International Journal of Computing and Network Technology
ISSN (2210-1519)
Int. J. Com. Net. Tech.6, No1. (Jan-2018)

http://dx-doi.org/10.12785/ijcnt/060103

Cyber Crime- Techniques, Prevention and Cyber Insurance

Saba Shoukat[1] and Adil Bashir[2]

[1]Jammu & Kashmir Bank Ltd. Srinagar, Jammu and Kashmir, India
[2]Electronics and Communication Engineering, NIT Srinagar, Jammu & Kashmir, India

Received: 20 may Oct. 2017, Revised: 15 Dec., 2017, Accepted: 21 Dec., 2017, Published: (1 Jan. 2018)

Abstract: Rapid technological advancements are changing our day-to-day lives. Technology has improved the way people think, act and respond. Presently, with the growth of digital revolution, everyone is reliant on information technology. Banks are using information technology that is built by the most intelligent brains and at the same time there are folks who are equally intelligent with technical knowledge but use their intelligence negatively and end up in performing unethical tasks. The intention of such kind of folks is to harm people by their unethical activities. With digital revolution, these criminals need not to commit the crime physically; rather they can reach every corner of the world virtually using a computer, internet and communication medium. By deciphering encrypted information, they can rob anything using computers, be it money or credit card details of an individual or data. This paper presents different types of cybercrimes like cyber extortion, cyber stalking etc. It also highlights the various techniques that are used by criminals in order to launch attacks and breach security of an organization, thus committing cyber-crimes. Also, the counter measures against cyber-crimes are presented.

Keywords: Cyber crime, cyber insurance, Malware, Hacking, Spyware.

1. Introduction

In today's world, every organization depends on cyberspace to carry out their business activities. With the development of cost effective information and communication technologies, even common man utilizes cyberspace for his day to day activities. As people are more dependent on internet in today's world as a result of which the personal lives of individuals, their friends and family are available in today's social websites like twitter, facebook etc. However taking the advantage of such type of present changing scenario cyber criminals are utilizing it as a source of income. People, from kids, for games, to teenagers, for educational activities and adults all depend on digital technology to make life simpler and more productive. Almost every aspect of life has become digital be it bank transactions or product purchase, unfortunately, this also makes hotspot for criminal activity who utilize this latest technology either for fun, greed, power, revenge, publicity, adventure, desire to access personal information or destructive purposes [1]. In modern world, cyber criminals are the most dangerous type of criminals.

Cyber-crime is defined as the ways in which computers and other types of portable electronic devices, such as cell phones and PDAs that aid connectivity to the internet can be used to break laws and cause harm. Therefore it is an unlawful act in which computer is used either a tool to commit real world crime or a target to steal information or affect the system with viruses or both. First Cybercrime was recorded in 1820 [5, 6]. That was when people used the calculating machines for wrong purposes. This study will enlighten different aspects of cybercrime, its types and preventions with special focus on cyber insurance.

2. TYPES OF CYBER CRIMES

This section presents different types of cyber-crimes that are used by malicious users to harm the organization or any individual [2,7].

A. Cyber Stalking and Harassment

This is the new form of cyber-crime where the online activities of a person are gathered that includes private and vital information which is later used by cyber-criminal to harass him/her. Most victims of this crime are women who are stalked by men and children who are stalked by adult predators. Cyber stalkers harass their victims via email, chat rooms, websites etc.

E-mail address: sabashoukat323@gmail.com, adilbashir.445@gmail.com

B. *Intellectual Property Crime*

Intellectual property means ownership of rights related to software, copyright, trademark etc. When these rights are violated or deprived either partially or completely its said to be an intellectual property right violation. We can also say that any unlawful act which deprives its owner partially or completely of his rights is a crime for example software piracy, infringement of copyright, trademark, patents, designs etc.

C. *Phishing*

It's a technique used by cybercriminals to steal confidential information such as credit card details, username password, PIN, bank account numbers, personal details etc. Phishing is typically done by email spoofing which means using fake emails requesting the user to enter these details [8].

D. *Cyber Defamation*

Defamation is to lower the image of a person or to harm his reputation. To do such kind of act using virtual medium is called as cyber defamation. It can be done by hacking a mail account and sending mails using abusive or vulgar language to unknown or known persons mail account.

