ISSN No. 0976-5697

Volume 8, No. 5, May – June 2017

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

A Review on Cyber Crime: Major Threats and Solutions

Amit Wadhwa
Asst. Professor, Department of Computer Science & Engineering
Amity University Haryana,
Gurgaon, India

Neerja Arora
Asst. Professor, Department of Computer Science & Engineering
KIIT Group of Colleges
Gurgaon, India

Abstract: Crime is a common word that we always heard in this globalization era. Crimes refer to any violation of law or the commission of an act forbidden by law. Over the past two decades, cybercrime has become an increasingly widely debated topic across many walks of life. It’s clear that rapid growth of the internet has created unprecedented new opportunities for offending. It is defined as crimes committed on the internet using the computer as either a tool or a targeted victim. This paper presents the types of Cybercrime Activities, important issues on the Security, Prevention, and Detection of Cyber Crime.

Keywords: Cybercrime, Crimeware, Trojan, Spyware, Threat Exchange

I. Introduction

Crime and criminality have been associated with man since long time ago. There are different strategies used by different countries to contend with crime. It is depending on their extent and nature. These developments present serious challenges for law and criminal justice, as it struggles to adapt to crimes that no longer takes place in the terrestrial world but in the virtual environment of cyberspace, which span the globe through the Internet’s instantaneous communication, and afford offenders new possibilities for anonymity, deception and disguise. In our daily life, economic activities, and national security highly depend on stability, safely, and resilient cyberspace. A network brings communications and transports, power to our homes, run our economy, and provide government with various services [1]. However, it is through the same cyber networks which intrude and attack our privacy, economy, social life in a way which is harmful.

Cyber crime is also known as computer crime that refers to any crime that involves a computer and a network. It is an attack on information about individuals, corporations, or governments. Although the attacks do not take place on a physical body, they do take place on the personal or corporate virtual body, which is the set of informational attributes that define people and institutions on the Internet. Computer can be considered as a tool in cyber crime when the individual is the main target of cyber-crime [2]. In addition, cyber crime also includes traditional crimes that been conducted with the access of Internet. For example, telemarketing Internet fraud, identity theft, and credit card account thefts. In simple words, cybercrime can be defined as any violence action that been conducted by using computer or other devices with the access of internet. This action can give harmful effects to other.

Cybercrime: The facts

- Cybercrime has now surpassed illegal drug trafficking as a criminal moneymaker.
- Somebody’s identity is stolen every 3 seconds as a result of cybercrime.
- Without a sophisticated security package, your unprotected PC can become infected within four minutes of connecting to the Internet.

II. Types of Cybercrime Activities

Cybercrime ranges across a spectrum of activities. At one end, are crimes that involve fundamental breaches of personal or corporate privacy, such as assaults on the integrity of information held in digital depositories and the use of illegally obtained digital information to blackmail a firm or an individual. At the other end of the spectrum are those crimes that involve attempts to disrupt the actual workings of the Internet. These ranges from spam, hacking, and denial of service attacks against specific sites to acts of cyberterrorism—that is, the use of the Internet to cause public disturbances and even death.

Criminals committing cybercrime use number of methods, depending on their skill-set and their goal. Here are some of the different ways cybercrime can take shape:

- Theft of personal data
- Copyright infringement
- Fraud
- Child pornography
- Cyberstalking
- Bullying

The broad range of cybercrime can be better understood by dividing them into two categories, which are Type I and Type II cybercrime, as described below:

A. *Type 1 Cybercrime:*

- Usually a single event from the perspective of the victim. An example would be where the victim unknowingly downloads a Trojan horse virus, which installs a keystroke logger on his or her machine. The keystroke logger allows the hacker to steal private data such as internet banking and email passwords.

- Another common form of Type 1 cybercrime is phishing. This is where the victim receives a supposedly legitimate email (quite often claiming to be a bank or credit card company) with a link that leads to a hostile website [3]. Once the link is clicked, the PC can then be infected with a virus.
- Hackers often carry out Type 1 cybercrime by taking advantage of flaws in a web browser to place a Trojan horse virus onto the unprotected victim's computer.
- Any cybercrime that relates to theft or manipulation of data or services via hacking or viruses, identity theft, and bank or e-commerce fraud.

