IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 20, Issue 1, Ver. I (Jan.- Feb. 2018), PP 30-34
www.iosrjournals.org

A Survey on: Cyber Crime & Information Security

*Hardik Runwal[1], Pooja Akulwar[2]
[1](Student Scholar, Computer Science & Engg. department, SSDGCT's Sanjay Ghodawat Institute, India)
[2](Assistant Professor, Computer Science & Engg. department, SSDGCT's Sanjay Ghodawat Institute, India)
Corresponding Author: Hardik Runwal

Abstract : *Cybercrime is not escapable and is highly linked with different parts of criminal environment. As there is vast use of internet users, abusage of technology is increasing which leads to cybercrime. Cybercrime is basically illegal act which leads to criminal activity. Cyber security is a mechanism by which computer data and equipment are protected from unauthorized access. This paper is mainly focused on cybercrime and its impact on society. It also describes cybercrime forms, causes and cyber security concept in detail.*

Keywords: *Fraud, Cybercrime, hackers, Security methods, privacy*

Date of Submission: 03-01-2018 Date of acceptance: 20-01-2018

I. Introduction

When a computer or network is the target, source tool, or the medium of crime, such a criminal activity is referred as computer crime, cybercrime, hi-tech crime, e-crime, or electronic crime.As there is no single specific definition of cybercrime or hi-tech crime the law of enforcements describes these crimes in two different parts:

1. **Hi-tech crime(Advanced cyber crime**)

The hardware and software attacks are done in a sophisticated manner

2. Cyber-enabled crime

Cybercrimes committed by many individuals or small groups have taken over the sophisticated traditional manner with the advent of new technologies as well as the Internet., due to which many complex networks of cybercriminals is being built across the world to perform criminal activities on an unpredictable scale, thus increasing crimes against children, as well as financial crimes and terrorism.

II. Literature Survey

Report show that many simple innovative tactics by cyber criminals which lead to unprecedented outcomes in global threat activity. Many extraordinary attacks are marked in the year 2016 which revealed new levels of cyber criminal attacks. These attacks include disrupted elections, bank heists, threat landscape etc. The bank heists included multiple million dollar virtual banks, the U.S. election process was attempted to be disrupted by the state sponsored groups. There has been a shift in the focus of attacks due to the new innovations and new sophistications. Sophisticated malwares and zero day vulnerabilities were used for developing straight sabotage. Meanwhile, with the help of cloud services and simple IT tools cyber criminals caused a large amount of disruption. Targeted attacks on government shift focus from economic sector to the politically motivated subversions. Cyber criminals execute these attacks which were politically devastating against the U.S. Democratic Party which leaked the stolen information reflecting a trend of overt campaign designs to destabilize organisations which disrupted the countries as it was highly spread. Before few years such cyber attacks were rare, but due to the success of several campaigns like the U.S. elections influenced politics to sow discord across globe. Email has become a dangerous threat to users as it is efficient. One in 131 emails nowadays contains malware, which is the highest rate in last five years. Thus emails have become the weapon of choice that allows infiltrators to hide from plain sight. Relying on spear-phishing emails over 400 businesses are targeted every day creating Business Email Compromise scams, draining about $3 billion in three years.Ransomware is considered as the profit centre for criminals all over the globe. 64 percent of Americans in the USA make an easy mark for ransomware scammers. More than triple the amount of new malware families have been released into the world Symantec identified about 100 new malwares with an increase of 36 percent of ransomware attacks worldwide. As 64 percent of Americans are ready to pay ransom the United States is the biggest and the softest targets. On an average, criminals demand about $1,077 per victim.The cloud infrastructure provides a frontier for cybercrime making the cloud a dangerous place for such vulnerabilities due to the growing reliance on cloud services for organisations. More than ten thousand of cloud databases were hijacked and held for ransom in 2016, the outdated versions were held without authentication and turned on.

III. Common Forms Of Cyber Crime

3.1 Malware
Malware is designed basically to damage, destroy or disrupt network services, computer software and computer data. The several types of malware include worm, viruses, Trojan horse, botnet, root kit, spyware.

3.2 Spam:
Spam is the unsolicited sending of emails in bulk for commercial purpose in an unlawful manner to various extent. Spam which is originating in India is considered for one percent amongst all the top 25 spam producing countries and thus ranking as the eighteenth country worldwide for originating spam.

3.3 Phishing:
Phishing has an impact of US$5 billion worldwide annually as per the 2015 analysis. It is an attempt to acquire information which is sensitive to get the money indirectly like acquiring passwords, username, credit card details by disguising as a trustworthy entity for malicious reasons.

3.4 Hacking:
A type of crime to access sensitive or personal information by breaking into a person computer is hacking.

3.5 Cyber Stalking:
Cyber stalking is a kind of online harassment by barraging messages and emails to the victim.

3.6 Fraud:
Any dishonest misrepresentation leads to encourage loss, which is computer fraud. Fraud results in altering computer input in unauthorized manner, destroying or stealing output, deleting data, misusing system tools and software packages. Real programming skills are required for this

3.7 Obscene:
Obscene is the offensive content, this communication may be illegal in some instances. These communications may be offensive for a variety of reasons.

