New Face of Terror: Cyber Threats, Emails Containing Viruses

Arun Kr. Singh[1]
Ahmad T. Siddiqui[2]

ABSTRACT

Cyber terrorism can be defined as any act which is unlawful or use of force or violence against any individuals or property to intimidate or to disturb a government, the civilians, etc. According to the FBI, "Cyber terrorism could thus be well defined as the use of computing resources to intimidate or coerce others". An example of cyber terrorism could be hacking into a hospital computer system and changing someone's medicine prescription to a lethal dosage as an act of revenge. It sounds farfetched, but these things can and do happen. The various forms of computer attack that exist have in common the relatively low level of risk for the criminal, set against a potential for harm and damage the resources.

Keywords: Cyber threat, email viruses, cyber terrorism.

1.0 INTRODUCTION

Cyber terrorism is a form of computer-related crime committed using internet technology; it covers all crimes committed in cyberspace. In the virtual world, crime can be automated, creating the potential for a large-scale cyber epidemic, capable of being launched remotely via a network (freeing the criminal from constraints of time and space), with the possibility of delayed action Internet technology facilitates a wide range of infractions: theft, information sabotage, copyright infractions, breach of professional trust, digital privacy, intellectual property, distribution of illegal content, anti-competitive attacks, industrial espionage, trademark infringements, disinformation, denial of service, various forms of fraud.

2.0 WHY THE INTERNET USED BY CYBER CRIMINALS

a) Virtually

The uncoupling of transactions from physical media (virtualization), communication tools

[1]Lecturer, Sherwood College of Professional Management, Lucknow (Research scholar Singhania University, Jhunjhunu, Rajasthan)
[2]Lecturer, Sherwood College of Professional Management, Lucknow (Research scholar Singhania University, Jhunjhunu, Rajasthan)

involving encryption, steganography and anonymity: these are factors which criminals in different countries exploit in order to collaborate while dispensing with physical meetings, operating in a flexible, secure manner and with complete impunity. They can form teams, plan crimes and carry them out, whether in the traditional manner or using new technologies. The global reach of the internet allows criminals to act globally, on a large scale and very rapidly.

b) Networking of resources The wide-scale networking of computer and information resources makes them attractive targets for economic crime using new technologies. The various forms of computer attack that exist have in common the relatively low level of risk for the criminal, set against a potential for harm and damage that greatly exceeds the resources necessary to launch an attack. Electronic identity theft, easy anonymity and the possibilities for taking control of computers make it easy to carry out illegal acts without exposing oneself to any great risk.

c) Exposing Cyber Criminals is difficult

Computer-related crime is sophisticated, and is usually committed across national borders, frequently with a time delay. The traces it leaves in the systems are intangible and difficult to gather and save. They take the form of digital information stored on all sorts of media: working memory, storage peripherals, hard discs, external discs and USB sticks, electronic components, etc. The problem is how to capture the wide variety of evidence turned up in a digital search.

3.0 TYPES OF CYBER ATTACKS a)

Stealing of users' passwords

The main methods used to obtain the connection parameters of legitimate users to gain access to systems are: Deception (social engineering):

Listening to traffic: "Trojan horse"

• Accessing the password storage file.
• Cracking passwords that are sent in encrypted form.
• Spying on users by activating their multimedia peripherals to record their connection parameters. Once in possession of the access key necessary to get into the systems (the combination of username and password), it is easy to penetrate the systems and carry out all sorts of read and write operations. The challenge for the hacker is to avoid being detected and to leave no trace of his presence in the systems accessed.

b) Denial-of-service attacks

A denial-of-service attack is typically carried out by overloading system capacity. Targeted systems, inundated with far more requests than they are equipped to cope with, crash and become unavailable. These attacks can be perpetrated by taking advantage of flaws in the operating system and exploiting certain system features, for example, buffer management (buffer overflow attack), causing serious malfunctioning which can lead to system shutdown. E-mail bombing, which involves flooding a user's inbox with messages, is one form of a denial-of-service attack.

c) Defacement attacks

A defacement attack is carried out by replacing the victim's web page with another, where the content of the new page (e.g. pornographic, political) will depend on the hacker's motives. One variation on this type of attack involves redirecting users to a decoy website that looks exactly the same as the one they were accessing, where they are asked to disclose their credit card information, These are semantic attacks, which subvert the meaning of the information content, and fall into the category of info war.

d) Spoofing Attacks

All TCP/IP & UDP (transmission control protocol/internet protocol) protocols can be corrupted and used to breach system security. Protocols and mechanisms that transport data through a network are equally at risk. Thus, it is possible to hijack a TCP session during a client-server working session.