B. Type 2 Cybercrime:

- They tend to be much more serious and covers things such as cyberstalking and harassment, child predation, extortion, blackmail, stock market manipulation, complex corporate espionage, and planning or carrying out terrorist activities.
- It is generally an on-going series of events, involving repeated interactions with the target. For example, the target is contacted in a chat room by someone who, over time, attempts to establish a relationship. Eventually, the criminal exploits the relationship to commit a crime.
- More often it is facilitated by programs that do not fit under the classification crimeware [4]. For example, conversations may take place using IM (instant messaging) clients or files may be transferred using FTP.

III. TOOLS USED IN CYBERCRIME

The software tools used in cybercrime are sometime referred to as *crimeware*. Crimeware is a software that is:

- used in the commission of the criminal act
- not generally regarded as a desirable software or hardware application
- not involuntarily enabling the crime

Like cybercrime itself, the term crimeware covers a wide range of different malicious, or potentially malicious software.

A. Crimeware: Bots

"Bot" term is short for robot – are one of the most sophisticated types of crimeware facing the Internet today. Bots are like worms and Trojans, but earn their unique name by performing a wide variety of automated tasks on behalf of their master (the cybercriminals) who are often safely located somewhere far across the Internet. Tasks that bots can perform run the gamut from sending spam to blasting Web sites off the Internet as part of a coordinated "denial-of-service" attack. Bots sneak onto a person's computer in many ways. Bots oftentimes spread themselves across the Internet by searching for vulnerable, unprotected computers to infect [5]. When they find an exposed computer, they quickly infect the machine and then report back to their master.

Their goal is then to stay hidden until they are awoken by their master to perform a task. Bots are so quiet that sometimes the victims first learn of them when their Internet Service Provider tells them that their computer has been spamming other Internet users [6]**.** Bots do not work alone, but are part of a network of infected machines called a "botnet." Botnets are created by attackers repeatedly infecting victim computers using one or several of the techniques mentioned above.

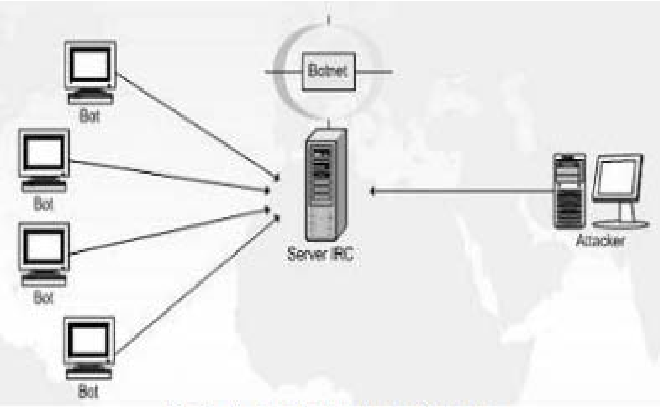

Fig. 1 A sample structure of botnets

B. Crimeware: Trojans and Spyware

Trojan horse and spyware are the two of the most popular methods used by cybercriminals.

1) Trojan Horse: A Trojan horse program presents itself as a useful computer program, while it actually causes havoc and damage to your computer. Increasingly, Trojans are the first stage of an attack and their primary purpose is to stay hidden while downloading and installing a stronger threat such as a bot. Unlike viruses and worms, Trojan horses cannot spread by themselves [7]. They are often delivered to a victim through an email message where it masquerades as an image or joke, or by a malicious website, which installs the Trojan horse on a computer through vulnerabilities in web browser. After it is installed, the Trojan horse lurks silently on the infected machine, invisibly carrying out its misdeeds, such as downloading spyware, while the victim continues with their normal activities.

2) Spyware: Spyware is a general term used for programs that covertly monitor your activity on your computer, gathering personal information, such as usernames, passwords, account numbers, files, and even driver's license or social security numbers. Some spyware focuses on monitoring a person's Internet behaviour; this type of spyware often tracks the places you visit and things you do on the web, the emails you write and receive, as well as your Instant Messaging (IM) conversations [8-9]. After gathering this information, the spyware then transmits that information to another computer, usually for advertising purposes. Spyware is similar to a Trojan horse in that users unknowingly install the product when they install something else. However, while this software is almost always unwelcome, it can be used in some instances for monitoring in conjunction with an investigation and in accordance with organizational policy.

Spyware is installed in many ways:

- Most often spyware is installed unknowingly with some other software that you intentionally install [10]. For example, if you install a "free" music or file sharing service or download a screensaver, it may also install spyware. Some Web pages will attempt to install spyware when you visit their page.