3.8 Cyber terrorism:
There has been an increase in the Internet problems as well as server scans which are a result of the organised efforts of many cyber terrorist. Cyber terrorist are a group of people to map the security holes of the government officials and the other critical system, such a critical and harmful security threat is called as cyber terrorism.

IV. Causes of Cyber Crime

The basic and main reason for the rise in cybercrime across the world is that catching such cyber criminals is difficult. The investment is high then the rate of return and also the risk is low in such situations certain people willingly take advantage of it leading to cybercrime. The sensitive information as well as data is accessed which helps for getting more the spent amount in return and also it is difficult to get caught in such situations thus resulting to the rise of cybercriminals.

V. How Cyber Crimes Are Brought To Execution

5.1 Malware

Malware typically infects a machine by tricking users into clicking and installing a program that they shouldn't from the Internet. When the click or installation occurs, the malicious code executes actions that the user doesn't anticipate or intend, which could include:

1. Self-replication in different parts of the file system
2. Blocking access to files, programs or even the system itself, sometimes forcing the user to make a payment to regain access
3. Breaking essential system components and rendering a device inoperable

5.2 Spam

Spam is sent by a "spammer," a company in the business of distributing unsolicited email. The Spammer and the advertiser sign an agreement wherein the spammer produces mails and sends. 10,000spam recipients advertise spam for less than $100 which is less than postal mailing which requires a few thousand dollars.

5.3 Phishing

1. The process of phishing involves the following steps:
2. Planning: Phishers decide which business to target and determine how to get e-mail addresses for the customers of that business.
3. Setup: They create methods for delivering the message and collecting data involving web pages and email addresses
4. Attack: From a reputable source message is sent by the phisher.
5. Collection: The victims information are entered into web pages or popup windows
6. Identity Theft: The information is used for illegal activities and fraud.

5.4 Hacking

Hackers mainly depend upon the computer code which is their main resource with their own ingenuity. A small number of hackers actually program code though there are large numbers of hackers; they seek for codes written by other people. There are many program hackers which explore computer and networks and create programs to exploit. A skilled hacker knows how the individual or an organisation can be hacked with the help of either phishing, spam or by spreading malicious malware.

5.5 Cyber stalking

Cyber stalking works as stalking in the physical world. Many offenders combine their online activities with more traditional forms of stalking and harassment such as telephoning the victim and going to the victim's home. Some cyber stalkers obtain victims over the Internet and others put personal information about their victims online, encouraging others to contact the victim, or even harm them. They want to create fear among victims.

5.6 Cyber terrorism

Certain people exploit vulnerabilities within hardware, software as well as internet in malicious manner. Computers that are connected to a network help to speed up the process of cyber terrorism with more efficiency. With the help of the internet service provider unknowingly cyber terrorism takes up a high.

VI. Causes of Cyber Crime

Cyber Security is the process of protecting a network, computer programs, protect data from damage, or unauthorized access.

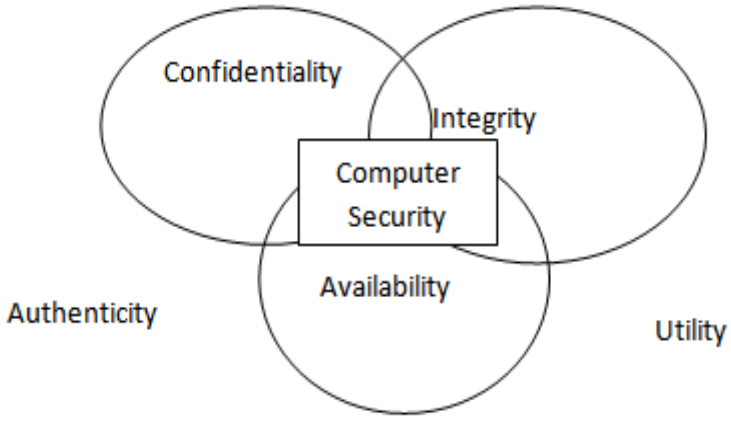

Fig 6.1 Elements of cyber security

There are three elements of cyber security confidentiality, integrity, and availability.

1. **Confidentiality:** There is a need to keep information secret from third parties that want to access to it, so just the right people can access it.
2. **Integrity**: Integrity is nothing but maintaining the accuracy and consistence of data over its life cycle. Data must not be changed and actions should be taken to ensure that data is not altered of accessed by unauthorized people.

3. **Availablity**: It is ensured by maintaining all hardware and also repairing hardware immediately whenever needed. It can access to data when it is needed, as such the information has value only if the authorized people can access at right time.

6.1 Security Methods

Following are the security methods from keeping data and system secure from virus and cybercrime:

6.1.1 Anti-virus

Do not install multiple anti-virus program at same time. Installing multiple anti-virus at a time may cause your computer to run very slow or it may crash. Install only one anti-virus at a time and keep it updated.

