CHAPTER

# Cybercrime classification and characteristics

12

**Hamid Jahankhani, Ameer Al-Nemrat, Amin Hosseinian-Far**

## INTRODUCTION

The new features of crime brought about as a result of cyberspace have become known as cybercrime.

Cybercrime is growing and current technical models to tackle cybercrime are inefficient in stemming the increase in cybercrime. This serves to indicate that further preventive strategies are required in order to reduce cybercrime. Just as it is important to understand the characteristics of the criminals in order to understand the motivations behind the crime and subsequently develop and deploy crime prevention strategies, it is also important to understand victims, i.e., the characteristics of the users of computer systems in order to understand the way these users fall victim to cybercrime.

The term "cybercrime" has been used to describe a number of different concepts of varying levels of specificity. Occasionally, and at its absolute broadest, the term has been used to refer to any type of illegal activities which results in a pecuniary loss. This includes violent crimes against a person or their property such as armed robbery, vandalism, or blackmail. At its next broadest, the term has been used to refer only to nonviolent crimes that result in a pecuniary loss. This would include crimes where a financial loss was an unintended consequence of the perpetrator's actions, or where there was no intent by the perpetrator to realize a financial gain for himself or a related party. For example, when a perpetrator hacks into a bank's computer and either accidentally or intentionally deletes an unrelated depositor's account records.

Wall (2007) argues that in order to define cybercrime, we need to understand the impact of information and communication technologies on our society and how they have transformed our world. Cyberspace creates new opportunities for criminals to commit crimes through its unique features. These features are viewed by Wall (2005) as "transformative keys," and are as follows:

1. "Globalization," which provides offenders with new opportunities to exceed conventional boundaries.
2. "Distributed networks," which generate new opportunities for victimization.
3. "Synopticism and panopticism," which empower surveillance capability on victims remotely.
4. "Data trails," which create new opportunities for criminal to commit identity theft.

To fully grasp how the Internet generates new opportunities for criminals to commit new Cybercrimes, Wall (2005) has compiled a matrix of cybercrimes which illustrate the different levels of opportunity each type of crime enables.

In Table 12.1, Wall (2005) illustrates the impact of the Internet on criminal opportunity and criminal behaviour. There are three levels of the Internet's impact upon criminal opportunity, as shown on the Y-axis of the table.

Firstly, the Internet has created *more opportunities for traditional crime,* such as phreaking, chipping, fraud, and stalking. These types of crime already existed in the physical or "real" world, but the Internet has enabled an increase in the rate and prevalence of these crimes. Traditional crime gangs are using the Internet not only for communication but also as a tool to commit "classic" crimes, such as fraud and money laundering, more efficiently and with fewer risks. Secondly, the Internet's impact has enabled *new opportunities for traditional crime,* such as cracking/hacking, viruses, large-scale fraud, online gender trade (sex), and hate speech. Hacking is the traditional documented form of committing offences against CIA (Confidentiality, Integrity, and Availability). However, recent developments include parasitic computing, whereby criminals use a series of remote computers to perform operations, including storing illegal data, such as pornographic pictures or pirated software.

Thirdly, the Internet's impact is so great it has led to *new opportunities for new types of crime* arising, such as spam, denial of service, intellectual property piracy, and e-auction scams.

As for the impact of the Internet on criminal behaviour, the table shows on the X-axis that there are four types of crime: integrity-related (harmful trespass); computer-related (acquisition theft/deception); content-related (obscenity); and content-related (violence). As Wall argues, for each type of these crimes there are three levels of harm: least; middle; and most harmful. So, for example, within the integrity-related (harmful trespass) type, phreaking and chipping is least harmful, whereas denial of service and information warfare is most harmful.

## WHAT IS CYBERCRIME?

In recent years there has been much discussion concerning the nature of computer crime and how to tackle it. There is confusion over the scope of computer crime, debate over its extent and severity, and concern over where our power to defeat it lies (Jahankhani and Al-Nemrat, 2011; Rowlingston, 2007). There are many available policy documents and studies that address how the nature of war is changing with the advent of widespread computer technology.

Wall in 2005, raised questions about what we understand by the term "Cybercrime," arguing that the term itself does not actually do much more than signify the occurrence of a harmful behaviour that is somehow related to a computer, and it has no specific reference in law. Over 10 years later, this argument is still true for many countries that still have very vague concepts in their constitutions regarding cybercrime.

