Tracking Digital Footprints of Scareware to Thwart Cyber Hypnotism through Cyber Vigilantism in Cyberspace

Neelabh

Submitted in May 2011; Accepted in July 2012

Abstract - The characteristics of the Internet, which include digitization, anonymity, connectivity, mobility, and transnational nature; blur the traditional model of crime investigation / law enforcement and call for new strategies. Many simple yet popular malicious activities over internet are carried out by scammers / con artists largely through electronic mails and websites using cyber hypnotism, often in combination with distribution and propagation of malware. Such crimes of persuasion need to be managed through due diligence. Recently, an added web-based threat is recognized in the form of scareware which is making even the savviest of computer users their victim, and therefore, there is a need to focus on trying to detect such suspicious activity as quickly as possible in order to shut it down. An in-depth analysis of few scareware reveal that they have created many new and not so widely recognized online threats with inside intelligence by providing primary delivery mechanism for malware such as rogue anti-virus and anti-spyware, which are beyond the reach of many legitimate anti-virus programs currently in use. They may cause a Denial of Service (DoS) attack forcing the system to crash or even a Distributed Denial of Service (DDoS) attack. Looking at such unprecedented challenges in cyberspace, a policy of cyber vigilantism adopting an active defense rather than a reactive approach is contemplated. It is felt that in this age of mobile workforce, many of such people working as cyber analytics, or cyber-crime researcher may accomplish this work of community policing and play as proactive guardians of cyberspace.

Index Terms - Internet, Cyber Hypnotism, Con Artist, Scareware, Cyber Vigilantism.

1. INTRODUCTION

The Internet, as understood today, is a vast global network of computers storing information on every conceivable subject of interest to humankind. Its' original designers aimed to create a communication system between trusted people and organizations for academic and military purposes resilient in the face of a nuclear attack. There were no views to the security of the computers attached to neither these networks nor the information stored in these computers. The commercial use of internet came as an afterthought. Today, it has evolved from a mere means of communication to an open and insecure system of worldwide network. Real world's constraints such as time and space do not exist on it. National boundaries have little meaning in cyberspace and information flows continuously and seamlessly across political, ethical and religious divides. Even the infrastructure that makes of cyberspace (software and hardware) is global in nature. Because of this global nature of cyberspace, the existing vulnerabilities are also open to the world and to anyone, anywhere, who has sufficient capability to exploit them. These infrastructures are, therefore, being continuously probed for weakness and vulnerability by new breed of professional cyber criminals primarily motivated by huge financial gains. In recent years, several electronic mail frauds and scareware, herein discussed as crimes of persuasion, have brought to light the darker side of the Internet.

This paper examines the concept that industry, government and the public are essentially naked in cyberspace, with privacy diminishing, identity theft increasing, financial accounts and intellectual property becoming highly vulnerable to cyber criminals. Taking lessons from real-world incidences, this paper discusses attackers' technique in general terms, more particularly related to cyber hypnotism (i.e., hypnotizing people through internet by exploiting various human weaknesses and emotional vulnerabilities in cyberspace) and related crimes of persuasion including email fraud besides scareware (a type of malware). In this context, Hypnotism, as understood, is "a wakeful state of focused attention and heightened suggestibility, with diminished peripheral awareness, usually induced by a procedure known as hypnotic induction, which is commonly composed of a long series of preliminary instructions and suggestions". This is in contrary to a popular misconception that hypnosis is a form of unconsciousness resembling sleep[1]. Malware, also known as malicious code & software (e.g., viruses, Trojan horse, worms, keyloggers, scareware, spyware etc.), meant specifically to damage or disrupt a system irreparably and to steal the personal information and address books existing on the system in cache memory / records, by hijacking the browser and redirect to a phishing – con webpage. Evidently, many cyber-crimes, largely carried out through a series of hypnotizing emails, are often associated with malwares and warrant a constant vigilance at individual level besides better technical controls. It is noteworthy that majority of such cyber-crimes do not require a high level of

EC-Council Certified Incident Handler, CYBER COPS India
E-mail: neelabh@cybercops.in

technical specification and can be prevented through 'due diligence', nevertheless, sophisticated cyber-crimes demand an altogether different approach. Cyber Vigilantism, as visualized in this communication, is " a proactive policy to attack the attackers in an ethical way with restraint in a limited manner rather than adopting a soft policy of passive reaction." In turn, it will encourage good guys into action and discourage the bad guys in the near future.