User datagram protocol (UDP) is a level 4 (transport), connectionless protocol. It is an alternative to using TCP for the rapid transfer of a small volume of data. UDP communications are not subject to any control mechanisms, so there are no checks for identification, flow or error. As a result, anyone can use the IP address of an authorized system user in order to penetrate it. UDP session theft can take place without alerting the application servers. Hackers exploit protocols and their limitations to:

- Paralyze networks;
- Redirect IP packets to a false destination (their own, for example); • overload systems by deluging them with junk messages;

- Prevent a sender from transmitting data;
- Take control of the flow of packet transmission, impeding the circulation of network traffic and degrading its performance (reliability, dependability, etc.).

4.0 TYPES OF CYBER

CRIMINALS a) Teenagers Hackers

Hackers in this category are the group of society that adhered the most rapidly to this new "cyber-culture". The explication resides in the fact that the Internet gives them the freedom they are looking for at their age: Within a few clicks, they can communicate with the world and explore new horizons. They don't have to wait to get a telephone or a car which still does not offer the same level of communication deepness and intensity that the Internet does. This is usually the case with all teenagers' attacks: they target a lot of victims to be put into the media spotlight but their actual harm to each individual is relatively negligent. They are very challenging, but need education not law.

b) The Greed-Prompted

This category of cyber-criminals is dangerous because they are usually unscrupulous and are ready to commit any type of crime, as long as it brings them some cash. This is why they are at the origin of child pornography often falsely called cyber-porn which encloses legal and illegal pornography on the Internet. This type of unscrupulous cyber-crime must be prevented. Usually current legislation is enough and just need small adaptation because, as mentioned above, the crime is still the same but it uses a different technology. They are usually well organized and know how to escape law enforcement agencies. They prefer offshore or low level of enforcement locations to establish their headquarters. They can act on their own, as mercenaries with organized crime or as "cyber-spy" for foreign governments.

These cyber-criminals can't be fought by education: they will not behave because most of them are already career criminals. The only appropriate tool to fight them is by enacting new Laws, harmonize international legislations and encourage coordination and cooperation between national law enforcement agencies.

c) The Cyber-Terrorists

This category is the newest as well as the potentially most dangerous. Their primary motive is

usually not only money but also a specific cause that they defend. They perform very serious cases like the shutdown of an airport tower control during 6 hours, the hacking of California government computers responsible to manage the delivery of electricity or the daily attack and penetration of federal agencies computer servers such as the National Security Agency (N.S.A.) and the Department of Defense (DOD) show the weaknesses and fragility of the National vital infrastructures.

The only way to prevent the action of potential cyber-terrorists like Osama bin laden is to massively fund global surveillance at a national level and this is what the U.S. Government is doing since 2008

5.0 THREATS TO SECURITY

Threats are the most notorious thing in today information technology world, every company, every computer owner terrorize by these notorious threats. In the category of threats all those things, which steal our information, corrupt our information, or misuse our resources, obstruct to using our resources identified. They are Virus, Spam, Worms, Trojans we can say it combined Malware.

5.1 Types of Threats A)

Viruses

A computer virus is a small computer program that is embedded in a larger, legitimate program. The virus is designed so that when a user executes the legitimate program, the virus executes first, and when it's finished doing whatever it was put together to do, the original program runs, without the user ever being aware that a virus was put into play. A virus can be either a file infector or a system (boot record) infector.

(i) File infectors

File infectors attach themselves to programs that users would use during their daily work. Some file infectors select one or more programs to infect each item the original infected program is run

(these are called direct-action) while other file infectors (called resident) install themselves into random access memory when the original infected program is run, and then waits to infect other programs when they are executed.