**Table 12.1** The Matrix of Cybercrime: Level of Opportunity by Type of Crime (Wall, 2005)

| | Integrity-Related (Harmful Trespass) | Computer-Related (Acquisition Theft/ Deception) | Content-Related 1 (Obscenity) | Content-Related 2 (Violence) |
|---|---|---|---|---|
| **More opportunities for traditional crime (e.g., through communications)** | Phreaking Chipping | Frauds Pyramid schemes | Trading sexual materials | Stalking Personal Harassment |
| **New opportunities for traditional crime (e.g., organization across boundaries)** | Cracking/Hacking Viruses H Activism | Multiple large-scale frauds 419 scams, Trade secret theft, ID theft | Online Gender trade Camgirl sites | General hate speech Organized pedophile rings (child abuse) |
| **New opportunities for new types of crime** | Spams (List construction and content) Denial of Service, Information Warfare, Parasitic Computing | Intellectual Property Piracy Online Gambling E-auction scams Small-impact bulk fraud | Cyber-Sex, Cyber-Pimping | Online grooming, Organized bomb talk/ Drug talk Targeted hate speech |

This lack of definitional clarity is problematic as it impacts upon every facet of prevention and remediation, while, number of people and businesses affected by various types of perceived cybercrime is "growing with no signs of declining."

The Commissioner of Metropolitan Police, Sir Bernard Hogan-Howe, in his commentary published in the Evening Standard in November 2013, highlighted that, in 2012-13 there has been a 60% rise in the number of reports of cybercrime. In the same financial year cybercrime and other types of fraud cost the British economy £81 billion. "*Criminals have realised there are huge rewards to be reaped from online fraud, while the risk of getting arrested falls way below that of armed robbers, for instance"* (Hogan-Howe, 2013).

Unlike traditional crime which is committed in one geographic location, cybercrime is committed online and it is often not clearly linked to any geographic location. Therefore, a coordinated global response to the problem of cybercrime is required. This is largely due to the fact that there are a number of problems, which pose a hindrance to the effective reduction in cybercrime. Some of the main problems arise as a result of the shortcomings of the technology, legislation, and cyber criminology.

Many criminological perspectives define crime on the social, cultural and material characteristics, and view crimes as taking place at a specific geographic location. This definition of crime has allowed for the characterization of crime, and the subsequent tailoring of crime prevention, mapping and measurement methods to the specific target audience. However, this characterization cannot be carried over to cybercrime, because the environment in which cybercrime is committed cannot be pinpointed to a geographic location, or distinctive social or cultural groups. For example, traditional crimes such as child abuse and rape allow for the characterization of the attacker based on the characteristics of the crime, including determination of the social status of the attacker, geographic location within country, state, district, urban or rural residential areas, and so on. However, in the case of cybercrime, this characterization of the attacker cannot be done, because the Internet is "anti-spatial." As a result, identifying location with distinctive crime inducing characteristics is almost impossible in cybercrimes. This, in turn, serves to render the criminological perspectives based on spatial distinctions useless.

Criminology allows for the understanding of the motivations of the criminals by analyzing the social characteristics of the criminals and their spatial locations (see Chapter 9). For example, poverty may be considered to be a cause of crime if poor areas exhibit high crimes, or a high percentage of criminals are found to come from poor backgrounds. Criminology helps in understanding the reasons behind the preponderance of crimes committed by people with particular characteristics, such as the over-representation of offenders from groups of people who are socially, economically or educationally marginalized. It was further explained that the association between geographic location and social characteristics had led to the association between crime and social exclusion in mainstream criminology.

However, in the case of cybercrime, such a correspondence appears to break down. One of the most important points to consider is that access to the Internet is disproportionately low among the marginalized sections of society who were considered to

be socially excluded and therefore more likely to commit a crime. Furthermore, the execution of a cybercrime requires that the criminal have a degree of skill and knowledge that is greater than the level of skills and knowledge possessed by the average computer user. It can, then, be said that cyber criminals are those who are relatively more privileged and who have access to the Internet, knowledge and skills at a level above the average person. Therefore, the relationship between social exclusion and crime that had been widely accepted in traditional crime could not be true in the case of cybercrimes, and that cyber criminals are fairly "atypical" in terms of traditional criminological expectations. Hence, the current perspectives of criminology that link marginality and social exclusion to crime have no use in explaining the motivations behind cybercrimes. Without an understanding of motives, it is difficult for law enforcement agencies and government to take effective measures to tackle cybercrime.

