The Digital Insider: Backdoor Trojans

Tom Kellermann, CISM and Yumi Nishiyama
The World Bank
Integrator Unit
December 8, 2003

Acknowledgements

The authors would like to give special thanks to the insights and contributions of the following individuals: Forrest “Skip” Allison, Jerry Dixon, Ken Dunham, Eduardo Gelbstein, Thomas Glaessner, Valerie McNevin, Shane Miller, Mudge, and Dave Thomas.

I. Introduction

While the traditional "Trojan horse" dates back to the days of ancient Greece in the classic fable of Helen of Troy, modern day Trojan Horse programs are smaller, digital, and far more prolific than in the days of Troy.[1] Trojans cloak malicious code by appearing as innocuous attachments in order to gain access inside a user's computer system. Once inside, they can rapidly reproduce and spread worldwide in a matter of minutes, performing damaging acts along the way. Symantec statistics state that 994 unique instances of malicious code, including viruses and worms, were introduced on just Microsoft Windows alone through 2Q 2003. New breeds of malevolent code can delete security software from infected systems, and are armed with advanced capabilities that allow them to essentially act as miniature processors. These include code that: contains its own Simple Mail Transfer Protocol (SMTP) server, acts as spyware, installs keystroke loggers, executes programs on its own, searches and destroys files in local and shared directories, and even terminates software programs.

In recent months, this rapid global proliferation of increasingly intelligent malicious code has come accompanied by a harmful attack method: Trojans that install backdoors into compromised network systems so that they may engage in malicious activity from within an infected system and then send data to remote locations. The Trojan code will disguise itself as an innocuous program, email, or image, etc., and when succeeding to obtain access to a system, the Trojan can unleash harmful code such as installing backdoors. Once the backdoor is established, any perpetrating cracker, hacker, or others with knowledge about the opening can use it for system entry. Because characteristically Trojans do not reproduce, they often combine forces with worms and viruses for added effectiveness. Thus, what appears to systems administrators as a single attack can oftentimes be a multi-faceted one in which the virus or worm acts as a smokescreen for another strike to the network. A previous World Bank Integrator Unit publication titled, "Blended Electronic Security Threats: Code Red, Klez, Slammer, and Bugbear" (June 2003) illustrated this phenomenon of combined attacks. The current paper builds upon the blended threat piece in order to highlight an advanced paradigm of attack methodology—that of the new insider threat.[2] Through the use of malicious Trojan horse programs, a remote hacker can essentially act as an insider threat, operating at will within a compromised system.

II. Today's Trojans

Since the first known instances of Trojans, they have evolved into tools for miscreants seeking to meet specific goals. The first Trojan computer infection is believed to have appeared in 1986 as a shareware program called "PC-Write."[3] Disguised as Quicksoft's PC-Write version 2.72, many users thought they were downloading a word processing program, but were instead, downloading infected files.[4] When these users launched what they believed to be PC-Write 2.72, they instead executed the PC-Write Trojan. The

---

[1] The Greeks had attempted to penetrate the gates of Troy for over a decade, with no avail. The Greek militants finally resorted to more of sly attempt, building a large wooden horse and offering it up to the people of Troy (Trojans) as a gift. The Trojans brought the horse in to the city and promptly started to celebrate their victory. In the small hours of the morning, several platoons of Greek warriors hiding inside the wooden horse unsealed the belly of the horse, and climbed down from it. Silently, they killed the Trojan sentries at all the city gates. The gates were then opened to the bulk of the Greek army, who had returned under the cover of darkness and unnoticed by the celebrating and drunken Trojans. Today, this term is used to refer to malicious or harmful code concealed inside seemingly harmless programming or data. Once the malicious code is delivered within a user's gates—including firewalls, intrusion detection systems, etc.—it allows outside users to obtain remote control of infected machines.

[2] For additional information, see Tom Kellermann and Yumi Nishiyama, "Blended E-Security Threats", June 2002, The World Bank, Washington D.C.

[3] For additional information, please see: http://www.cknow.com/vtutor/vthistory.htm.

[4] In fact, Quicksoft, the company that produced PC-Write, did not release a version 2.72.