(ii) System infectors

System infectors don't attack ordinary programs; rather, they target specific files and portions of computer disks that are used when a computer is turned on or rebooted. Some system infectors attach themselves to the Master Boot Record (MBR) of a hard disk while others only infect the DOS boot sector of hard disks and floppy disks. Some viruses do both infect both ordinary files and system files. These are called "multi partite".

(iii) File system infectors

Another category of viruses are File System (or Cluster) viruses that modify the directory table entries. Thus, when a user runs a specific program, the modified directory entry actually points to a different location, where the virus is and the virus executes, and then runs the program that the user originally desired. This is sort of like when someone asks you to pass the salt at the dinner table and you stop use it yourself first before passing it on.

Attributes of Viruses

A stealth virus is one that hides the modifications it has made. For example, one common modification is to change the size of a file, since a file infector adds code to an existing program. This hiding of the change of file size is usually done by monitoring system calls to functions that would report such changes, and substituting false information.

- A polymorphic virus is one that creates different versions of itself. The purpose of this functionality is to create many versions in the hopes that at least some of the versions will evade identification by antivirus scanners that are keyed to look for specific versions of viruses. Another analogy to biological viruses is worth noting: just as genetic diversity in a population decreases the chance of a single disease wiping out a population, the diversity of software systems on a network similarly limits the destructive potential of viruses.
- Armoring is a technique used in writing viruses so that antivirus programmers can take the virus apart in order to determine how it works and what its intended functionality is.
- A companion virus is one that creates a new program with the same name as an existing program. When a user attempts to run the original program, the new, virus laden program is run instead. When the virus laden program has finished executing, it will typically then run the original program so as to not alert the user that anything untoward has occurred.

- A cavity virus is one that fills empty spaces in the host program's program code with itself so as to avoid detection.
- An encrypted virus is written so that it can has infected be changed or removed from the computer it
- A tunneling virus is one that calls system functions (interrupt handlers) in the operating system directly, thus bypassing antivirus programs that may be loaded and are set up to provide the same functionality.

B) Worms

A worm is similar to a virus in that it makes copies of itself, but it does not need to attach itself to a host (another computer program) in order to survive. Instead, when executed, it can simply replicate itself from machine to machine via a network. Like viruses, however, a worm can perform secondary actions ranging from merely nuisance level to highly destructive. A worm can replicate extremely quickly because of the multiplier effect of a network. Suppose a worm only infects two other machines (in real life, a worm on one machine would typically infect hundreds or thousands of machines.) The first infected machine infects two other machines, each of which can again infect two more machines. After only 16 rounds of infections, over 65,000 machines would be infected.

C) Trojans

Trojan Horses (known as a 'Trojan ' for short) differs from viruses and worms in that they don't replicate themselves, relying on a separate mechanism for distribution. Instead, their primary feature is that they masquerade as a legitimate program or offer something desirable (such as a link for something free or interesting), but harbor a malevolent purpose.

5.2 Finding Strategies

A piece of malware that can be easily found is much less effective than one that can stay hidden. As a result, well written malware uses a variety of techniques to avoid detection. Common means of detection include looking for changes in file attributes, and looking for virus signatures. The first virus detection technique to come into play was to compare the attributes of existing files to a database that contains the actual, well-known attributes. Viruses would alter the size and date attributes of a file during the process of infecting it. Those modifications were easily spotted as the files attacked were commonly used files whose attributes were widely known. (I

still remember listening to warnings at PC User Group meetings in the mid 80's about "If your COMMAND.COM file isn't dated <something>, it's been infected!")This technique for detecting malware has been around for a long time, so even older viruses that simply infected a file would often alter the information contained in the File Allocation Table about the file, such as the date last updated and the file size, setting those values back to the original, correct ones. Another technique of evasion was to infect the boot sector of a computer instead of the data or program files on the hard disk. When the computer was turned on, the boot sector virus was loaded into memory, which would then load the original boot sector code as well, and transfer control to it. Thus, the operating system wasn't aware of the presence of the virus since the virus was part of the environment for as long as the operating system had been running.

Polymorphic viruses usually contain two pieces the part that does the infection (the virus itself) and the engine that provides the algorithms that encrypt and modify the code in the infector. Each time the engine generates the infector, the algorithm inside the engine customizes the end result so that there isn't single standard signature in the virus file. The infector also has to include the engine as part of its payload, and so the engine needs to modify its own code as well, without affecting the core generation algorithms.