The UK law enforcement agencies sort any crime involving computers into one of three categories. Firstly, a computer can be the target of criminal activity, for example, when a website is the victim of a denial-of-service attack, or a laptop is stolen. Secondly, computers can act as an intermediary medium, where the computer is used as a vehicle for crime against a business or individual, for example, hacking into a website to steal documents or funds. Thirdly, it can be an intermediary facilitator, for example, when criminals use the computer for activities that are related to the crime, but are not in themselves criminal, such as planning and research. As a medium, the computer can perform as the criminal's modus operandi, and as an intermediary, computer systems act as a buffer between offenders and their victims, affecting how an offence is undertaken or executed. As a facilitator, a computer can enable communications between offenders in a globally accessible space which is near relatively instantaneous. When the computer performs as an offending medium, the offender-victim/conspirator contact must be considered, whereas when it acts as an offending facilitator, it aids the contacts between offenders. The difference between these categories is often a matter of emphasis, and it is possible for a computer to play both roles in a single given offence, as an Internet e-commerce based fraud may also involve significant online communication between offenders.

In 2001 The Council of Europe (CoE), adopted its Convention on Cybercrime Treaty, known as Budapest Convention which identifies several activities to be cybercrime offences (CoE, 2001)

- *Intentional access without right to the whole part of any computer system.*
- *Intentional interception, without right, of non-public transmissions of computer data.*
- *Intentional damage, deletions, deterioration, alteration, or suppression of computer data without right.*
- *Intentional and serious hindering of the function of a computer system by inputting, transmitting, damaging, deleting, deterioration, altering, or suppressing computer data.*
- *The production, sale, procurement for use, importation, or distribution of devices designed to commit any of the above crimes, or of passwords or similar data used to access computer systems, with the intent of committing any of the above crimes.*

On March 1st, 2006 the Additional Protocol to the Convention on Cybercrime came into force. Those States that have ratified the additional protocol are required to criminalize the dissemination of racist and xenophobic material through computer systems, as well as threats and insults motivates by racism or xenophobia.

An additional definition has utilized existing criminological theory to clarify what is meant by computer crime. Gordon et al. adapted Cohen and Felson's Life-Style Routine Activity Theory (LRAT)—which states that crime occurs when there is a suitable target, a lack of capable guardians, and a motivated offender—to determine when computer crime takes place. In their interpretation, computer crime is the result of offenders "…perceiving opportunities to invade computer systems to achieve criminal ends or use computers as instruments of crime, betting that the 'guardians' do not possess the means or knowledge to prevent or detect criminal acts" (Gordon and Ford, 2006; Jahankhani and Al-Nemrat, 2010; Wilson and Kunz, 2004).

The definition should be designed to protect, and indicate violations of, the confidentiality, integrity and availability of computer systems. Any new technology stimulates a need for a community to determine what the norms of behaviour should be for the technology, and it is important to consider how these norms should be reflected, if at all, in our laws.

## WHAT ARE THE CLASSIFICATIONS AND TYPES OF CYBERCRIME?

The other approach to defining cybercrime is to develop a classification scheme that links offences with similar characteristics into appropriate groups similar to the traditional crime classifications. Several schemes have been developed over the years. There are suggestions that there are only two general categories: *active* and *passive* computer crimes. An active crime is when someone uses a computer to commit the crime, for example, when a person obtains access to a secured computer environment or telecommunications device without authorization (hacking). A passive computer crime occurs when someone uses a computer to both support and advance an illegal activity. An example is when a narcotics suspect uses a computer to track drug shipments and profits.