PC-Write Trojan performed two actions: wiped out the file allocation table (FAT)[5] and formatted the hard drive so that all saved data was deleted.[6] Because Trojan horse programs are unable to self-replicate, they are often associated with viruses and worms that provide them with spawning, as well as transmission, capabilities. Box 1 provides a history of worms.

Box 1: A Brief History of Worms

In November 1988, a programmer named Robert Morris launched the first prolific worm. Short for "write once read many," the "worm" was a self-replicating computer program released into the internet as an experiment on diffusion. Though Morris originally launched the program at MIT, within a few hours, the worm had rendered computers throughout the university system, military, and medical research facilities, useless. The worm was only intended to spread; instead, it spread and, on account of bugs in the software, crashed many systems along its path. In fact, the United States General Accounting Office (GAO) estimates that the total cost of havoc wreaked by the "Morris Worm" totals approximately USD $10-$100 million.

Ironically, when Morris realized the full implication of what he had done, he and a friend disseminated a warning message throughout the network. However, on account of system breakdowns, or because people had terminated their connection to the network entirely, the message did not reach users quickly enough, or rapidly enough. Morris was eventually charged over $10,000, sentenced to community service and three years of probation, for violating the Computer Fraud and Abuse Act.

Importantly, this is an example of unintended consequences. This computer program serves as the foundation upon which modern day worms have been created. Only now, the trend is to harness the capabilities of these powerful programs in order to launch targeted online attacks.

While today, Trojans still conduct acts of file deletion, they have also become sophisticated tools tailored for a variety of purposes including financial gain, hacktivism, and espionage. The following illustrate ways in which Trojan horses, which historically required social engineering or phishing methods to manipulate users to instigate their malicious activity, have now become far more devious, efficient, and almost self-sufficient entities.

Trojans as Moles—

Malicious code is increasingly used for illegal surveillance purposes. Many Trojans now contain keystroke logging and/or password sniffing capabilities so that sensitive user data can be collected. Others contain programs capable of taking screen shots of the infected computer's files. In most cases, this harvested data is stored in a temporary file and then emailed to remote miscreants. An example of this type of spyware is the recent Sysbug Trojan, spread in November 2003. This Trojan mole gathers user information from infected computers then disseminates the data to multiple email addresses coded within the Trojan.[7] Moreover, these programs may be combined with certain worms that inherently contain their own Simple Mail Transfer Protocol (SMTP) server. With its own SMTP server, the blended threat can engage in communications activities (e.g., sending e-mails) on its own, rather than having to establish a connection to an SMTP server on the infected machine.

Opening Backdoors—

While Trojans may have surveillance capabilities, to be effective, communications channels must exist through which Trojans inside the infected machine and remote hackers/crackers send and receive data. Quite possibly the biggest threat posed by a Trojan infection is its ability to open "backdoors" in a

[5] A system a PC uses to organize contents on the hard drive.

[6] http://www.dragonpc.biz/hn101/security_trojan.htm

[7] For addition information, please see the F-Secure virus definition of Sysbug at: http://www.f-secure.com/v-descs/sysbug.shtml.

compromised system, allowing a malevolent user(s) to remotely control the infected computer and subsequently have access to the computer's network. Once a Trojan horse has been introduced into a user's computer system it plants a program that searches for vulnerable, open ports. When it locates a target, the Trojan uses this open port as a communications channel. Through these backdoors, remote crackers can launch malicious code to vandalize, alter, move, or delete files on the infected computer. They may also harvest sensitive user information such as financial account numbers and passwords from the victim's locally stored data files, and then transmit this information through the backdoors. The Sysbug Trojan is a recent example. Sources state that Symantec has seen a 50% rise in compromised backdoors.[8]

Collaborating with Malicious Bots—

Another way in which remote hackers and crackers manipulate tunnels in a compromised system is by launching bots through Trojan horse programs. Short for robot, a bot is a script that autonomously imitates a legitimate user or client computer. Bots, however, are "intelligent" applications that are programmed to find and analyze information on the Internet. Originally created for data mining functions, bots are capable of crawling across the Internet in search of specific information, utilizing a form of adaptive intelligence to 'make decisions' along the way for more efficient processing. Recently, however, many Trojans have combined powers with bot technology for malicious purposes. Bots can establish connections with an infected host's Internet Relay Chat (IRC) channel.[9] They then act as proxies, standing by the open IRC channel, awaiting commands by a remote cracker. The GTBot Trojan is an example of a weapon that will unleash an IRC bot.[10]