5.3 Some historical notorious threats

(i)The Brain

The "Brain", a virus written by two Pakistani brothers in the software business in 1986, was created in order to track piracy. Unfortunately for them, the virus spread beyond the Pakistan borders and the world was introduced to the dark side of computer programming.

(ii) Stoned virus

"Stoned", making its debut in 1987, got its name from a message it would display on the user's computer: "Your PC is now stoned!" Subsequent variants displayed different messages or no message at all

(iii) CAP virus

The CAP virus upped the ante in Microsoft macro exploits in February of 1997. Hailing from

Venezuela, this Word macro virus was specifically designed to fool users through a variety of techniques in order to stay hidden while propagating, and worked really well in that endeavor

(iv) Happy99.exe worm

January 1999 marked the release of HAPPY99.EXE, a Windows 95/98 executable file that was spread over the Internet. Technically a computer worm, created a nuisance effect, displaying a fireworks show which was sleight of hand to distract the user from the real purpose, changing the Windows system file, winsock32.dll that controls access to the Internet. Once modified, the new winsock32.dll caused a copy of the worm to be sent along with email or posts to Usenet.

(v)Melissa

Things got interesting a short later when Melissa showed up. Another Word 97 macro, Melissa (I still keep hearing the Allman Brothers in the background) was embedded in a document that was attached to an email message with an alluring subject line like "Important message from <your name>" and a body that said "Here is the document you asked for don' else!" show anyone Now, who could resist this? In those innocent times (April of 1999, to be specific), not many people. When the user opened the document, the macro virus automatically executed and performed a number of actions, some of which were rather novel at the time.

(vi) ILOVEYOU

A piece of Visual Basic script (known as VBScript), it was attached to an email message like Melissa, but also employed other means of transmission as well. Usenet postings, IRC communications and Windows file sharing were all also used. The ILOVEYOU virus was a piece of VBScript (Visual Basic script) that infected machines through a variety of means. It was attached to an email message and USENET news postings, transmitted through Internet Relay Chat (IRC) and even via Windows file sharing.

(vii)DDOS Attacks

The new millennium also featured the debut of the first widespread Distributed Denial of Service ("DDOS") attack. Dozens of high profile web sites are shut down for hours as a series of DDOS attacks were orchestrated through UC Santa Barbara computers that were hijacked by miscreants

who planted malware on them.

(viii) Anna Kournikova

In February of 2001, knockout tennis player Anna Kournikova was made even more famous as digital pictures of her were offered as bait in another email attachment virus. Like Melissa and ILOVEYOU, executing the attachment forwarded the message and virus attachment to every address in the recipient's address book.

(ix) Code Red

This worm scans the Internet for servers that are at risk, and when it finds one, copies itself to that server. The new copy then continues the search for other unwatched servers. Code Red also performs three other tasks replicating itself for the first 20 days of each month, defacing server's home pages, and attacking www.whitehouse.gov. It's been a couple of years, but I still see Code Red attack attempts on our servers. It's amazing that there are still unmatched servers out there.

(x)Nimda

Late in the week after the 9/11 terrorist attacks on the World Trade Center and the Pentagon, the Nimda virus flooded the Internet and attacked millions of computers worldwide. The virus used yet more sophisticated methods, including multiple approaches, to infect and replicate, and was tremendously successful despite the increased wariness of users and administrators due to previous high profile infections.

- The first approach took advantage of a flaw in IIS that allowed an attacker to navigate to any desired folder on the drive that contained the Web site, and then access files in it.
- The next approach used a mass mailer program that executes every 10 days. Like many other routines, it searches for email addresses on the system and replicates itself through email sent to those addresses.

6.0 SECURITY TOOLS

Securing information, services, systems and networks entails ensuring availability, integrity and confidentiality of resources, as well as non-repudiation of certain actions, and the authenticity of events or resources. Data security is only meaningful if it is applied for data and processes which

we are certain to be exact (notion of quality of data and processes) so that they may be stable over time (notion of data stability and service continuity).