Literature has widely categorizes four general types of cybercrime by the computer's relationship to the crime:

- *Computer as the Target: theft of intellectual property, theft of marketing information (e.g., customer list, pricing data, or marketing plan), and blackmail based on information gained from computerized files (e.g., medical information, personal history, or sexual preference).*
- *Computer as the Instrumentality of the Crime: fraudulent use of automated teller machine (ATM) cards and accounts, theft of money from accrual, conversion, or transfer accounts, credit card fraud, fraud from computer transaction (stock transfer, sales, or billing), and telecommunications fraud.*

- *Computer Is Incidental to Other Crimes: money laundering and unlawful banking transactions, organized crime records or books, and bookmaking.*
- *Crime Associated with the Prevalence of Computers: software piracy/ counterfeiting, copyright violation of computer programs, counterfeit equipment, black market computer equipment and programs, and theft of technological equipment.*

Yar (2006), who has subdivided cybercrime into four areas of harmful activity, illustrates a range of activities and behaviors rather than focusing on specific offences. This reflects not only the various bodies of law, but also specific courses of public debate. The four categories are as follows:

> ***Cyber-trespass*:** the crossing of cyber boundaries into other people's computer systems into spaces where rights of ownership or title have already been established and causing damage, e.g., hacking and virus distribution.
> ***Cyber-deceptions and thefts*:** the different types of acquisitive harm that can take place within cyberspace. At one level lie the more traditional patterns of theft, such as the fraudulent use of credit cards and (cyber) cash, but there is also a particular current concern regarding the increasing potential for the raiding of online bank accounts as e-banking become more popular.
> ***Cyber-pornography*:** the breaching of laws on obscenity and decency.
> ***Cyber-violence*:** the violent impact of the cyber activities of others upon individual, social or political grouping. Whilst such activities do not have to have a direct manifestation, the victim nevertheless feels the violence of the act and can bear long-term psychological scars as a consequence. The activities referred here range from cyber-stalking and hate-speech, to tech-talk.

In addition to the above, Yar (2006) has added a new type of activity which is "crime against the state," describing it as encompassing those activities that breach laws which protect the integrity of the nation's infrastructure, like terrorism, espionage and disclosure of official secrets.

Gordon and Ford (2006) attempted to create a conceptual framework which law makers can use when compiling legal definitions which are meaningful from both a technical and a societal perspective. Under their scheme, they categorize cybercrime into two types:

1. The first type has the following characteristics:
   - *It is generally a singular, or discrete, event from the perspective of the victim.*
   - *It is often facilitated by the introduction of crime-ware programs such as keystroke loggers, viruses, rootkits or Trojan horses into the user's computer system.*
   - *The introductions can (but not necessarily) be facilitated by vulnerabilities.*

2. At the other end of the spectrum is the second type of cybercrime, which includes, but is not limited to, activities such as cyber stalking and harassment, blackmail, stock market manipulation, complex corporate espionage, and planning or carrying out terrorist activities online. The characteristics of this type are as follows:
   - *It is generally facilitated by programs that do not fit under the classification of crime-ware. For example, conversations may take place using IM (Instant Messaging), and clients or files may be transferred using the FTP protocol.*
   - *There are generally repeated contacts or events from the perspective of the user.*

## CYBERCRIME CATEGORIES

### Phishing

Is the act of attempting to trick customers into disclosing their personal security information; their credit card numbers, bank account details, or other sensitive information by masquerading as trustworthy businesses in an e-mail. Their messages may ask the recipients to "update," "validate," or "confirm" their account information.

Phishing is a two time scam, first steals a company's identity and then use it to victimize consumers by stealing their credit identities. The term Phishing (also called spoofing) comes from the fact that Internet scammers are using increasingly sophisticated lures as they "fish" for user's financial information and password data.

Phishing becomes the most commonly used social engineering attack to date due to the fact that it is quite easy to be carried out, no direct communication between hacker and victim is required (i.e., hacker does not need to phone their prey, pretending that they are a technical support staff, etc.). Sending mass-mails to thousands of potential victims increases the chance of getting someone hooked. There are usually three separate steps in order for such attacks to work, these are:

1. Setting up a mimic web site.
2. Sending out a convincingly fake e-mail, luring the users to that mimic site.
3. Getting information then redirect users to the real site.

In step 1, the hacker steals an organization's identity and creates a look-alike web site. This can easily be done by viewing the targeted site's source code, then copying all graphics and HTML lines from that real web site. Due to this tactic, it would really be very hard for even an experienced user to spot the differences. On the mimic web site, usually there will be a log-in form, prompting the user to enter secret personal data. Once the data are entered here, a server-side script will handle the submission, collecting the data and send it to the hacker, then redirect users to the real web site so everything look unsuspicious.

The hardest part of phishing attack that challenges most hackers is in the second step. This does not mean it is technically hard, but grammatically it is! In this step,

the hacker will make a convincingly fake e-mail which later will be sent by a "ghost" mailing program, enabling the hacker to fake the source address of the e-mail.