Malicious IRC bots can be programmed to do anything from flooding users' machines in massive Distributed Denial of Service (DDoS) attacks, to launching synchronized fanning attacks, or spreading worms that infect other user machines with backdoors. There are even armies of IRC bots standing by to launch what sources fear is a large-scale, coordinated attack. In fact, CERT states that GTBot Trojan has infected over 140,000 systems,[11] thus converting them from harmless user computers, to soldiers standing by awaiting instructions from a remote commander to launch a potentially harmful attack. These compromised systems, also known as zombie bots, can relegate processing power from the legitimate user over to the remote attacker.

Remote Control Capabilities—

While remote access to user information is a compelling threat, equally harmful is the fact that Trojans can provide hackers and crackers with uninhibited control over compromised systems, including the power to execute programs, manipulate data files, pilfer sensitive information, alter computer settings, and cause denial of service attacks. In addition to the Backdoor.IRC.Bot.B mentioned above, the Subseven Trojan provides illegitimate users with the ability to obtain control over infected systems. The Subseven Trojan is initially sent as an e-mail attachment, but attempts to deceive the victim by feigning to be a customized message. Subseven can launch a function similar to a continuous screen camera, enabling the hacker to receive screen shots of the victim's computer.

---

[8] Krebs, Brian, "Computer Worms Breeding More 'DDoS' Attacks," washingtonpost.com, 4 Nov 2003, The Washington Post, accessed on 4 Nov 2003 at: <http://www.washingtonpost.com/ac2/wp-dyn/A61786-2003Nov4?language=printer>.

[9] IRC began as a talk feature for Unix based operating systems. IRC is based on a client-server model. Clients are programs that connect to a server, a server is a program that transports data, (messages), from a user client to another. IRC allows for multiple users on multiple servers to talk in real time.

[10] GTBot is a shortened name for Global Threat Robot. This program was originally called Aristotle's Trojan.

[11] This statistic is from CERT Coordination Center (CERT/CC), "CERT Advisory CA-2003-08 Increased Activity Targeting Windows Shares," 11 Mar 2003, accessed on 3 Dec 2003 at: <http://www.cert.org/advisories/CA-2003-08.html>.

The Power to Launch Itself—

Modern day Trojans no longer need a user to launch the Trojan code. Examples, like the EG Trojan Horse program, automatically launch when a victim comes across a particular website. Originally discovered in Russia, EG is 2,580 bytes and commonly spreads to other computers via file-sharing mediums such as e-mail, shared networks, removable media, Internet Relay Chat and others. A common sign of infection is the occurrence of five or more browser windows opening autonomously and simultaneously. When a user visits a malicious website, the original browser window displays the text: "This site is temporary unavailable" while the other four windows contain different exploits that all target Internet Explorer. The danger is that one of the five windows will exploit a vulnerability in the victim's computer system so that it can download itself onto the user's computer and from there, execute a malicious file called trojan.exe, a multi-dropper file used to install several other pieces of software code onto the target machine.

A similar attack strategy was used during the recent infection of Interland Inc., a web-hosting company in Atlanta, Georgia.[12] In this case, footers on web pages hosted on the company's servers were injected with malicious code.[13] When unsuspecting Internet surfers came across an infected web page, the malicious code would automatically download itself onto the surfer's computer. Once taking residence within a computer system, the malicious code grabbed an executable program from another location that downloaded a proxy server onto the infected computer; and hidden behind the shield of a proxy server, remote hackers and crackers could covertly engage in illicit activities. In other words, characteristic of a multipurpose blended threat, though the overt manifestations of this infection included Internet traffic delays or disruptions, it is conceivable that the underlying purpose of the proxy server remains to be identified—but can include anything from espionage to data theft or other forms of malicious activity.