- A person who wants to monitor your online activities may also manually install spyware. Depending on how this is done, this might be acceptable surveillance of an individual or an unwelcome, even illegal, invasion of privacy [11].

IV. IMPORTANCE OF CYBERSECURITY IN CYBERCRIMES

Everyday criminals are invading countless homes and offices across the nation-not by breaking down windows and doors, but by breaking into laptops, personal computers and wireless devices via hacks and bits of malicious code.

A. The collective impact is staggering

Billions of dollars are lost every year repairing systems hit by such attacks. Some take down vital systems, disrupting and sometimes disabling the work of hospitals, banks, and 9-1-1 services around the country**.**

B. Who is behind such attacks?

It runs the gamut—from computer geeks looking for bragging rights…to businesses trying to gain an upper hand in the marketplace by hacking competitor websites, from rings of criminals wanting to steal your personal information and sell it on black markets…to spies and terrorists looking to rob our nation of vital information or launch cyber strikes. Today, these computer intrusion cases—counterterrorism, counterintelligence, and criminal—are the paramount priorities of our cyber program because of their potential relationship to national security.

Cybersecurity is the body of technologies, processes and practices designed to protect networks, digital equipment, information and services from unintended or unauthorized access, change or destruction. In a computing context, the term security implies cybersecurity [11]. Cybersecurity is the process of applying security measures to ensure confidentiality, integrity, and availability of data. It attempts to assure the protection of assets, which includes data, desktops, servers, buildings, and most importantly, humans.

The goal of cybersecurity is to protect data both in transit and at rest. Countermeasures can be put in place thereby increasing the security of data. Some of these measures include, but are not limited to, access control, awareness training, audit and accountability, risk assessment, penetration testing, vulnerability management, security assessment and authorization.

C. Types of computer security - an overview

Types of computer security risks include virus, spyware, and malware. To help you understand types of computer security, entire theory has been divided into the following three parts:

- Internet and Network Security
- Standalone Computer Security
- Data Loss by Accidents

Internet Security is the one most people are concerned with as it deals with malware and hackers. The Network Security, deals with the security problems on networks of any size. This includes external problems as well as problems from users of computers inside the network. Standalone computers refer to computers that are not connected to any network (but may be connected to Internet). This part will cover the possible security vulnerabilities on such systems [12]. Finally, the Data Loss part is applicable to networks and computers in the networks as well as standalone computers.

V. THE CONCEPT OF CYBER PREVENTION AND DETECTION

The mantra of any good security engineer is: 'Security is a not a product, but a process.' It's more than designing strong cryptography into a system; it's designing the entire system such that all security measures, including cryptography, work together.

A state of computer "security" is the conceptual idea, attained by use of three processes: threat prevention, detection, and response [13]. These processes are based on various policies and system components, which include the following:

- User account access controls and cryptography can protect systems files and data, respectively.
- Firewalls are by far the most common prevention systems from a network security perspective as they can (if properly configured) shield access to internal network services, and block certain kinds of attacks through packet filtering.
- Intrusion Detection Systems (IDSs) are designed to detect network attacks in progress and assist in post-attack forensics, while audit trails and logs serve a similar function for individual systems.
- "Response" is necessarily defined by the assessed security requirements of an individual system and may cover the range from simple upgrade of protections to notification of legal authorities, counter-attacks, and the like.

Prevention Tips

Cybercrime prevention can be straight-forward - when armed with a little technical advice and common sense, many attacks can be avoided. The tips below provide basic information on how you can prevent online fraud:

A. Keep your computer current with the latest patches and updates

By regularly updating your computer with patches and other software fixes, you block attackers from being able to take advantage of software flaws (vulnerabilities) that they could otherwise use to break into your system [13]. Taking advantage of "auto-update" features in your software is a great start toward keeping yourself safe online.

B. Make sure your computer is configured securely

Configuring popular Internet applications such as your Web browser and email software is one of the most important areas to focus on.

C. Choose strong passwords and keep them safe

Passwords are a fact of life on the Internet today—we use them for everything. The following tips can help make your online experiences secure:

- Strong passwords have eight characters or more and use a combination of letters, numbers and symbols (e.g. # $ % ! ?)
- Avoid using any of the following as your password: your login name, anything based on your personal information such as your last name, and words that can be found in the dictionary. Try to select especially strong, unique passwords for protecting activities like online banking.
- Keep your passwords in a safe place and try not to use the same password for every service you use online.
- Change passwords on a regular basis, at least every 90 days.