The main purpose of this fake e-mail is to urge the users going to the mimic web site and entering their data that hackers wanted to capture. Commonly employed tactics are asking users to response over emergency matters such as warning that customers need to log-in immediately or their accounts could be blocked; notifying that someone just sends the user some money and they need to log in now in order to get it (this usually is an effective trap to PayPal users), etc. Inside this fake e-mail, users often find a hyperlink, which once clicked, will open the mimic web site so they can "*log in.*" As discussed before, the easiest way to quickly identify a fake e-mail is not just by looking at the address source (since it can be altered to anything) but to check English grammar in the e-mail. You may find this sounds surprising, however, 8 out of 10 scam e-mails have obvious grammar mistakes. Regardless of this, the trick still works.

In the last step, once a user has opened the mimic web site and "*log in,*" their information will be handled by a server-side script. That information will later be sent to hacker via e-mail and user will be redirected to the real web site. However, the confidentiality of user's financial data or secret password has now been breached.

Due to the recent financial crises, mergers and takeovers, many changes have taken place in the financial marketplace. These changes have encouraged scam artists to phish for customers' details.

The key points are:

- Social engineering attacks have the highest success rate
- Prevention includes educating people about the value of information and training them to protect it
- Increasing people's awareness of how social engineers operate
- Do not click on links in the e-mail message
- It appears that phishing e-mail scam has been around in one form or another since February 2004 and it seems to be still evolving, similar to the way virus writers share and evolve code.

According to the global phishing survey carried out by the Anti-Phishing working group published in 2013 (APWG, 2013)

1. *Vulnerable hosting providers are inadvertently contributing to phishing. Mass compromises led to 27% of all phishing attacks.*
2. *Phishing continues to explode in China, where the expanding middle class is using e-commerce more often.*
3. *The number of phishing targets (brands) is up, indicating that e-criminals are spending time looking for new opportunities.*
4. *Phishers continue to take advantage of inattentive or indifferent domain name registrars, registries, and subdomain resellers. The number of top-level registries is poised to quintuple over the next 2 years.*
5. *The average and median uptimes of phishing attacks are climbing.*

According to Symantec Intelligence Report (2013) Fake offerings continue to dominate Social Media attacks, while disclosed vulnerability numbers are up 17% compared to the same period in 2012 (Symantec, 2013).

## SPAM

Another form of Cybercrime is spam mail, which is arguably the most profound product of the Internet's ability to place unprecedented power into the hands of a single person. Spam mail is the distribution of bulk e-mails that advertise products, services or investment schemes, which may well turn out to be fraudulent. The purpose of spam mail is to trick or con customers into believing that they are going to receive a genuine product or service, usually at a reduced price. However, the spammer asks for money or sensible security information like credit card number or other personal information before the deal occur. After disclosing their security information the customer will never hear from the spammer.

Today, spammers who spread malicious code and phishing e-mails are still looking for the best way to reach computer users by using social engineering and technical advances, however, according to a Symantec Intelligence Report (Symantec, 2012), spam levels have continued to drop to 68% of global e-mail traffic in 2012 from 89% highest in 2010.

In April 2012, political spams were back in action targeting primarily US and French population. The complex situation in Syria has also become the subject of spam e-mails too.

In 2012, USA was in second place after India for spam origination with China ranked as number 5 (Kaspersky, 2012).

## HACKING

Hacking is one of the most widely analyzed and debated forms of cyber-criminal activity, and serves as an intense focus for public concerns about the threat that such activity poses to society. The clear-cut definition of hacking is "the unauthorized access and subsequent use of other people's computer systems" (Yar, 2006).

The early hackers had a love of technology and a compelling need to know how it all worked, and their goal was to push programs beyond what they were designed to do. The word hacker did not have the negative connotation as it has today.

The attacks take place in several phases such as information gathering or reconnaissance, scanning and finally entering into the target system. Information gathering involves methods of obtaining information or to open security holes. It is just like the way in which the traditional type of robbery is carried out. The robber will find out the whole information about the place that wants to rob before making attempt. Just like this the computer attacker will try to find out information about the target. Social Engineering is one such method used by an attacker to get information.