2. E-MAIL FRAUD AND CYBER HYPNOTISM

Cyber-crime is regarded as computer-mediated activities which are either illegal or considered illicit by parties and which can be conducted through global electronic networks[2]. Conceptually cyber-crimes differ little from traditional crimes as they frequently involve perpetrators who have no physical presence at or even near the crime scene. In such crimes when no direct physical evidence exists, inferential evidence, or evidence that some aspect of the system has been modified as a direct result of the intrusion, is the primary source of clues. In fact, cyber-attacks come in two forms: one against data, the other on control systems. The first type attempts to steal or corrupt data and deny services. The vast majority of internet and other computer attacks fall into this category. Individuals, who wish to use computer as a tool to facilitate unlawful activity are finding that the Internet provides a vast, inexpensive, and potentially anonymous way to commit unlawful acts. The Net enables transaction between people who do not know, and in many cases cannot know each other's physical location. As of 2012, the estimated number of Internet users worldwide reaches 2,267,233,742[3]. Most of these users have electronic mail (email) accounts on one or more mail systems and emails are being utilized by cyber criminals as the vehicle of persuasion. According to Symantec, a security-software vendor, about nine-tenths of the 140 billion emails sent daily are spam (unsolicited bulk commercial emails); of these about 16% contain money-making scams including phishing attacks[4]. E-mail fraud relies on naïve individuals who put their confidence in 'get-rich-quick' schemes such as 'too-good- to-be-true' investments or offers to sell popular items at 'impossibly low' prices. In this, confidence tricks tend to exploit the inherent greed and dishonesty of their victims: the prospect of a 'bargain' or 'something for nothing' can be very tempting. Over the years; email has evolved from a means of easy communication to one of the cornerstones of a large-scale criminal economy. For example, Spam today is best known as a way to steal a person's identity and sensitive data or to gain access to corporate intellectual property and used as phishing[5]. The spam emails are often sent from Internet cafes equipped with satellite Internet at a very low cost. They consume significant resources of targeted computer and are used as a delivery mechanism for cyber-attacks. Spam often contains viruses, worms, scams, and drive-by download malwares. Symantec reports that 91.9% of email traffic is spam and that 95% of all spam is generated by botnets (i.e., malware infected remotely controlled computers)[6]. It may be noted that by opening spam, users open their machines and their entire network to become members of a botnet, which can compromise the entire network.

Phishing, is a variation on "fishing", " the idea being that bait is thrown out with the hopes that while most will ignore the bait, some will be tempted into biting"[7]. It is the act of attempting to fraudulently acquire sensitive information by masquerading as a trustworthy person or business with a real need for such information in a seemingly official electronic notification or message (most often an email, or an instant message)[8]. Phishing may lead to identity theft and fraud by finding out the users' personally identifiable information (PIIs) such as user name, passwords and credit card details typically for an economic gain by masquerading as a trustworthy entity in an electronic communication; such as pretending to be from a well-known organization, a legitimate online retailer, trustworthy companies, bank, government agency or someone claiming to be a prospective employer. Some phishing emails try to convince that something good will come from participation. More commonly, phishing attacks use email or malicious web sites to solicit personal, often financial information. Clicking a link in a phishing email typically takes one to fake website that may be related to even a scareware website. Common methods of installing malware in phishing attacks are carried out through fake advertisements or 'popup' windows on web sites. Experts suggest not clicking on links directly from a suspicious e-mail. Similarly, it may be mentioned that secure web sites use a technique called SSL (Secure Socket Layer), indicated by HTTPS:// instead of HTTP:// at the beginning of the address (the "S" stands for "Secure") and by a locked padlock icon which must be found either at the address bar or in the bottom right hand corner of browser window. A padlock appearing anywhere else on the page does not represent a secure site. It is also suggested if the first part of the web address consists of numbers; the site should probably not be trusted. Phishing attacks usually use a combination of email spoofing and web spoofing to trick people into giving personal and financial information. In particular, phishing and pharming (luring people to disclose sensitive information by using bogus emails and websites) are two popular security threats that netizens and financial institutions are facing at large. Pharming is a hacker's attack aiming to redirect a website's traffic to a bogus website where they harvest the users' information[9]. Pharming can be conducted either by changing the hosts file on a victim's computer or by exploitation of a vulnerability in DNS server software.