D. Protect your computer with security software

Several types of security software are necessary for basic online security, that include firewall and antivirus programs [13]. Integrated security suites such as Norton Internet Security combine firewall, antivirus, antispyware with other features such as antispam and parental controls have become popular as they offer all the security software needed for online protection in a single package.

E. Protect your personal information

To take advantage of many online services, you will inevitably have to provide personal information to handle billing and shipping of purchased goods. Since not divulging any personal information is rarely possible, the following list contains some advice for how to share personal information safely online:

- Keep an eye out for phony email messages.
- Don't respond to email messages that ask for personal information.
- Steer clear of fraudulent Web sites used to steal personal information.
- Pay attention to privacy policies on Web sites and in software.
- Guard your email address.

F. Review bank and credit card statements regularly

One of the easiest ways to get the tip-off that something has gone wrong is by reviewing the monthly statements provided by your bank and credit card companies for anything out of the ordinary.

VI. WHAT TO DO IF YOU ARE A VICTIM?

There is a nonstop flood of Trojans, bots, and phishing attacks assaulting the Internet everyday-infections and identity thefts can happen to anyone. If you believe you have been a victim of online fraud or crimeware, there are a series of steps you can take in to respond to and recover from the incident:

- Disconnect immediately. Unplug the network cable, phone, or cable line from your machine. This can prevent data from being leaked back to the attacker.
- Scan your computer with an up-to-date antivirus program such as Norton Antivirus or Norton Internet Security (a complete security software suite).
- Back up your critical information. Sensitive data may be leaked by crimeware and it also may be inadvertently destroyed or lost during the clean-up effort. If you have back-up software installed, make a copy of your valuable files.
- Consider going back to ground-zero by re-installing the operating system of your computer (e.g. Microsoft Windows) or using back-up software.
- Close affected accounts immediately and File a police report.
- Set up a fraud alert with the 3 national consumer reporting agencies (Equifax, Experian, TransUnion).
- Contact government agencies. If your driver's license or social security number have been stolen.

VII. COMBATING THE THREATS

In recent years, we’ve built a whole new set of technological and investigative capabilities and partnerships—so we’re as comfortable chasing outlaws in cyberspace as we are down back alleys and across continents. That includes:

- A Cyber Division at FBI Headquarters “to address cyber crime in a coordinated and cohesive manner”.
- Specially trained cyber squads at FBI headquarters and in each of our 56 field offices, staffed with “agents and analysts who protect against investigate computer intrusions, theft of intellectual property and personal information, child pornography and exploitation, and online fraud”.
- New Cyber Action Teams that “travel around the world on a moment’s notice to assist in computer intrusion cases” and that “gather vital intelligence that helps us identify the cyber crimes that are most dangerous to our national security and to our economy”.
- Our 93 Computer Crimes Task Forces nationwide that “combine state-of-the-art technology and the resources of our federal, state, and local counterparts”.
- A growing partnership with other federal agencies, including the Department of Defense, the Department of Homeland Security, and others—which share similar concerns and resolve in combating cyber crime.

VIII. RECENT TRENDS IN SECURITY

A. Windows Hello Waves Off Passwords

A new feature in Windows 10 addresses a common frustration among gadget lovers: the inconvenience and insecurity of passwords. A biometric system like Windows Hello has security and usability advantages over conventional passwords. The security advantages come from the asymmetric cryptography where the only secrets are stored on the user's device and not in the cloud. This protects users from losing authentication credentials if a service they use is ever breached by an adversary because there are no credentials or secrets stored on a server. Biometric authentication has been growing in popularity in the mobile phone arena, where fingerprint scanners are built into some popular phone models. It's less popular on the desktop, though, where scanners need to be purchased separately [14]. The inclusion of facial and iris recognition in Windows may boost the popularity of biometric authentication on computing devices.

B. No Need to Waste Brain Space on Yahoo Passwords

Yahoo has given users an alternative to remembering passwords for their email accounts, rather than promoting the two-factor authentication system it already had in place [14]. The new system, which sends verification codes to phones and then supplies an on-demand password upon the code's entry, makes it easier for hackers to break in.

Advantages of Two-Factor Authentication

Two-factor authentication uses two different components in combination to authenticate an individual. Those components could be something the user knows, something the user possesses, or something inseparable from the user.