E. *Cyber Vandalism*

Vandalism means destroying or damaging property of another individual or organization illegally. Cyber vandalism includes destroying the data or information stored in computer or cloud server. It simply means online deleting, altering or adding content to someone else's content in a malicious manner.

F. *Hacking*

Hacking is one of the major threats that exists in today's world and numerous people and organizations have suffered huge economic and social losses due to this threat. Hacking incidents are increasing at an alarming rate. Hackers are grouped into black-hat hackers who carry their operations illegally, white-hat hackers who are ethical hackers and are hired by an organization on contractual basis to check vulnerabilities of computer system, grey-hat hackers act to improve systems and network security. They breach the security weakness of the system without permission to highlight that weakness to their owners and blue-hat hackers are outside computer security consulting firms. Other types of hackers include Script Kiddies, Elite Hackers, Hacktivists and Phreakers.

G. *Cyber Extortion*

It includes stealing of private or personal information and threatening to release it to public with the demand for money to avert or stop the attack.

H. *Cyber Terrorism*

It is an act of terror committed electronically against individuals, businesses, organizations, and against the government itself. For instance, a simple email propagating that there will be a bomb attack can be considered as cyber terrorism.

I. *Password Sniffing*

It's a technique used by cyber criminals to crack user passwords. Password sniffers are programs used by cybercriminals to monitor and record the name and password of network users as they login at site.

J. *Denial of Service Attacks*

It's an attempt to make system or network unavailable to its users either temporarily or permanently. It occurs when computer is flooded with more requests than it can handle. Systems can hang because of this type of attack. Usually target sites are sites hosted by banks, credit card payment gateways etc.

K. *Virus Attacks*

Virus is self-replicating program, which affect other programs and systems. Viruses can spread through emails which are framed in such a way that it persuades the victim to open the attachment of email. By opening the attachment virus is launched and systems get infected. These viruses thus hamper the functioning of computers by slowing down the network.

L. *Trojan Horse*

A program that infects the system and allows the hackers to take control of the system. Trojan is used as an application to steal data from computers. Trojan Horses are common technique for planting other problems in computers including viruses, worms, logic bombs and salami attacks. These are generally spread through email attachments.

M. *Child Pornography*

It involves the use of internet to create, distribute or access materials that sexually exploit under-age children.

N. *Data Diddling*

It is one of the oldest and simplest methods of computer related crimes. It involves changing the data before or during entry into computer system and then changing it back after processing is done. It can be carried electronically through virus.

3. TECHNIQUES FOR LAUNCHING CYBER ATTACKS

There are various techniques used by cyber criminals through several channels to launch cyber-crimes. Some of the techniques include:

A. *Dumpster Diving*

The technique in which personal information of an individual or an organization is collected by scanning or searching through their trash and the information thus collected is used to carry out a cyber-attack on computer networks. Such type of data are usually written on CDS, sticky notes, etc. and crushed and thrown in the bins.

B. *Eavesdropping*

An unauthorized interception of private communication channels to listen to the exchanged traffic and later using it for unauthorized and illegal purposes.

C. *Denial of Services*

This technique is employed to stop the system or website from functioning either temporarily or permanently. Usually web servers of high profile organizations like banks, media, Government, etc. are targeted. This attack results in financial loss of an organization or individual.

D. *Phishing*

A technique used to steal personal and financial data. It is a hybrid technique as it involves both use of technological means and social engineering and typically carried by email from the fake websites which appear identical to the legitimate one and directs the user to enter the personal information.

E. *Trap Doors*

Also known as back door as it provides a secret way of gaining access to an application or system or data. Hacker often plants a backdoor on systems to gain access later.

F. *Session Hijacking*

Exploitation of valid computer session of a victim to gain unauthorized access to information or data in a system. For session hijacking session of the victim should be active otherwise he cannot gain the access to the system.

G. *Malware*

Software designed for malicious purpose to damage or gain an unauthorized access to computer system. This software when installed on the system performs unwanted tasks for benefit to the hacker. It includes viruses, worms, Trojans etc.

H. *Spyware*

It is a type of malware that collects information about users without their knowledge. It's difficult to detect its presence and gets installed through pop-up advertisements.