(i) Data encryption

Encryption techniques make it possible to preserve data confidentiality, check data integrity and authenticate entities. There are two main types of data encryption system: symmetric (privatekey) encryption, and asymmetric public-key encryption. Various encryption algorithms exist. Irrespective of whether they operate in symmetric or asymmetric mode, they are founded on the use of keys. In general, how robust they are hinges on the ability to manage encryption keys in a secure manner, on the length of the key (the minimum length of the key is determined by the type of algorithm), and on the security of the physical and software platform in which the encryption algorithms are installed and run.

(ii) Symmetric encryption

In order to encrypt or decrypt a text, one needs a key and an encryption algorithm. If the same key is used for both operations (encryption and decryption), the encryption system is termed "symmetric". The sender and receiver have to possess and use the same private key to make data confidential and to be able to understand them. This poses the problem of managing the distribution of private keys .The main symmetric encryption algorithms are: DES, RC2, RC4, RC5, IDEA and AES.

(iii) Asymmetric or public-key encryption

An asymmetric encryption system is based on the use of a unique pair of matching keys. This double-key comprises a public key and a private key. Only the public key can be known to everyone, whereas the private key must remain confidential and be kept secret. The sender encrypts a message with the recipient's public key and the recipient decrypts the message with his private key. The main public-key encryption algorithms, named after their inventors, generally use keys of length ranging from 512 to 1024 bits, or sometimes 2048 bits. They are: RSA (stands for Rivest, Shamir, Adelman), Diffie-Hellman, El Gamal

(iv) Digital certificates

A digital certificate is the digital identity card of an entity (legal or physical person) or an information resource, subject of the certificate. It contains, among other things, the identity of the subject (holder), the public key assigned to the subject and the identity of the issuing body. The X.509 standard (directory authentication framework) offers an architectural framework for the establishment of an authentication service based on the use of digital certificates, and specifies the structure and format of a digital certificate. This standardized structure is adopted in many solutions on the market

(v) Trusted third party

Whatever name it may go by trusted third party (TTP), registration authority, certification authority, or certificate authority - the main function of the body setting up a public key infrastructure is to issue certificates vouching for the public key assigned to an entity (identify certificate). A certification authority is a trusted third party which issues digital certificates and serves to verify the validity of certain information

(vi) Secure IP protocols

The need to accommodate security requirements militated in favor of a revision of version 4 of the internet protocol. Moreover, there was also a need to provide for a wider range of addresses and increase the number of available internet addresses, as well as to allow dynamic allocation of bandwidth to support multimedia applications. As a result, a revised version of the IP protocol has been produced called "internet protocol next generation" (IPnG), or IP version 6 (Pv6).

(vii) IPv6 protocol

In 1994, the Internet Activity Board (LAB) addressed the security requirements of the IP protocol. Version 6 of the LP protocol (IPv6) includes authentication and confidentiality facilities.

(viii) IPSec protocol

With IPSec, the content of packets transported by the protocol can be made confidential. IPSec offers data confidentiality and authentication services at the level of transfer by the IP protocol, through the insertion of an authentication header (AH) or an encapsulating security payload

header (ESP).

(ix) Environment partitioning

The separation and masking of a private environment vis-a-vis the public internet is achieved through the installation of one or more firewall systems. A firewall is a system for filtering and, as the case may be, blocking data flows. It analyses the flow, authorizing it if it meets certain conditions, or otherwise rejecting it by partitioning a network one can create separate IP environments by making the access points of the networks one wishes to separate physically independent of one another.

7.0 PROPOSED SYSTEM FOR EMAIL (CONTAINING VIRUS) DETECTION

To virus detection we can choose a critical value C. If a computer shows the symptoms of sending e-mail with viruses to other computers more than C in very short time period T, so we can say this computer could be infected, But a normal user can also send emails to a list of users, so could be fall in this category, and in generally it could be happens .But there is a very big difference also in this event. If a virus send a e-mail to another computer, and as the mails opens any at any computer, then computer would become infected also, and will try to send the email address list available on that computer with the rate greater than C in time period T means like nuclear chain reactions. If User sends this mail, then this procedure happens rarely. After combining these two observations we have virus detection algorithm as follows

7.1 Email virus detection algorithm

1. Monitor regularly the number of emails with attachments sent by the nodes in the Lab (Network).
2. If a node Nl sent more than C Emails. Within Time period T, put all the recipients of the emails in a observe list.
3. If any host in the watch list sent more than C email within time period T, then virus infection in node Nl is confirmed.
4. If none of the Node in a observe list sent more than C Emails within time period T, the observe list is canceled.