There are two main categories under which all social engineering attempts could be classified, computer or technology-based deception and human-based

deception. The technology-based approach is to deceive the user into believing that is interacting with the "real" computer system (such as popup window, informing the user that the computer application has had a problem) and get the user to provide confidential information. The human approach is done through deception, by taking advantage of the victim's ignorance, and the natural human inclination to be helpful and liked.

Organized criminals have the resources to acquire the services of the necessary people. The menace of organized crime and terrorist activity grows ever more sophisticated as the ability to enter, control and destroy our electronic and security systems grows at an equivalent rate. Today, certainly, e-mail and the Internet are the most commonly used forms of communication and information sharing. Just over 2 billion people use the Internet every day. Criminal gangs "buying" thrill-seeking hackers and "script kiddies" to provide the expertise and tools, this is called cyber child labor.

## CYBER HARASSMENT OR BULLYING

Cyber-harassment or bullying is the use of electronic information and communication devices such as e-mail, instant messaging, text messages, blogs, mobile phones, pagers, instant messages and defamatory websites to bully or otherwise harass an individual or group through personal attacks or other means. "At least in a physical fight, there's a start and an end, but when the taunts and humiliation follow a child into their home, it's 'torture,' and it doesn't stop" (Early, 2010). Cyber-bullying, taunts, insults and harassment over the Internet or text messages sent from mobile phones has become rampant among young people, in some cases with tragic consequences. Derek Randel, a motivational speaker, former teacher and founder of StoppingSchoolViolence.com, believes that "cyber-bullying has become so prevalent with emerging social media, such as Facebook and text messaging, that it has affected every school in every community" (Early, 2010; StopCyberbullying, 2013).

## IDENTITY THEFT

this is the fastest growing types of fraud in the UK. Identity theft is the act of obtaining sensitive information about another person without his or her knowledge, and using this information to commit theft or fraud. The Internet has given cyber criminals the opportunity to obtain such information from vulnerable companies' database. It has also enabled them to lead the victims to believe that they are disclosing sensitive personal information to a legitimate business; sometimes as a response to an e-mail asking to update billing or membership information; sometimes it takes the form of an application to a (fraudulent) Internet job posting. According to the All Party Parliamentary Group, the available research, both in the UK and globally, indicates that identity fraud is a major and growing problem because of the escalating and evolving methods of gaining and utilizing personal information. Subsequently, it is expected to increase further over the coming years.

This is an issue which is recognized in the highest levels of Government.

In 2012 alone CIFAS, the UK's Fraud Prevention Service, identified and protected over 150,000 victims of these identity crimes (CIFAS, 2012).

### PLASTIC CARD FRAUD

Plastic Card Fraud is the unauthorized use of plastic or credit cards, or the theft of a plastic card number to obtain money or property. According to APACS (analysis of policing and community safety framework), the UK payments association, plastic card losses in 2011 was £341m, of which £80m was the result of fraud abroad (Financial fraud action UK, 2012). This typically involves criminals using stolen UK card details at cash machines and retailers in countries that have yet to upgrade to Chip and PIN.

The biggest fraud type in the UK is card-not-present (CNP) fraud. In 2011 65% of total losses was CNP, which was £220.9 Million (down by 3%) (Financial fraud action UK, 2012). CNP fraud encompasses any frauds which involve online, telephone or mail order payment. The problem in countering this type of fraud lies in the fact that neither the card nor the cardholder is present at a physical till point in a shop. There are a number of methods that fraudsters use for obtaining both cards and card details, such as phishing, sending spam e-mails, or hacking companies' database, as aforementioned.

### INTERNET AUCTION FRAUD

Internet auction fraud is when items bought are fake or stolen goods, or when seller advertises nonexistent items for sale which means goods are paid for but never arrives. Fraudsters often use money transfer services as it is easier for them to receive money without revealing their true identity.

Auction fraud is a classic example of criminals relies on the anonymity of the internet. According to action fraud 2013, some of the most common complaints involve:

- *Buyers receiving goods late, or not at all*
- *Sellers not receiving payment*
- *Buyers receiving goods that are either less valuable than those advertised or significantly different from the original description*
- *Failure to disclose relevant information about a product or the terms of sale.*

These fraudulent "sellers" use stolen IDs when they register with the auction sites, therefore tracing them is generally a very difficult tasks.