An added threat in new millennium is the recognition of internet as a useful tool by scammers/con artists, using hypnosis as a tool to make money by exploiting various human weaknesses and emotional vulnerabilities. Hypnotizing people through the internet has a greater range. It allows the scammers / con artists to manipulate the victim's mind and play with it like revealing something that he / she doesn't want to reveal or making him / her to do something else. Given email's nature of human to human communications, it is being used as a social engineering vehicle by con artists/scammers. It is observed that many of the cyber-crimes related to data theft and identity theft display a judicious mix of cyber hypnotism and malwares. Recognizing the convergence of cyberspace and hypnotism, the author has used cyber hypnotism as a basket term for the type of scams and frauds, referred as crimes of persuasion, popularly known as London scams, Nigerian fraud, Canadian fraud, Romance scam, Lottery scam etc. These are scams that appeal to people's greed, goodwill or other emotions to use the victim to provide the access and assistance to information, the money or other resources, that are the target of the criminal. What is common in all these scams is that scanned versions of official documents are emailed to potential victims in order to convince the genuineness of the transaction. Internet users, now, need to be more vigilant as new and more insidious mind tricks arise every day, especially if a message is either too good or too bad to be true. Users are too often seduced by a wonderful offer or alert. It is suggested to be suspicious if someone contacts unexpectedly and asks for personal information. Appeals to achieve happiness via increased wealth, relationships or health are tempting people to become scapegoat. It is noted that if the message appears to be one of gain then promotion-focused individuals tend to be motivated and get attracted to go ahead, whereas others who are prevention-focused individuals, tend to be motivated to avoid the sky falling i.e., heavy losses. Both types of individuals are illusioned by legitimacy and/or associated with such messages. In cyberspace, for instance, in order to convince the legitimacy of the email, all publicly available highly-personalized information is included by scammers/con artists in such emails. Furthermore, they create a story line in such a way that it induces the emotional sensitivity of the innocent human beings, and then they ask either for wire transferring the money or provide a website link within an email, which serves many purposes. For example, the link may be relating to a login page of any financial institution so as to get the PIIs from the legitimate users, resulting not only in the theft of login information but also in the identity theft as well as credit card fraud. The link may be relating to a login page of any email account like Gmail, Yahoo, RediffMail etc. where the user enters his / her login information and unknowingly helps the con artists in delivering his / her secret credentials. Afterwards, the scammer / con artist may use the contacts present in the address book and will try to scam other people from the contacts. Similarly, the link may be related to a legitimate website embedded with blended malware which makes the website visitors' machines a cyber- victim. However, this remains hidden from the first-owner of the computer system. By this way, the scammer/con artist creates a backdoor in the computer system and is able to monitor and control the computer system remotely. This information is generally sold in the underground market of internet. All such incidents are happening because people are hypnotized to such an extent that they are ready to believe what the scammers / con artists are trying to convey. Furthermore, a widespread use of commodity operating systems and software products delivering rich functionality but lacking security has aggravated the problem.

Investigation of cyber-crime cases and appraisal of threat data analyses of online crimes especially related to cyber hypnotism reveals that many of these are being carried out with basic equipment and a simple scheme with little efforts. Hence, contrary to popular belief, most of such attacks perpetrated against computer systems do not require a high level of technical sophistication, yet present an unprecedented challenge for law enforcement authorities. As technologies become more user-friendly, computer-users require less computer knowledge and are, therefore, more vulnerable to cyber-crime, home users perhaps the most. Often poorly protected, personal computers are a favorite target for such criminals.

3. CYBER VIGILANTISM: A DISCUSSION

McAfee reports a 660% rise in scareware over the past two years, and a 400% increase in reported incidents in 12 months. It also reports that cybercriminals make profits upwards of $300 million worldwide from scamming consumers with scareware [10]. A study conducted by U.K. Government in February 2011 on the cost of cyber-crime reports that U.K. citizens are losing £ 30m due to scareware and fake anti-virus[11]. Furthermore, it is a rgued that fake anti-virus software operation generate many millions of dollars and investing this dirty money into Internet Service Providers (ISPs) for shady dealings is also emerging as a very sensible move for bad guys. ISP's are often accused of not doing enough to police illegal traffic. In order to curb scareware, it is felt that anti-virus deployment in computer systems must be made mandatory while hiring an internet connection from ISPs or their vendors, which may be audited by ISP's at the time of providing internet services to their potential customers and may be counterchecked by cyber vigilantes. It is observed that cyber criminals are increasingly using highly reputable and popular legitimate websites and social networking pages to infect computers.

Looking at such unprecedented challenges, the author strongly advocates a policy of involving high tech cyber security experts and encouraging cyber vigilantism with government as regulatory authority to co-ordinate them. During cyber-crime investigations, the exact nature and positioning of cyber-crime evidence can be crucial to unraveling the chain of events. Time stamps in logs, records of network activity, new directories and files created by the attacker, incoming /

