Cybercrime

Matheus Redecker[1]

[1]Pontifícia Universidade Católica do Rio Grande do Sul

matheus.redecker@acad.pucrs.br

1. Introduction

Every day, criminals are invading countless homes and offices across the world, not by breaking down windows and doors, but by breaking into laptops, personal computers, and wireless devices via hacks and bits of malicious code. Computer crime, or cybercrime, is crime that involves a computer and a network. The computer may have been used in the commission of a crime, or it may be the target. Debarati Halder and K. Jaishankar define cybercrimes as: ”Offences that are committed against individuals or groups of individuals with a criminal motive to intentionally harm the reputation of the victim or cause physical or mental harm, or loss, to the victim directly or indirectly, using modern telecommunication networks such as Internet (Chat rooms, emails, notice boards and groups) and mobile phones (SMS/MMS)”.

Such crimes may threaten a nation’s security and financial health. Issues surrounding these types of crimes have become high-profile, particularly those surrounding hacking, copyright infringement, child pornography, and child grooming. There are also problems of privacy when confidential information is intercepted or disclosed, lawfully or otherwise. Debarati Halder and K. Jaishankar further define cybercrime from the perspective of gender and defined ’cybercrime against women’ as ”Crimes targeted against women with a motive to intentionally harm the victim psychologically and physically, using modern telecommunication networks such as internet and mobile phones”. Internationally, both governmental and non-state actors engage in cybercrimes, including espionage, financial theft, and other cross-border crimes.

2. Cybercrime

Cybercrime is a fast-growing area of crime. More and more criminals are exploiting the speed, convenience and anonymity of the Internet to commit a diverse range of criminal activities that know no borders, either physical or virtual, cause serious harm and pose very real threats to victims worldwide.

Organised crime has been quick to take advantage of the opportunities offered by the Internet, particularly the growth in e-commerce and online banking. Specialist criminal groups target individuals, small businesses and large corporate networks to steal personal information in bulk in order to profit from the compromised data available to them. Common cyber threats for consumers and business are:

- Consumers;
- Phishing: bogus emails asking for security information and personal details;
- Webcam manager: where criminals takeover your webcam;
- File hijacker: where criminals hijack files and hold them to ransom;
- Keylogging: where criminals record what you type on your keyboard;

- Screenshot manager: allows criminals take screenshots of your computer screen;
- Ad clicker: allows a criminal to direct a victim's computer to click a specific link
- Business;
- Hacking information: allows a criminal to stole information of the company;
- Distributed Denial of Service (DDOS) attacks: allows a criminal to get down the website of the company.

2.1. Fraud and financial crimes

Computer fraud is any dishonest misrepresentation of fact intended to let another to do or refrain from doing something which causes loss. The fraud may be facilitated using computer systems, including bank fraud, carding, identity theft, extortion, and theft of classified information. A variety of internet scams, many based on phishing and social engineering, target consumers and businesses.

2.2. Cyber terrorism

Government officials and information technology security specialists have documented a significant increase in Internet problems and server scans since early 2001. But there is a growing concern among federal officials that such intrusions are part of an organized effort by cyber terrorists, foreign intelligence services, or other groups to map potential security holes in critical systems. A cyber terrorist is someone who intimidates or coerces a government or organization to advance his or her political or social objectives by launching a computer-based attack against computers, networks, or the information stored on them. Cyber terrorism in general, can be defined as an act of terrorism committed through the use of cyberspace or computer resources. As such, a simple propaganda in the Internet, that there will be bomb attacks during the holidays can be considered cyber terrorism. There are also hacking activities directed towards individuals, families, organized by groups within networks, tending to cause fear among people, demonstrate power, collecting information relevant for ruining peoples' lives, robberies, blackmailing etc.

2.3. Cyber extortion

Cyber extortion occurs when a website, e-mail server, or computer system is subjected to or threatened with repeated denial of service or other attacks by malicious hackers. These hackers demand money in return for promising to stop the attacks and to offer "protection". According to the Federal Bureau of Investigation, cyber extortionists are increasingly attacking corporate websites and networks, crippling their ability to operate and demanding payments to restore their service. More than 20 cases are reported each month to the FBI and many go unreported in order to keep the victim's name out of the public domain. Perpetrators typically use a distributed denial-of-service attack.

2.4. Cyberwarfare

The U.S. Department of Defense (DoD) notes that the cyberspace has emerged as a national-level concern through several recent events of geo-strategic significance. Among those are included, the attack on Estonia's infrastructure in 2007, allegedly by Russian hackers. "In August 2008, Russia again allegedly conducted cyber attacks, this time in a coordinated and synchronized kinetic and non-kinetic campaign against the country of Georgia. Fearing that such attacks may become the norm in future warfare among nation-states, the concept of cyberspace operations impacts and will be adapted by warfighting military commanders in the future.

2.5. Ransomware

Hospitals, school districts, state and local governments, law enforcement agencies, small businesses, large businesses—these are just some of the entities impacted recently by ransomware, an insidious type of malware that encrypts, or locks, valuable digital files and demands a ransom to release them. The inability to access the important data these kinds of organizations keep can be catastrophic in terms of the loss of sensitive or proprietary information, the disruption to regular operations, financial losses incurred to restore systems and files, and the potential harm to an organization's reputation. And home computers are just as susceptible to ransomware, and the loss of access to personal and often irreplaceable items—including family photos, videos, and other data—can be devastating.