Take, for example, the humble ATM machine. Withdrawing cash from it requires a combination of something the user possesses -- a bank card -- and something the user knows -- the PIN. Two-factor authentication has been touted as a good way to secure accounts. Banks for some time have been criticized for not moving fast enough on 2FA.

C. Facebook Launches ThreatExchange to Stymie Cybercrime

The launch of Facebook ThreatExchange "is about Facebook being one of the larger threat vectors for phishing attacks and looking to share this threat information so companies can be aware and be proactive to prevent cybercriminals using its platform as the threat du jure". Facebook has announced ThreatExchange, an API-based platform for technology companies to share information on security threats. It had been working on the platform for about a year, with Pinterest, Tumblr, Yahoo and Twitter. Bitly and Dropbox recently joined in. ThreatExchange is based on Facebook's ThreatData threat analysis framework. Facebook layered APIs on top of the existing Facebook platform infrastructure so participants can query the available information and control which other participants they publish their information to, using a predefined set of data fields.

IX. CONCLUSION

Cybercrime, also called as computer crime, is the use of a computer as an instrument to perform illegal tasks, such as committing fraud, trafficking in child pornography and intellectual property has grown in importance as the computer has become central to commerce, entertainment, and government. There are common-sense steps that can prevent or reduce having one's financial information stolen online, as well as to avoid other scams and threats, but cybercrime in these areas persists largely due to a lack of consumer education.

In this paper the concept of cybercrime and it its various types have been studied. Further we discussed some tools to be used for cybercrime all over the world. Finally, it concluded with various techniques to be used to detect and recover from cyberattacks.

REFERENCES

[1] Ammar Yassir and Smitha Nayak, “Cybercrime: A threat to Network Security”, IJCSNS International Journal of Computer Science and Network Security, VOL.12 No.2, February 2012, pp-84-88.

[2] Er. Harpreet Singh Dalla and Ms. Geeta, “Cyber Crime A Threat to Persons, Property,Government and Societies”, International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 5, May 2013,pp-997-1002.

[3] Kusum Agroiya, Ritu Sharma and Dr. Mukesh Sharma, “Distributed Denial of Service(DDoS): Attacks and Defense Mechanism” , International Conference on Advanced Information Communication Technology and Engineering, 2013.

[4] P. Ferguson, “Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing. Technical report”, The Internet Society, 1998.

[5] Shuchi Juyal and Ruchika Prabhakar, “A comprehensive study of DDoS attacks and defense mechanism” , Journal of Information and operation management, Volume 3, Issue1, 2012, pp-29-33.

[6] Soumya Tiwari , Anshika Bhalla and Ritu Rawat, “Cyber Crime and Security”, International Journal of Advanced Research in Computer Science and Software Engineering, Volume 6, Issue 4, April 2016, pp-46-52.

[7] Wadhwa, A. and Garg, A., 2015. Studying and Analyzing Virtualization While Transition from Classical to Virtualized Data Center. International Journal of Computer Applications, 117(14), pp.10-14

[8] Shilpa yadav, Tanu shree and Yashika arora, “Cyber Crime and Security”, International Journal of Scientific & Engineering Research, Volume 4, Issue 8, August-2013, pp-855-861.

[9] Pooja Aggarwal , Neha, Piyush Arora and Poonam , “REVIEW ON CYBER CRIME AND SECURITY”, IJREAS, Vol. 02, Issue 01, Jan 2014.

[10] Seema Vijay Rane and Pankaj Anil Choudhary, “Cyber Crime and Cyber Law in India”, Cyber Times International Journal of Technology and Management, September 2012, Vol. 5 Issue 2.

[11] Amit Wadhwa and Dr. V. K. Gupta, “Framework for User Authenticity and Access Control Security over Cloud”. International Journal on Computer Science and Engineering (IJCSE), Vol 06, No. 04, April, 2014

[12] Ravi Sharma, “Study of Latest Emerging Trends on Cyber Security and its challenges to Society”, International Journal of Scientific & Engineering Research, June 2012 , ISSN 2229-5518, Volume 3, Issue 6, 1.

[13] Wadhwa, Amit. "Comprehensive Analysis of Security Issues and Solutions While Migrating to Cloud Environment." International Journal of New Innovations in Engineering and Technology 4.4 (2016)

[14] Sunakshi Maghu, Siddharth Sehra and 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 (2014), pp-835-840.