outgoing mail or other packets during the period when the intruder was actively exploiting the system; all of these are important pieces of the overall puzzle. It is suggested that these professional cyber vigilantes can be utilized to gather such evidences. Cyber Vigilantism by private citizens is a response to their frustration with the number of rogue sites in operation and what they believe is the unwillingness or inability of our government to take them down. It is felt that conventional law enforcement just can't match the skills needed. Besides, one can't trust law enforcement to keep ones secrets from becoming public knowledge. It is worth to mention that after 9/11, it is self-styled vigilantes who came to America's rescue. Similarly, Cyber Vigilante Groups may be used as a source of information in the Figure1 against fraud, wherein consuming the bandwidth of fraudulent banking and lottery sites in an attempt to force them off the internet. It is learnt that few of the cyber vigilantes are open source cyber analysts who also visit extremist sites to glean information. One of the most famous examples of such Cyber Vigilante Groups is The Jester (th3j35t3r) who forces off Cyber Jihad websites[12]. They can offer advise and tools on how to avoid scammers and list suspected fraudulent websites. They can search logs of Internet service providers for "attack packets" and try to trace where they are coming from and who is behind them. They can also assist when businesses are faced with the first manifestations of cyber-crimes, such as threats besides educating internet users so that they take basic precautions when surfing the web. In addition, cyber vigilantes may also be utilized for website and domain ratings to benefit users. It is worth to record that most interesting action occurs behind the scenes, wherein security vendors, internet service providers, domain name registrars and some of the most talented individual researchers globally communicate every day on new attacks, compromises, bots and threats. Malware and exploit samples, locations of compromised hosts and information on crime ware are shared as quickly as the information is generated. Most importantly, these non-governmental people, many of them working for free, are all there working together as cyber vigilante to thwart various cyber threats. Such voluntary security professionals/academia take reports every day from the internet provide timely and actionable information on botnets and malware threats and also pass this information to the public.

4. SCAREWARE: FORENSIC RESEARCH METHODOLOGY

Scareware is malware masquerading as free or trial anti-virus software or some other free online scam[13]. In this context, the author while performing the routine activities in the month of July 2010 in Computer-Aided INvestigative Environment (CAINE), a Linux operating system that offers a complete forensic environment, received an email message of an international cyber security conference (Figure 1). Since the email was highly personalized, hence, the author thought it to be a benign one. It is noteworthy that the email was received in the inbox and not in the spam. It was containing a website link of the international conference's website. In order to know more about the theme and topics of the conference, the author clicked on the given link. The website too looked like a legitimate one. After few seconds, the author observed a pop-up alert with a warning message of privacy violations. It gave an impression as if a trial version of anti-virus software had scanned the system under reference but unable to clean these privacy violations. The popup alert also displayed the recommendation to purchase full version of the trial version to remove privacy violations (Figure. 2).

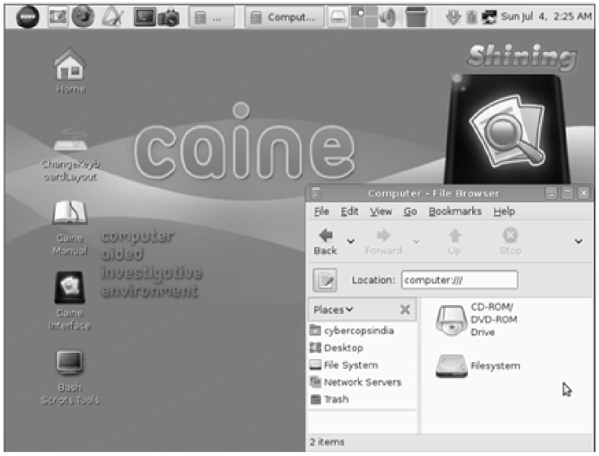
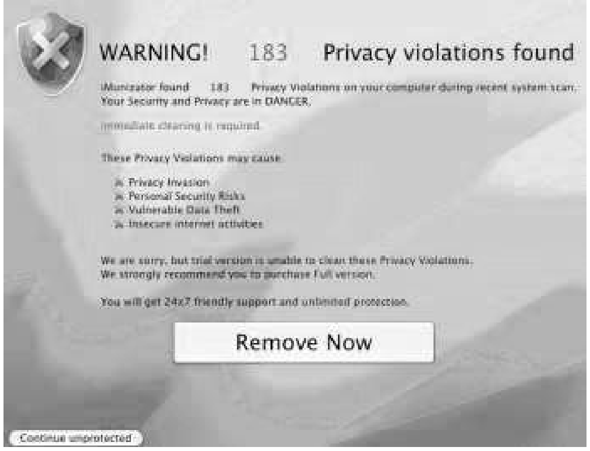


Figure 1: "CAINE Operating System Environment"



WARNING! 183 Privacy violations found

iMunizator found 183 Privacy Violations on your computer during recent system scan. Your Security and Privacy are in DANGER.

Immediate cleaning is required.

These Privacy Violations may cause:

- Privacy Invasion
- Personal Security Risks
- Vulnerable Data Theft
- Insecure internet activities

We are sorry, but trial version is unable to clean these Privacy Violations. We strongly recommend you to purchase Full version.