Firstly, we decide the hosts that the virus control system has to take action on. Obviously, these hosts include all the hosts that have received virus emails. This means that the virus containment algorithm must record all these hosts. After the hosts are identified, they will be

isolated. By isolation we mean that all the emails with attachments sent from these hosts are blocked until the virus email is deleted. In order not to isolate hosts that have already deleted virus emails, we can use the following mechanisms if the users can be assumed to be honest and cooperative. After the virus control system block these identified host, the system sends an email to these hosts telling them the reason for the isolation. It also asks the user to delete virus emails. Once the user reads the email and deletes the virus email, he will send a reply to the virus control system and the system will remove his computer from the isolation list

8.0 RECOMMENDATIONS

For controlling cyber terrorism

- We have to Adopt Multidimensional Approach
- New technology must implement in Real Legislation
- International legislation should adopt
- Make cyber-education compulsory
- Global Surveillance Needed

8.1 How to Make Your Pc Secured

Protect Your Personal Computer

If you think that your home computer was safe from outside attacks, think again. Home computers are as susceptible as office computers to online attacks. Here are some extremely important guidelines for home computer owners.

1. Use the latest version of a good anti-virus software package that allows updating from the Internet.
2. Use the latest version of the operating system, web browsers and e-mail programs.
3. Don't open e-mail attachments unless you know the source. Attachments, especially executables (those having .exe extension) can be dangerous.
4. Confirm the site you are doing business with. Secure yourself against "Web- Spoofing11. Do not go to websites from email links.
5. Create alphanumeric passwords containing at least 8 digits. They should not be dictionary words. They should combine upper and lower case characters.
6. Use different passwords for different websites.
7. Send credit card information only to secure sites.
8. Use a security program that gives you control over "Cookies" that sends information back to websites. Letting all cookies in without monitoring them could be risky.

REFERENCES

[1] M. Chandrasekaran, S. Vidyaraman and S. Upadhyaya, SpyCon: Emulating User Activities to Detect Evasive Spyware, 2007, Performance, Computing, and Communications

Conference, 2007. IPCCC 2007.
[2] McAfee, Potentially Unwanted Programs: Spyware and Adware, 2005. http://www.mcafee.com/us/local_content/white_papers/wp_antiSpyware_s hadesofgray.pdf
[3] M. Boldt, B. Carlsson, Privacy-Invasive Software and Preventive Mechanisms, Systems and Networks Communications, 2006. ICSNC '06. International Conference, pp 21, Oct. 2006.
[4] Richard H. Stern, FTC cracks down on Spyware and PC hijacking, but not true lies, IEEE Computer Society, 2005.
[5] Spyware. www.us-cert.gov/reading_room/Spywarehome_0905.pdf
[6] Q. Hu, T. Dinev, Is Spyware an Internet Nuisance or Public Menace, Communications of the ACM. New York, Vol. 48, No. 8, pp. 61-66, August 2005.
[7] W. Ames, Understanding Spyware: risk and response, IEEE IT Professional, Vol. 6, No. 5, pp. 25-29, September-October 2004.
[8] Y. Lee, Kozar, K. A., Investigating Factors Affecting the Adoption of Anti-Spyware Systems, Communications of the ACM. New York, Vol. 48, No. 8, pp. 72-77, August 2005.
[9] W. Harrison, T. Bollinger, User Confidence – and the Software Developer, IEEE Software, Vol. 21, No. 6, pp. 5-8, November.-December 2004.
[10] T. Bollinger, Software in the Year 2010, IEEE IT Professional, Vol. 6, No. 6, pp. 11-15, Nov.-Dec. 2004.
[11] M. Wu, Y. Huang, Y. Wang, S. Kuo, A Stateful Approach to Spware Detection and Removal, 12th Pacific Rim International Symposium on Dependable Computing (PRDC'06), 2006, IEEE Computer Society.
[12] Moshchuk, T. Bragin, S. D. Gribble, and H. M. Levy, A Crawler-based Study of Spyware on the Web, 13th Annual Network and Distributed Systems Security Symposium (NDSS 2006).
[13] EarthLink Inc., "EarthLink Spy Audit," www.earthlink.net/about/press/pr_spyAudit/, April 2004.
[14] N. Arastouie, M. R. Razzazi, Hunter: An Anti Spyware for windows Operating System, information and Communication technologies: from theory to applications, ICTTA 2008.
[15] The silent epidemic of 2005: 84% of Malware on computers worldwide is Spyware, http://www.pandasecurity.com/
[16] O. Henchiri, N. Japkowicz, A Feature Selection and Evaluation Scheme for Computer Virus Detection, International Conference on Data Mining (ICDM2006)
[17] R. Moskovitch, C. Feher, N. Tzachar, E. Berger, M. Gitelman,S. Dolev, and Y.Elovici, Unknown Malcode Detection Using OPCODE Representation, ISI 2008, June 17-20, 2008, Taipei, Taiwan.
[18] C. D. Bozagac, Application of Data Mining based Malicious Code Detection Techniques for Detecting new Spyware, White paper, Bilkent University 2005.
[19] M. G. Schultz, E. Eskin, E. Zadok, and S. J. Stolfo, Data Mining Methods for Detection of New Malicious Executables, Proceedings of IEEE Symposium on Security and Privacy, pp.38-49, 2001.
[20] S. R. White. Open Problems in Computer Virus Research. Virus Bulletin Conference, 1998.
[21] D. Gryaznov Scanners of the Year 2000: Heuristics. In: The 5th International Virus Bulletin, 1999.
[22] I.H. Witten, E. Frank, Data Mining: Practical Machine Learning Tools and Techniques,

