number I-091015-PSA: "Internet of Things poses opportunities for cybercrime." The PSA warns about potential vulnerabilities and advocates protective measures that should be taken to mitigate risk associated with them.

Kaspersky, security solution provider, deployed more than 50 honeypots worldwide, and detected 105 million attacks on Internet of Things (IoT) devices from 276,000 unique IP addresses, within only the first six months of 2019. The number of attacks in 2019 is nine times greater than the number found in the first half of 2018, which totalled 12 million attacks [14].

Mirai is a malware family that hones in on weak IoT devices to use in a large-scale DDoS attacks. Mirai was popularized by its massive cyberattack that swept both the US and Europe in 2016, causing the largest internet blackout in US history. Mirai, responsible for 39% of attacks, exploited unpatched vulnerabilities; while Nyadrop,

which comprised another 39% of attacks, used password brute-forcing attacks.

IV. CONCLUSION

Cybercrime is not a threat that can be ignored. It is not going away anytime soon. A good level of cyber defence, an ability to detect and respond to attacks and ever developing knowledge and awareness amongst technical teams, manager and staff/users has never been more important. Usage of innovative tactics like cyber deception, reverse engineering, and offensive AI need to be considered to ensure technology is leveraged to the fullest extent to protect the organisation. The potential costs are just too big to ignore. To conclude, keeping up with the latest approaches to staying one step ahead of the cybercriminals is essential.

REFERENCES

[1] National Institute of Standard and Technology: *http://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf*

[2] https://cybercrime.gov.in/

[3] https://www.merriam-webster.com/dictionary/cybercrime

[4] https://www.naavi.org/pati/pati_cybercrimes_dec03.htm

[5] R Nagpal – Beware! Cyber Criminals are on the prowl, Navhind Times March 17, 2002.

[6] Smt. K Prasanna Rani, 'Nature of Cyber Crime – Strategies to tackle Cyber Crime' Cri.LJ,

[7] https://en.wikipedia.org/wiki/Ransomware

[8] Lance James, Phishing Exposed, Elsevier 2005.

[9] Tan, Koon. Phishing and Spamming via IM (SPIM). Internet Storm Center.

[10] *Ollmann, Gunter. The phishing guide: understanding and preventing phishing attacks. Technical info. July, 2006*

[11] *Spam Slayer: Do you speak spam? PCWorld.com*

[12] https://www.nbcnews.com/tech/security/ubiquiti-networks-says-it-was-victim-47-million-cyber-scam-n406201

[13] "The Internet of Things" by Michael Miller

[14] https://www.kaspersky.com/about/press-releases/2019_iot-under-fire-kaspersky-detects-more-than-100-million-attacks-on-smart-devices-in-h1-2019

AUTHOR'S PROFILE

Mr Pranav C is undergraduate student of Sir MV Institute of Technology, Bangalore, India doing Engineering in Electronics & Communication. His interests are in Big Data, Machine Learning and Cyber Security. He is an IT buff and keeps himself updated with the latest developments in the areas of technology and IT security. He is also member of Institute of Electrical and Electronic Engineers.