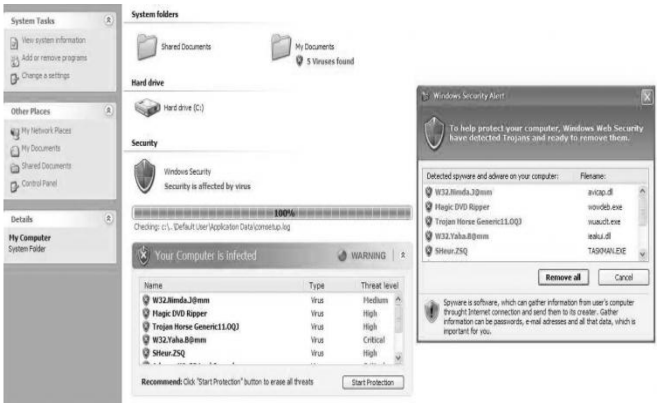
You will get 24x7 friendly support and unlimited protection.

Figure 2: "Popup Alert"

After selecting 'Remove Now' option, an Antivirus XP Professional tool got downloaded, which revealed that the system is infected with serious threats displaying a full-screen image of My Computer's environment that always appear in Microsoft Windows XP, with a message to remove the Viruses and Trojans found in the system (Figure

3). The Windows Operating System typeface (a look similar to the 'My Computer' in Windows XP environment) raised an immediate suspicion for further investigation about its genuineness since the author was working in a Linux environment as shown in the Figure. 1. Hence, it was decided to carry out further investigation.

Evidently, the threat warning was a fake one probably a scareware (rogue anti-virus & anti-spyware program) attack. Usually, scareware sellers use popup advertisements deliberately designed to look legitimate using the same typefaces as Microsoft and other well-known software providers. They appear, often when the user is switching between websites, and falsely warn that a computer's security has been compromised. If users click on the popup message, they are directed towards another website where they can download the fake anti-virus software supposedly needed to clean up their computer.



Checking: c:\..\Default User\Application Data\comsetup.log

Name	Type	Threat level
W32.Nimda.J@mm	Virus	Medium
Magic DVD Ripper	Virus	High
Trojan Horse Generic11.OQJ	Virus	High
W32.Yaha.B@mm	Virus	Critical
SHeur.ZSQ	Virus	High

Recommend: Click "Start Protection" button to erase all threats

To help protect your computer, Windows Web Security have detected Trojans and ready to remove them.

Detected spyware and adware on your computer:	Filename:
W32.Nimda.J@mm	avicap.dll
Magic DVD Ripper	wowdeb.exe
Trojan Horse Generic11.OQJ	wuauclt.exe
W32.Yaha.B@mm	ieakui.dll
SHeur.ZSQ	TASKMAN.EXE

Spyware is software, which can gather information from user's computer throught Internet connection and send them to its creater. Gather information can be passwords, e-mail adresses and all that data, which is important for you.

Figure 3: "Fake Warning of Infection (AntiVirus XP Professional)"

After clicking on the "Remove All" in Figure. 3, a website opened having URL address as www.scan4you.biz, and IP address as '85.31.101.148' which was reverse mapped as '85.31.101.148.static.nano.lv' with the Route / AS as '85.31.96.0/21' / '43513'[14]. On further forensic analysis of the popup and the website, it was found that the image shown in the website was hosted at "http://i080.radikal.ru/1004/c9/760db777d446.jpg" (Figure. 4).

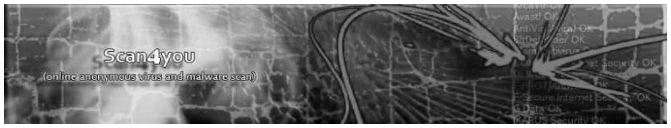


Figure 4: "Image of Website from where Scareware was downloaded"

On clicking the 'Buy Now' button shown in the website, a fraudulent payment page opened asking for all PIIs as well as financial information (viz. username, password for login into the anti-virus account, email id, credit card number, PIN number, issue/expiry date, full name of the card holder). Further details of the payment page are given in Table 1.

URL of Payment	**4-open-davinci.com**
Hosted IP Address	92.241.177.188
ISP	OAO Webalta
Location	Yoshkar-ola, Russia

Table 1: "Fraudulent Payment Page Details"

Instead of providing the information on the fraudulent payment website, the author registered the scareware by reverse engineering the downloaded malicious tool for further investigation in Windows XP environment. After installation, at the very first instant following major changes were observed:

1. Task Manager was disabled
2. Malfunctioning of [Ctrl] + [Alt] + [Delete] command
3. 'Folder Options' disabled
4. New registries were created, and the existing ones were modified

Default start page, & default search engine of Internet Browsers were changed to www.lameplaying.com/index.php/database.