Smoke Screens—

On January 25, 2003, a buffer overflow vulnerability in Microsoft SQL Server resulted in the widespread execution of a malicious code from a yet unknown source. Known by names such as Sapphire, Slammer, and SQLSlammer, this worm worked on a stack buffer overflow vulnerability. This type of vulnerability is common, and occurs when large quantities of data are sent to a system—so large, in fact, that the sent code extends beyond its limited length and therefore overwrites legitimate disk data. With the Slammer worm, this vulnerability allowed arbitrary code to be executed in order to shut down an entire server. Once a server was infected with the worm, the code self-propagated by sending 375 byte packets to randomly chosen IP addresses, targeting other UDP port 1434 for infection. By the end of January 2003, approximately 200,000 unpatched machines running SQLServer 2000 were victims of denial-of-service exploits caused by the Slammer worm.[14] Moreover, 90% of the vulnerable systems became victims within the first 10 minutes of the attack. What is particularly interesting to note is that at the time of this attack, the presence of a file named IERK8243.SYS was identified in the victims' machines. There is now speculation that the Slammer attack was executed in order to introduce IERK8243.SYS into the victims' machines. The anti-virus world has dubbed IERK8243.SYS, the "Slanret device driver."

What is a Device Driver?—

Device drivers are trusted components of the operating system that have full access to all system hardware. There are no restrictions on what device drivers can do. Each operating system provides some

---

[12] Sources indicate that the culprit in this infection was the EG Trojan.

[13] Details of the attack method were obtained from Jaikumar Vijayan, "Security Breach at Web Host Leaves Sites at Risk," ComputerWorld, 8 Sep 2003, accessed on 4 Nov 2003 at: <http://www.computerworld.com/printthis/2003/0,4814,84675,00.html >.

[14] Lemos, Robert, "'Slammer' attacks may become way of life on Net," 6 Feb 2001, CNET News.com, accessed 8 Dec 2003 at: <http://msn-cnet.com.com/2009-1001-983540.html>.

way of adding new device drivers to the system; in other words, device drivers need to be written according to the semantics imposed by the operating system.[15]

The Slanret device driver, however, is not a normal device driver. Once a computer system has established this malicious device drive, it is possible for other malicious programs to utilize this kernel mode driver Trojan and thus operate covertly. The Slanret device driver is specifically designed to hide other programs' processes, files, and registry keys so that they become invisible on any user-level application. In other words, it is a stealth program.

Stealth Programs—

Stealth programs are the bane of virus scanners, making both detection and the identification of solutions a problem for anti-virus researchers because of their evasive behavior. Slanret, also known as IERK,[16] is a kernel mode Trojan, or root kit— a program capable of executing commands at the root level of a computer system. This particular Trojan becomes stealth because it is deep enough in the operating system that its processes, registry modifications and dropped files can remain hidden. In other words, because this program is effectively intercepting control of software processes, it can delude the compromised system into being blind to designated processes taking place on the computer system. Through this technique, these Trojans, as well as the backdoors through which data is being transmitted, can elude the detection of such user-level applications as Windows Explorer, system task manager, and virus detection software, among others. Moreover, stealth programs use evasion techniques such as polymorphism, metamorphism, entry-point obscuring, killing anti-virus scanners and compressions. Each of these techniques are described below.

A polymorphic virus is characteristically composed of a decryptor code within the malicious software, or malware. The malware first executes this decryptor code to restore the original code— in other words, to its original, pre-encrypted state. Usually, encryption is applied using simple, logical or arithmetic instructions, such as XOR, NOT, ADD or SUB instructions. To decrypt the malware, the same instructions are applied to the encrypted code.

To obtain metamorphism, the malware goes step-by-step through its own assembler code and constructs new code of equal ability from its own framework. It is likely that this opcode changing is applied repeatedly in each generation of the malware. The malware achieves mutation with the help of a metamorphic engine. These metamorphic engines come with their distinctive name and versions. The usual technique of a malware using Entry-Point Obscuring (EPO) is to patch a call to the virus code. The patch address replaces a normal call in the code of the infected file or it replaces a known API. Win32 file infectors often use the three methods mentioned above. The malware contains a routine that stops running anti-virus programs and therefore avoids detection.