(Second Edition), Morgan Kaufmann, 2005.
[23] M. A. Maloof, Machine Learning and Data Mining for Computer Security: Methods and Applications, Springer, 2006.
[24] M. Wu, Y. Huang, S. Kuo, Examining Web-based Spyware Invasion with Stateful Behavior Monitoring, 13th IEEE International Symposium on Pacific Rim Dependable Computing, 2007.
[25] R. S. Sandhu, "Lattice-Based Access Control Models," IEEE Computer, 26(11), p. 9-19, 1993.
[26] R. Sellers, "SPYWARE – An Evolution in Process", SANS Institute, May 2004.
[27] J. Wang, P. S. Deng, Y. Fan, L. Jaw, Y. Liu, Virus Detection Using Data Mining Techniques, IEEE Security, 2003.
[28] T. Abou-Assaleh, N. Cercone, V. Keselj, and R. Sweidan. "N-gram-based detection of new malicious code". In Proceedings of the 28th Annual International Computer Software and Applications Conference -Workshops and Fast Abstracts - (COMP-SAC'04) -Volume 02, pp 41–42, 2004.
[29] D. Jurafsky and H. M. James. Speech and Language Processing. Prentice- Hall, Inc, 2000
[30] W. Cavnar and J. Trenkle. "N-gram-based text categorization." In Proceedings SDAIR-94. 1994.
[31] What Is Spyware?, Anton Chuvakin. http://www.windowsdevcenter.com/pub/a/windows/2005/11/22/what-is- Spyware.html
[32] O. Henchiri, N. Japkowicz, A Feature Selection and Evaluation Scheme for Computer Virus Detection, International Conference on Data Mining (ICDM 2006).
[33] J. Z. Kolter and M. A. Maloof. "Learning to detect malicious executables in the wild". In Proceedings of the 2004 ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, 2004.
[34] K.S. Reddy, S.K. Dash, and A.K. Pujari, "New Malicious Code Detection Using Variable Length n-grams", ICISS 2006, LNCS 4332, pp. 276–288,2006.
[35] Y. Elovici, A. Shabtai, R. Moskovitch, G.Tahan, and C. Glezer, "Applying Machine learning Techniques for Detection of Malicious Code in Network Traffic", Proceedings of the 30th annual German conference on Advances in Artificial Intelligence, Germany . pp. 44–50, 2007.
[36] R. Moskovitch, D. Stopel, C. Feher, N. Nissim, Y. Elovici, "Unknown Malcode Detection via Text Categorization and the Imbalance Problem", ISI 2008, June 17-20, 2008, Taiwan, 2008.
[37] http://csciwww.etsu.edu