Furthermore, following files were being created in each and every folder with hidden attribute selected by default:

1. tsjgiq.exe
2. khx <no extension>
3. khy <no extension>
4. <foldername>.EXE i.e., copy of each folder with an extension of .EXE

Apparently, all the above files were using rootkit technique. A rootkit is software that enables continued privileged access to a computer while actively hiding its presence from administrators by subverting standard operating system functionality or other applications[15]. It may be noted that once a rootkit is installed, it allows an attacker to mask the ongoing intrusion and maintain privileged access to the computer by circumventing normal authentication and authorization mechanisms.

Later on entering the URL of Gmail.com in Mozilla Firefox web browser, it opened a website www.lameplaying.com/index.php/database (IP address: 67.215.65.132) demonstrating possibility of Pharming.

Furthermore, network forensic was carried out by installing an Intrusion Detection and Prevention System (IDPS) in order to monitor the network activities, supposedly being carried out after the installation of scareware. It indicated that the scareware was continuously sending packets with variable size (in bytes) to an IP address with following log analysis data (Table 2).

Hosted IP Address	92.241.190.172
Company / ISP	Heihachi Ltd. / OAO Webalta
Location	Moscow, Russia

Table 2: "Details of Scareware to external IP Address"

It is noteworthy that although an internet connection of 2 Mbps (= 2,048 Kbps) was being used, there was a significant change in the network bandwidth before and after the installation of scareware that can be populated as in Table 3 and Table 4, respectively.

Ping	Download	Upload	Total Bandwidth
34 ms	512 Kbps	460.8 Kbps	2048 Kbps

Table 3: "Before installation of scareware"

Ping	Download	Upload	Total Bandwidth
96 ms	32 Kbps	8 Kbps	2048 Kbps

Table 4: "After installation of scareware"

Network forensic on the packet captured and the log files obtained from IDPS revealed that multiple requests and information were being sent as given in Table 5.

IDPS logs indicated port ranges between 1888 & 2132. Furthermore, for the IP address 77.91.227.248:2129, the remote system's MAC ID (i.e., machine address) was found to be 00-19- E0-A0-B2-8E. A route map of jebena.ananikolic.su is given in Figure. 5.

Protocol / URL	Port No.	Country	IP Address
jebena. ananikolic.su	2129	Moscow, Russia	77.91.227.248
UDP	2132	Moscow, Russia	92.241.190.130
UDP	2132	Moscow, Russia	92.241.190.172
UDP	2132	Moscow, Russia	92.241.190..237
UDP	1888	Brno, Czech Republic	89.102.0.150
http://search alligator.com/	80	Bellevue, US	8.5.1.41

Table 5: "Details obtained from network forensic"

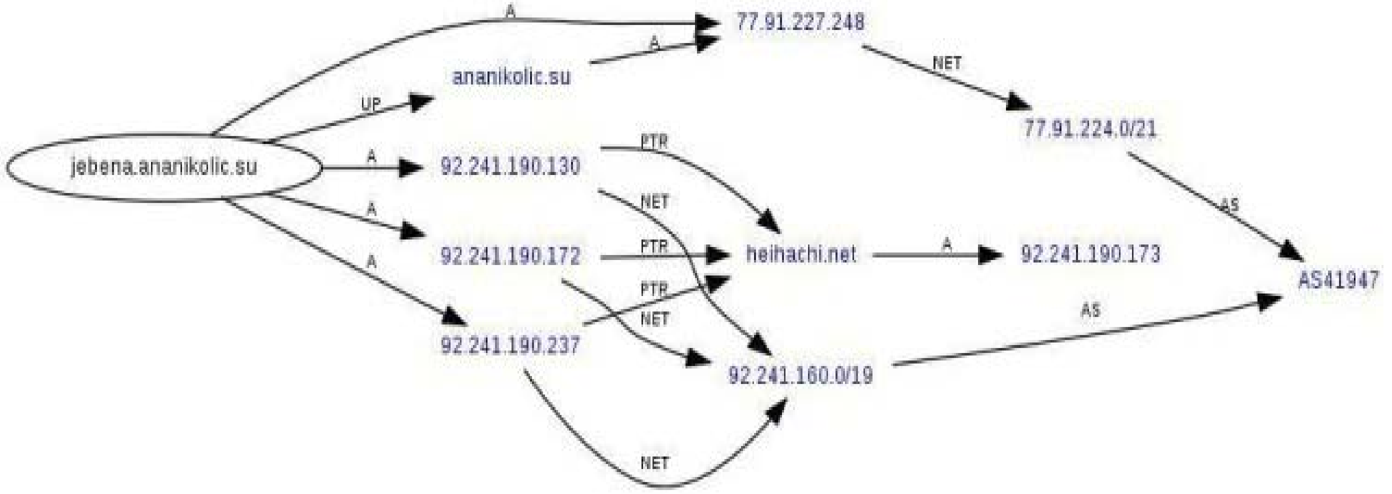


Figure 5: "Route Map of jebena.ananikolic.su"

Additionally, when the scareware was run in a network environment, there were multiple PING requests being relayed with payload (Table 6).