For compression, the malware uses utility programs that compress the file and its codes. The problem is not only that UPX-compressed files come in different forms to evade detection, but also the possibility of a false positive in detection. Different compressions used by the malware are easily overcome by supporting the compression in the scanner.

[15] They are called virtual device drivers (VXD) in Windows 95/98, and they are called kernel-mode device drivers in Windows NT.

[16] The authors would like to thank Ken Dunham on his research for IERK, or Slanret.

Box 2: EasyWWW.A Trojan Horse Compromises Computer Security[17]

EasyWWW.A is a new Trojan horse that spreads primarily via a web page that exploits a current Internet Explorer vulnerability, but which could also spread via e-mail, Internet relay chat (IRC), weak network shares, peer-to-peer (P2P) file-sharing networks, website download, and removable media. EasyWWW.A is currently in the wild and being distributed as the file easywww.exe. EasyWWW.A takes advantage of the Microsoft Internet Explorer MHTML Download and Execution XSS Vulnerability (IR#207012, Nov. 25, 2003) for propagation and execution. If a malicious web page containing an MHTML link to easywww.exe is visited, then two files, easywww.exe and easywww2.exe, are downloaded onto the target computer in the Windows directory, and execution is attempted.

Non-Discriminatory Technologies—

Despite an overwhelming number of threats to Windows based systems, a recent trend is the cross-platform threat. Windows, Macs, and Linux based systems are all equally vulnerable to attack. The Septer.Trojan masqueraded as an American Red Cross webpage, but was in reality a harmful, cross-platform Trojan intended for stealing credit card information from unsuspecting users.[18] The Simile.D virus is capable of infecting both Windows and Linux systems alike.

Additionally, there are an increasing number of threats that attack across a variety of devices. Not only do they compromise computers systems, but also mobile telephones, personal digital assistants (PDAs), printers, faxes, short messaging systems (SMS), and other types of portable handsets. As convergence and interoperability enable multiple devices to be a part of the same network, this will be an increasing risk.

Box 3: The Trojan Defense

Four recent cases in the United Kingdom and United States illustrate how Trojans are not just offensive weapons, but can also create legal quagmires. In separate incidents, two UK men were accused of having child pornography on their home computers. A third UK man, nineteen year old Aaron Caffrey, was accused of launching a denial of service attack in September 2001 against the Port of Houston. Fourth, in the state of Alabama in the US, a man was accused of tax fraud for errors in his tax calculations.

In each of these four cases, the computer crime suspect was released by the court based upon their claims that a Trojan horse or virus—and not the individual himself—committed the said crime. Forensics experts purportedly investigated the suspects' computers and found proof of Trojan horse programs on the hard drives of the two UK men accused of porn. While no Trojan was discovered on Caffrey's computer, the fact that he engaged in internet relay chatroom activities—where malicious code can unknowingly infect the user's computer—was enough to throw doubt on Caffrey's guilt. The defendants collectively claimed that Trojans acted to: download pornographic material onto the UK men's computer, cause calculation errors on the US man's computer, and convert Caffrey's machine into a proxy server intended for malicious acts in his respective case.

First, though Trojan horse programs may conceivably engage in such antics by making a legitimate user's computer remotely controllable by malicious outside users, no hard forensics evidence provided a link. To reiterate, Caffrey's computer did not even contain traces of a Trojan. Nonetheless, the court's knowledge about the powerful and stealth capabilities of rogue programs sufficed to shed enough doubt on the suspects' guilt so that they could not be prosecuted. Second, these three cases collectively demonstrate the difficulties associated with forensics in computer crime. Although it is possible to link a computer user's identity to a specific computer, it is a challenge to attribute activities on that computer to that specific user. In other words, computers are anonymous enough that one user can log in under the identity of another user, particularly with the ubiquity of public computer terminals. Third, malicious programs further convolute the forensics issue by enabling computers to be remotely controlled and used as attack launch pads; this is more the case with always-on Internet connections. In short, these cases illustrate the increasingly difficult time courts have in tracking surreptitious Trojan horse programs as they become more and more autonomous in their actions, and stealth in their movements.