Ransomware has been around for a few years, but during 2015, law enforcement saw an increase in these types of cyber attacks, particularly against organizations because the payoffs are higher. The number of ransomware incidents—and the ensuing damage they cause—will grow even more this year if individuals and organizations don't prepare for these attacks in advance.

In a ransomware attack, victims—upon seeing an e-mail addressed to them—will open it and may click on an attachment that appears legitimate, like an invoice or an electronic fax, but which actually contains the malicious ransomware code. Or the e-mail might contain a legitimate-looking URL, but when a victim clicks on it, they are directed to a website that infects their computer with malicious software. One the infection is present, the malware begins encrypting files and folders on local drives, any attached drives, backup drives, and potentially other computers on the same network that the victim computer is attached to. Users and organizations are generally not aware they have been infected until they can no longer access their data or until they begin to see computer messages advising them of the attack and demands for a ransom payment in exchange for a decryption key. These messages include instructions on how to pay the ransom, usually with bitcoins because of the anonymity this virtual currency provides.

3. Issues and implications

A report (sponsored by McAfee) estimates that the annual damage to the global economy is at $445 billion; however, a Microsoft report shows that such survey-based estimates are "hopelessly flawed"and exaggerate the true losses by orders of magnitude. Approximately $1.5 billion was lost in 2012 to online credit and debit card fraud in the US. In 2016, a study by Juniper Research estimated that the costs of cybercrime could be as high as 2.1 trillion by 2019.

Most measures show that the problem of cybercrime continues to worsen. However, Eric Jardine argues that the frequency, cost and severity of cybercrime cannot be well understood as counts expressed in absolute terms. Instead, these numbers need to be normalized around the growing size of cyberspace, in the same way that crime statistics in the physical world are expressed as a proportion of a population (i.e., 1.5 murders per 100,000 people). Jardine argues that, since cyberspace has been rapidly increasing in size each year, absolute numbers (i.e., a count saying there are 100,000 cyberattacks in 2015) present a worse picture of the security of cyberspace than numbers normalized around the actual size of the Internet ecosystem (i.e., a rate of cybercrime). His proposed intuition is that if cyberspace continues to grow, you should actually expect cybercrime

counts to continue to increase because there are more users and activity online, but that as a proportion of the size of the ecosystem crime might actually be becoming less of a problem.

4. Combating cybercrime

A computer can be a source of evidence. Even where a computer is not directly used for criminal purposes, it may contain records of value to criminal investigators in the form of a logfile. In most countries a Internet Service Providers are required, by law, to keep their logfiles for a predetermined amount of time. For example; a European wide Data Retention Directive states that all E-mail traffic should be retained for a minimum of 12 months.

Due to easily exploitable laws, cybercriminals use developing countries in order to evade detection and prosecution from law enforcement. In developing countries, such as the Philippines, laws against cybercrime are weak or sometimes nonexistent. These weak laws allow cyber criminals to strike from international borders and remain undetected. Even when identified, these criminals avoid being punished or extradited to a country, such as the United States, that has developed laws that allow for prosecution. While this proves difficult in some cases, agencies, such as the FBI, have used deception and subterfuge to catch criminals. For example, two Russian hackers had been evading the FBI for some time. The FBI set up a fake computing company based in Seattle, Washington. They proceeded to lure the two Russian men into the United States by offering them work with this company. Upon completion of the interview, the suspects were arrested outside of the building. Clever tricks like this are sometimes a necessary part of catching cyber criminals when weak legislation makes it impossible otherwise.

As technology advances and more people rely on the internet to store sensitive information such as banking or credit card information, criminals are going to attempt to steal that information. Cyber-crime is not only becoming more of a threat to people across the world. Raising awareness about how information is being protected and the tactics criminals use to steal that information is important in today's world. According to the FBI's Internet Crime Complaint Center in 2014 there were 269,422 complaints filed. With all the claims combined there was a reported total loss of $800,492,073. But yet cyber-crime doesn't seem to be on the average person's radar. There are 1.5 million cyber-attacks annually, that means that there are over 4,000 attacks a day, 170 attacks every hour, or nearly three attacks every minute. Anybody who uses the internet for any reason can be a victim, which is why it is important to be aware of how one is being protected while online.

4.1. FBI

In recent years, The FBI have 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;
- The 93 FBI's 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.

5. References

Furnell, Steven. "Cybercrime in society." Connected Minds, Emerging Cultures: Cybercultures in Online Learning (2008).

Halder, Debarati, Karuppannan Jaishankar, and K. Jaishankar. Cyber crime and the victimization of women: laws, rights and regulations. Information Science Reference, 2012.

https://en.wikipedia.org/wiki/Cybercrime

https://www.fbi.gov/about-us/investigate/cyber

http://www.nationalcrimeagency.gov.uk/crime-threats/cyber-crime

http://us.norton.com/cybercrime-definition

http://www.interpol.int/Crime-areas/Cybercrime/Cybercrime