Protocol	Port No.	Request Type	Information
ICMP	6	Type 8 (Echo Request)	BOOTPS DHCP Server
SSDP	190		239.255.255.250

Table 6: "Scareware in a Networking Environment"

On further investigation, it was revealed that by using IPNAT (IP Network Address Translator) a request list was being sent at a very short but regular interval to the Russian IP addresses containing following parameters:

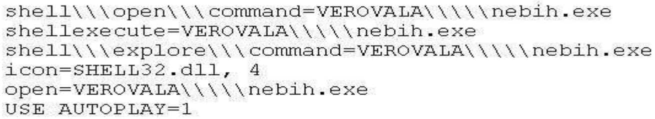
1. Subnet mask
2. Domain name
3. Router
4. Domain Name Server

Finally, the source file was located which was functioning as scareware having following aliases. Interestingly, these aliases were changing their names after every reboot randomly from the following ones:

NEBIH.EXE	:	141,824 bytes
RMHZB.EXE	:	138,752 bytes
1412294.EXE	:	140,800 bytes
86221.EXE	:	133,120 bytes
73911852.EXE	:	size was varying after every click

After performing intensive malware forensic, some very interesting information was uncovered. These were:

(1) Shell Command of Scareware:



```
shell\\\open\\\command=VEROVALA\\\\\nebih.exe
shellexecute=VEROVALA\\\\\nebih.exe
shell\\\explore\\\command=VEROVALA\\\\\nebih.exe
icon=SHELL32.dll, 4
open=VEROVALA\\\\\nebih.exe
USE AUTOPLAY=1
```

Figure 6: "Scareware shell command"

Here, the command icon=SHELL32.dll, 4 as shown in Figure. 6 was actually trying to conceal its icon as shown in number 4 (Figure. 7):

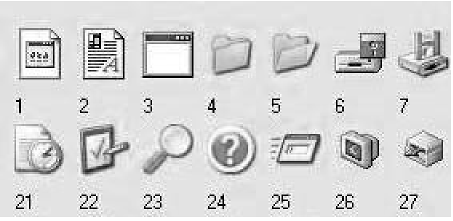


Figure 7: "SHELL32.dll icon graphics codes"

(2) MD5 hash value of NEBIH.EXE is as under 04509f3c5ef5b90a7addc09e65454fcc350745a39

(3) Following website links were found:
1. www.egydown.com (website for Cracked software),
2. www.filestube.com (malicious search engine),
3. www.thepiratebay.org (torrent website),
4. jebena.ananikolic.su (pornographic contents)

(4) Additionally, an encrypted HTML file was also revealed on the following path: C:\Documents and Settings\<username>\local settings\temp\cfircyh => HTML.Crypted!IK
It appears that to avoid detection by antivirus software, authors of HTML.Crypted!IK malware use browser features like JavaScript and VisualBasic Script. These scripts are small and very often quite simple encryption routines hiding the malicious parts of the script. Till date, the author isn't able to decrypt the HTML file.

(5) VEROVALA and NEBIH.EXE was showing a unique behavior in that it was using the same file icon as the antivirus software installed in the system under reference. Perhaps, it was done in order to fool those victims / users who just click on the icon but never read the full filename (with extension). As soon as any Plug-and-Play (UPnP) device was inserted, this file used to copy itself into it with the hidden attribute selected by default.

(6) Behavioral Pattern of VEROVALA / NEBIH.EXE: The registry values added to the system as soon as the USB drive is inserted were:
1. HKEY_USERS\.DEFAULT\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced|Hidden
2. HKEY_USERS\S-1-5-21-4058357071-1071901202-2123665184-1000\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced|Hidden
3. HKEY_USERS\S-1-5-18\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced|Hidden
4. HKEY_USERS\.DEFAULT\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced|Hidden
5. HKEY_USERS\S-1-5-21-4058357071-1071901202-2123665184-1000\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced|Hidden
6. HKEY_USERS\S-1-5-18\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced|Hidden
7. HKEY_USERS\S-1-5-21-4058357071-1071901202-2123665184-1000\Software\Microsoft\Internet Explorer\Main|Default_Search_URL
8. HKEY_USERS\S-1-5-21-4058357071-1071901202-2123665184-1000\Software\Microsoft\Internet Explorer\Main|Search Page
9. HKEY_USERS\S-1-5-21-4058357071-1071901202-2123665184-1000\Software\Microsoft\Internet Explorer\Search_Assistant
10. HKEY_LOCAL_MACHINE\Software\Microsoft\Internet Explorer\Main|Start page

(7) RMHZB.EXE created following registry keys:
1. \Registry\Machine\Software\Microsoft\Windows NT\CurrentVersion\Winlogon
2. C:\documents and settings\<username>\application data
3. My Computer\HKEY_LOCAL_MACHINE\Software\Microsoft\WindowsNT\Current Version\Winlogon\Taskman

(8) RMHZB.EXE and NEBIH.EXE is seen to perform following behavior:
1. Uses rootkit technologies to conceal its presence,

interrogation or removal.