## CYBER-ATTACK METHODS AND TOOLS

Any Internet-based application is a potential carrier for worms and other malware; therefore Internet messaging is not exceptional. Criminals use these common chat methods for ID theft purposes by getting to know the individuals who they are communicating with or via the spreading of malware, spyware, and viruses.

E-mails are a critical tool in the hands of criminals. Not only is e-mail one of the fastest and cheapest mediums form spamming and phishing, but they are easily manipulated into carrying deadly virus attacks capable of destroying an entire corporate network within minutes. Some viruses are transmitted through harmless-looking e-mail messages and can run automatically without the need for user intervention (like the "I Love You" virus). Technically, attacks on "system security that can be carried out via electronic mail" can be categorized into the following:

- Active content attacks, which take advantage of various active HTML (hypertext markup language) and other scripting features and bugs.
- Buffer overflow attacks, where the attacker sends something that is too large to fit into the fixed-size memory buffer of the e-mail recipient, in the hopes that the part that does not fit will overwrite critical information rather than being safely discarded.
- Shell script attacks—where a fragment of a Unix shell script is included in the message headers in the hopes that an improperly configured Unix mail client will execute the commands.

Staged downloaders are threats which download and install other malicious codes onto a compromised computer. These threats allow attackers to change the downloadable component to any type of threat that suits their objectives, or to match the profile of the computer being targeted. For example, if the targeted computer contains no data of interest, attackers can install a Trojan that relays spam, rather than one that steals confidential information. As the attackers' objectives change, they can change any later components that will be downloaded to perform the requisite tasks.

A virus is a program or code that replicates itself onto other files with which it comes into contact. A virus can damage an infected computer by wiping out databases or files, damaging important computer parts, such as Bios, or forwarding a pornographic message to everyone listed in the e-mail address book of an infected computer.

2007 was the year when botnets were first used. A bot is shot from robot where cyber criminals take over control of their victim's computer without his or her knowledge. This occurs when cyber criminals or hackers install programs in the target's computer through a worm or a virus. Collections of these infected computers are called botnets. A hacker or spammer controlling these botnets might be renting them for cyber criminals or other hackers, which in turn make it very hard for authorities to trace back to the real offender.

In March 2009, BBC journalist investigated the world of Botnets. The BBC team investigated thousands of Trojan horse malware infected, mostly domestic PCs running Windows, connected via broadband Internet connections, which are used to send most of the world's spam e-mails and also for Distributed Denial of Service attacks, and blackmails against e-commerce websites. The BBC team managed to rent a botnet of over 21,000 malware-infected computers around the world. This botnet was said to be relatively cheap, as it was mostly infecting computers in less developed countries, which have less security measures installed on them.

A keylogger is a software program or hardware device that is used to monitor and log each of the keys a user types into a computer keyboard. The user who installed the program or hardware device can then view all keys typed in by that user. Because these programs and hardware devices monitor the keys entered, a hacker user can easily find user passwords and other information a user may wish and believe to be private.

Keyloggers, as a surveillance tool, are often used by employers to ensure employees use work computers for business purposes only. Unfortunately, keyloggers can also be embedded in spyware, allowing information to be transmitted to an unknown third party. Cyber criminals use these tools to deceive the potential target into releasing their personal sensitive data and restoring it for later access to the user's machine, if the data obtained contained the target ID and password. Furthermore, a keylogger will reveal the contents of all e-mails composed by the user and there are also other approaches to capturing information about user activity.

- Some *keyloggers* capture screens, rather than keystrokes.
- Other *keyloggers* will secretly turn on video or audio recorders, and transmit what they capture over your Internet connection.

## CONCLUSION

All countries face the same dilemma of how to fight cybercrime and how to effectively promote security to their citizens and organizations.

Cybercrime, unlike traditional crime which is committed in one geographic location, is committed online and it is often not clearly linked to any geographic location. Therefore, a coordinated global response to the problem of cybercrime is required. This is largely due to the fact that there are a number of problems, which pose a hindrance to the effective reduction in cybercrime. Some of the main problems arise as a result of the shortcomings of the technology, legislation and cyber criminology.

Many criminological perspectives define crime on the social, cultural and material characteristics, and view crimes as taking place at a specific geographic location. This definition of crime has allowed for the characterization of crime, and the subsequent tailoring of crime prevention, mapping and measurement methods to the specific target audience. However, this characterization cannot be carried over to cybercrime, because the environment in which cybercrime is committed cannot be pinpointed to a geographic location, or distinctive social or cultural groups.