Make sure that your installed anti-virus program allows you to install new updates. Many tools are pre-installed on a new computer system needs paid registrations and at certain point these tools will stop working or stop getting new updates.There is need to make insure that the anti-virus software gets automatically updated itself regularly. Everyday new viruses are written and get spread through different ways.Never disable your anti-virus if you are installing any cracked software or game. When anti-virus is enabled it will delete some files of that software and that software will stop running. Disabling anti-virus may cause to crash of system or due to some virus your hard disk may get corrupt.

6.1.2 Firewall

A firewall is first program in a computer system and most important program, because firewall sees incoming data from internet. firewall keeps track on the outgoing information like a security guard. Firewall decides which data can enter into system and which data can leave the system. Firewall defends against untrusted connections from internet and from local networks, either it can give a clear path to viruses and hackers to enter into computer.

6**.1.3 Spam**:

The following are key points to prevent from spam:

1. **Watch out for social networking spam**:

As there is increasing popularity of social networking among people, there is also increase in social networking SPAM every month. There are various engineering techniques which are making very difficult to distinguish between legitimate and fraudulent emails.

2. **Responding to Spam emails**:

If you receive a spam email or message, never respond to those email/messages. Instead responding spam message delete it or you can report the message to your anti-spam supplier.

3. **Don't click on untrusted links:**

Never click on links that you receive from any unknown source or people. Sending malicious emails through any attachments and links is one of the primary tools of frauds portfolio. It is very easy for frauds to generate a mail with fake attachments and forward it. After clicking on such links, personal details like bank account number are asked. Never give such personal details on untrusted mails.

4. **Keep Your Software And Operating System Updated**:

Even if you have a good security installed on your computer, it will protect computer if it is not updated. By updating operating system time to time it can give very good security from viruses and hackers and updated OS and software can eliminate bugs. Make sure that auto update is on. Try to avoid use 0f cracked operating system.

6.1.4 Phishing:

5. Be aware of emails asking for personal/confidential information specially debit card number or mobile number. Legitimate organisations never ask personal information through emails. They will directly contact you for information.
6. Make sure that you are familiar with websites privacy policy. Do not trust on unfamiliar websites, keep watch on generic looking websites.
7. Make sure that you have installed effective software or anti-virus program that prevents you from fake websites and blocks that websites.
8. Do use an SSL certificate to secure traffic to and from your website.

6.1.5 Cyber Stalking:

Following are methods to prevent from cyber stalking:

1. Always log out of computer programs when you are done working with them and use screen saver with a strong password.
2. Keep a strong password to computer or keep password during booting time of machine, it will be more secure.
3. Never share your password with unknown person.
4. Try to change password frequently.
5. If you find suspect that some unauthorized person is using spyware software shutdown your computer, try to contact nearest cybercrime cell.

6.1.6 Hacking

Update your Operating system and other software time to time. The operated system keeps hackers away through performing crime outdated programs. Extra protection of computer system enables all Microsoft product updates so that the Office Suite will be updated at the same time. Consider retiring particularly susceptible software such as Java. Download up-to-date security programs, including antivirus and anti-malware software, anti-spyware, and a firewall. Do not keep sensitive data on cloud. They are very less clouds that provide high security to data. If the data such as photos is no more important, then store on cloud. Don't store financial documents or personal information in cloud.

Conclusion

It can be seen that computer security is a continuous battle, as hackers are getting smarter day by day also there is growing importance for security. No one ever said that this was going to be easy. There are lot of cyber crime victims who refuse to report petty crimes, because they feel what they have lost are not big loss and they ignore it. Computer crime should be stopped; complaints should be reported against it.

References

[1]. Steven Malby, Robyn Mace, Anika Holterhof, Comprehensive Study on Cybercrime draft by united nation, feb 2013
[2]. NS Safa, R Von Solms, An information security knowledge sharing model in organizations, Computers in Human Behavior, Elsevier 2016
[3]. Ammar Yassir and Smitha Nayak, Cyber Crime: A threat to Network Security, IJCSNS International Journal of Computer Science and Network Security, VOL.12 No.2, February 2012
[4]. Jacob, G., Filiol, E., Debar, H.: Formalization of viruses and malware through process algebras, International Conference on Availability, Reliability and Security (ARES 2010). IEEE 2010.
[5]. Sunakshi Maghu, Siddharth Sehra ,Avdesh Bhardawaj," Inside of Cyber Crimes and Information Security: Threats and Solutions", International Journal of Information & Computation Technology, ISSN 0974-2239 Volume 4, Number 8, 2015
[6]. Shilpa Yadhav, Tanushree , " Cyber Crime and security", International Journal of Scientific & Engineering Research, Volume 4, Issue 8, August-2013.
[7]. Ammar Yassir and Smitha Nayak," Cybercrime: A threat to Network Security", International Journal of Computer Science and Network Security, VOL.12 No.2, February 2012

IOSR Journal of Computer Engineering (IOSR-JCE) is UGC approved Journal with Sl. No. 5019, Journal no. 49102.

Hardik Runwal."A Survey on: Cyber Crime & Information Security." IOSR Journal of Computer Engineering (IOSR-JCE) 20.1 (2018): 30-34.