2. Found on infected systems and resists interrogation by security products.
3. Has code inserted into its Virtual Memory space by other programs.
4. Writes to another Process's Virtual Memory (Process Hijacking)
5. Created as a Process on Disk.
6. This Process deletes other processes from disk.
7. Crashing down the computer terminals arbitrarily.

Currently, a number of digital tampering detection techniques are available [16]. Interestingly, for further confirmation when author contacted www.virscan.org on 25th September, 2010 and submitted sample of NEBIH.EXE the result was astonishing. Out of 35 malware scanners existing on the website none was able to show that its' a scareware or a malware. Everyone showed it as a clean file. However, on 27th September, 2010 when author again contacted the abovementioned website, the result was that 11% i.e., 4 out of 35 scanners found it as a malware[16].

5. SCAREWARE: IMPLICATIONS

Tracking digital footprints of scareware samples under study indicate that a Denial of Service (DoS) attack using the Universal Plug and Play (UPnP) NOTIFY directive can be carried out by sending a malicious UDP packet to port 1900 containing a Simple Service Directory Protocol (SSDP) advertisement. An attacker can force the Windows client to connect back to a specified IP address and pass on a specified Hypertext Transfer Protocol (HTTP) or Hypertext Transfer Protocol Secure (HTTPS) request. If the system that the victim is attempting to contact for the device description is configured to "echo" such requests, the system will enter an infinite download loop that will quickly consume the system's resources and cause it to crash. It may be mentioned that denial of service is considered as one of the most difficult attacks to detect [18].

Additionally, a distributed denial of service (DDoS) attack using the UPnP NOTIFY directive can also be launched. It is similar to the first exploit, except the attacker sends the SSDP announcement to broadcast addresses and multicast. Multiple machines reply to the IP address to obtain the device description performing a DDoS attack against the system. This was seen when author tested the scareware in a networking environment where multiple systems are connected to the Internet.

6. CONCLUDING REMARKS

Malware is widely available on the internet for anyone wanting to cause mischief, theft, espionage or cyber-crime. The majority of internet users worldwide have fallen victim and they feel incredibly powerless against faceless cyber criminals. The fundamental issue is that there is a law enforcement model that's geographically based, but there's no geography on the internet. An in-depth data analysis of crimes of persuasion including the case study under reference demonstrates that many of the popular cyber-crimes are related to data theft and identity theft and display a judicious mix of cyber hypnotism and malwares. Such crimes can be handled, to a large extent, with constant vigilance at individual level in combination with safe security practices including deployment of malware threat mitigation controls. On the contrary, sophisticated cyber-attack in the form of scareware demands a better and more coordinated strategy on national level, which is required to be implemented by developing a suitable corporate defense plan including involvement of cyber vigilantes to ensure stronger cyber security. It is evident from present study that in such a scenario, when the branded and reputed anti-virus/anti-spyware vendors are unable to detect such well-crafted and encrypted malware planted by the clever but malicious entrepreneurs, the common man is left with no choice. Neither the local law enforcement agencies are equipped to cater the victim's need, nor the government with their policies. Furthermore, the scareware scam is hard for police or other law enforcement agencies to investigate because the individual sums of money involved are minuscule. Nonetheless, these cyber criminals strike time and again. Hence, the author advocates that to discourage criminals and to instill faith in the digital medium at large, there is an urgent need to coordinate all cyber vigilantes. Undoubtedly, proactive security is need of hour wherein the central government may act as a regulatory authority for these cyber vigilantes' supposedly high tech cyber security experts, who, in coordination, may prove valuable assets to safeguard the national economy in an unsafe cyberspace and to disseminate knowledge and information related to it.

ACKNOWLEDGMENT

The author expresses his deep sense of gratitude to Anil K Saini, USMS, GGS IP University, Delhi, for his valuable suggestions and encouragement. Thanks are also due to anonymous reviewer of Journal – BIJIT for valuable suggestions.

REFERENCES

[1]. Professional Clinical Hypnotherapists of Australia. Frequently Asked Questions. Retrieved June 23, 2012, from http://www.pcha.com.au/hypnotherapy-faq.html.

[2]. International Telecommunication Union (2009, May 12). ITU Publication on Understanding Cybercrime: A Guide for Developing Countries. Retrieved June 23, 2012, from http://www.itu.int/ITU-D/cyb/cybersecurity/projects/ crimeguide.html.

Continued to page no. 473