4. PREVENTION METHODS AGAINST CYBER CRIME

To safeguard individuals and organizations day-to-day activities over internet, several mechanisms can be used to protect personal and private information to be known to malicious users. This can be done in various ways detailed below [3, 4]:

- Treat confidential information as confidential.
- Never reveal sensitive data on the internet.
- Have strong firewall installed on your system.
- Never write your passwords. Memorize them.
- Ensure to change password every 3 months.
- Antivirus scan must be done regularly.
- Type the URL of bank rather clicking links.
- Look for padlock sign on the browsers toolbar.
- Never open attachments in your mail unless you are sure of the sender.
- Never respond to badly written email.
- Keep your card details like card number and CVV confidential.
- Never allow anybody else to use your card.
- Choose strong password.
- Never buy from sites you don't trust.
- Make passwords complicated using special characters, upper and lower case and numbers.
- Make sure that your system is configured securely.
- Ignore Pop Ups.
- Taught children about child pornography crime and how to avoid that.

Though there are so many legal ways to protect cyber-crime, an effective provision has to be made and has to be implemented.

5. CYBER INSURANCE

It is an insurance product used to protect businesses and individual users from Internet based risks. Coverage provided by cyber-insurance policies may include first party coverage against losses such as data destruction, extortion, theft, hacking and denial of service attacks, liability coverage compensating companies for losses including regular security-audit, post-incident public relations and investigative expenses and criminal reward funds. Cyber insurance is beneficial in the event of large scale security incident. Cyber insurance is a risk management technique in which network user risks are transferred to an insurance company in return for a fee i.e. insurance premium.

6. CONCLUSION

With the advancement in communication and information technology, cybercriminals are gaining more opportunities to commit the cybercrime. Cyber criminals are technocrats with technical skills who use various methods to create harm to individuals or organizations private information. Protection of cyber-crime is the major concern as anybody can be the victim of cybercrime and in just a moment of time it can lead an individual or an organization to suffer the losses. It's also a big threat to human life. With growing technology cyber criminals have everything they need in their lap. Cyber techniques have been improved over time and with rise in technology and cybercrime there is need to conduct research analysis of cybercrimes to find the best ways to protect sensitive data and take appropriate steps against cyber-attack. Awareness among people is also very important. People should also realize the need to report any type of cybercrime that has occurred, unless they report, such type of crimes will continue.

References

[1] Cyber crime and fraud management by IIBF, Macmillan India Ltd, 2014. ISBN-13: 978-9350593028.

[2] Alpna and Dr Sona Malhotra , Cyber Crime –Its types, analysis and prevention techniques, International Journal of Advanced Research in Computer Science and Software Engineering. vol 6, issue 5, 2016.

[3] M. L. Prasanthi and T. A. S. K. Ishwarya, Cyber Crime-Prevention & Detection, International journal of advanced research in computer and communication engineering. vol 4, issue 3, 2015.

[4] V. Kandpal, Latest face of cybercrime and its prevention in india, International Journal of Science, Technollogy and Management, Volume 6, Issue 4, 2017.

[5] Cyber Crime survey report, KPMG, India. 2014.

[6] http://criminal.findlaw.com/criminal-charges/computer-crime.html

[7] http://study.com/academy/lesson/what-is-computer-security-definition-basics.html

[8] https://www.us-cert.gov/report-phishing

Saba Shoukat received her Bachelor of Technology (B.Tech) in Electronics and Communication Engineering from Islamic University of Science and Technology, Jammu & Kashmir, India in year 2011. She has done Cisco Certified Network Associate (CCNA) and is currently working in Jammu and Kashmir Bank as Relationship Executive. Her research interests are Cyber Security, Embedded Systems and Wireless Communication.

Adil Bashir received his Bachelor of Technology (B.Tech) in Computer Science and Engineering from Islamic University of Science and Technology, Jammu & Kashmir, India in year 2011. He has done his Master of Technology (M.Tech) in Communication and Information Technology from National Institute of Technology (NIT) Srinagar, India in 2013. Presently he is a research scholar at NIT Srinagar in the Department of Electronics and Communication. His research interests are Internet of Things, Wireless Sensor Networks, Embedded Systems and Network Security.