In 2014, a world-leading unit to counter online criminals will be established in UK in order to change the way police deals with cybercrime as was reported by the Commissioner of Metropolitan Police in November 2013.

The aims are fivefold:

1. To bring more fraudsters and cyber-criminals to justice;
2. To improve the service to their victims;
3. To step up prevention help and advice to individuals and businesses;

4. To dedicate more organized crime teams to stemming the harm caused by the most prolific cyber-criminals;
5. To invite business and industry to match the Metropolitan police determination and work with together to combat fraud and cybercrime.

Clearly, the traditional way of policing cybercrime has not been working despite, plethora of internet-related legislation. This is because of the high volume online nature of the crimes.

## REFERENCES


Anti-Phishing Working Group (APWG), 2013. Global Phishing Survey: Trends and Domain Name Use in 1H2013. http://docs.apwg.org/reports/APWG_GlobalPhishingSurvey_1H2013.pdf (accessed December 2013).

CIFAS, The UK's Fraud Prevention Service, 2012. http://www.cifas.org.uk/ (accessed December 2013).

Council of Europe (CoE), 2001. Convention on Cybercrime. Budapest, 23.11.2001, http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm (accessed December 2013).

Early, J.R., 2010. Cyber-bullying on increase. http://www.tmcnet.com/usubmit/2010/02/07/4609017.htm (accessed January 2014).

Financial fraud action UK, 2012. Fraud: The Facts 2012. The definitive overview of payment industry fraud and measures to prevent it, http://www.theukcardsassociation.org.uk/wm_documents/Fraud_The_Facts_2012.pdf (accessed January 2014).

Gordon, S., Ford, R., 2006. On the definition and classification of cybercrime. J. Comput. Virol. 2 (1), 13–20.

Hogan-Howe, Bernard, the Commissioner of Metropolitan Police, 2013. Met to Tackle the wave of cybercrime with 'world-leading unit' published in the Evening Standard, 21st November 2013. http://www.standard.co.uk/news/crime/commentary-sir-bernard-hoganhowe-on-new-cybercrime-push-8954716.html (accessed January 2014).

Jahankhani, H., Al-Nemrat, A., 2011. Cybercrime Profiling and trend analysis. In: Akhgar, B., Yates, S. (Eds.), Intelligence Management, Knowledge Driven Frameworks for Combating Terrorism and Organised Crime. Springer, London, ISBN 978-1-4471-2139-8.

Jahankhani, H., Al-Nemrat, A., 2010. Cybercrime. In: Jahankhani, et al. (Eds.), Handbook of Electronic Security and Digital Forensics. World Scientific, London, ISBN 9978-981-283-703-5.

Kaspersky, 2012. Spam in April 2012: Junk Mail Gathers Pace in the US, http://www.kaspersky.co.uk/about/news/spam/2012/Spam_in_April_2012_Junk_Mail_Gathers_Pace:in_the_US (accessed January 2014).

Rowlingston, R., 2007. Towards a strategy for E-crime prevention. In: ICGeS Global e Security, Proceedings of the 3rd Annual International Conference, London, England, 18–20 April 2007, ISBN 978-0-9550008-4-3.

StopCyberbullying, 2013. http://stopcyberbullying.org/index2.html (accessed January 2014).

Symantec, 2012. Intelligence Report: October 2012, http://www.symantec.com/connect/blogs/symantec-intelligence-report-october-2012 (accessed January 2014).

Symantec, 2013. Intelligence Report: October 2013, http://www.symantec.com/connect/blogs/symantec-intelligence-report-october-2013 (accessed January 2014).

Wall, D., 2007. Hunting Shooting, and Phishing: New Cybercrime Challenges for Cybercanadians in The 21st Century. The ECCLES Centre for American Studies. http://bl.uk/ecclescentre,2009.

Wall, D.S., 2005. The internet as a conduit for criminal activity. In: Pattavina, A. (Ed.), Information Technology and the Criminal Justice System. Sage Publications, USA, ISBN 0-7619-3019-1.

Wilson, P., Kunz, M., 2004. Computer crime and computer fraud. Report to Montegmery County Criminal Justice Coordination Commission, http://www.mongomerycountymd.gov (accessed September 2007).

Yar, M., 2006. Cybercrime and Society. Sage Publication Ltd, London.