[17] Avien, December 2, 2003

[18] For additional information see Symantec Septer.Trojan webpage at: http://www.symantec.com/avcenter/venc/data/septer.trojan.html.

III. The Escape Route: Rogue HTTP Tunnels

Tunneling is the processes by which a new communications channel is embedded within another. Often this is performed to not only hide a session's contents from casual observation, but to allow compromised hosts located on an internal network to use firewall and filter allowed protocols to act in collusion with outside agents. HTTP tunneling is a process by which data is encapsulated in hypertext transfer protocol (HTTP) to enable transfer between networks. In many instances, worms will be used to establish rogue http tunnels. Freely available software is in wide circulation to help automate the planting of backdoors, e.g. rogue HTTP tunnels, within proprietary networks. Once implanted, these illegitimate throughways provide miscreants with easily accessible network entry.

Internal systems can communicate to external targets while appearing to be standard web surfing or other allowed activities. The more common modus operandi utilizes a variant of HTTP tunneling known as *Reverse HTTP Tunneling*. In this case, what appears to be a client system browsing web servers contacts a specified web server and allows commands to be sent back to it. Thus, the client becomes a server to the intruders external systems. The key to thwarting rogue HTTP tunnels lies in detection.

Red Flags[19]*—*

Education and awareness are the keys to defense tactics in e-security. Users can look for the following indicators in order to determine the presence of rogue tunnels in a computer system:

- What are the longest sessions running on port 80? HTTP sessions are usually short lived and initiated per-page (or per graphic). A session to port 80 that lasts more than 60 seconds is a red flag.
- HTTP sessions operate in client server fashion. Clients typically consume while the servers provide information. Client systems that produce significantly more data than they consume, signal the possibility of a reverse tunnel.
- Lack of browser identification to the server.
- Small packets comprising the data stream.
- Large time spacing between small packets from client to server.
- Connection attempts at even time intervals from internal systems to the same external system that are reset with no data exchange.

Tools such as TCP Dump (www.tcpdump.org) and TCP Trace (www.tcptrace.org) are useful in finding rogue HTTP tunnels based upon their more obvious characteristics. When dealing with a suspicious HTTP Tunnel, it is important to start the 'sniffer' machines sooner rather than later and store the captures[20] for later off-line analysis. These rogue tunnels are relatively easy to see.

It is critical to determine:

- How did the intruder get in the first place?
- What is this compromised system connected too?

Another method by which malicious code can compromise a network is by shielding itself in encrypted tunnels. Once safely within the walls of the encrypted tunnel, it is virtually impossible for anti-virus or intrusion detection software to identify the malicious code. Furthermore, these encrypted tunnels provide a direct route right through the network firewall.

[19] Special thanks to Mudge for providing valuable insights as to Reverse Tunnel detection
[20] 96bytes as a truncation length for the packet capture is fine if you are using TCP dump.

IV. The Perpetrators

Today's most dangerous threat is not a 16 year old script kiddie. An entire subculture of highly educated and sophisticated hackers exists. Much as organized crime in the U.S. moved into narcotics trafficking in the 1970's, other criminal syndicates have realized that identity theft, funds transfer and extortion are lucrative business models in the information age. Cyber-crime has become the cocaine of the new millennium. Hackers have evolved from the back room hacker with a dialup connection launching DDOS attacks, to hacker cells who launch staged attacks meant to plant bots and backdoor Trojans within financial networks. This sub-culture should not be underestimated. Sophisticated, organized hacker cells no longer desire to merely force a website and network offline, but seek instead to either compromise the networks (and computers) that are attached to an infected computer, and/or to steal authentication/passwords. Hackers can "transit" through one compromised machine into all of the networks to which the information technology infrastructure is connected.

The Bugbear worm illustrates this phenomenon. In late May of 2003 a blended threat from eastern Europe by the name of Bugbear.B was unleashed on the Net. Within one hour it had been sighted in 115 countries[21]. Bugbear.B specifically focused on computers linked to Internet domains owned by over 1,200 financial institutions. Hard drives that were shared with an infected system were also in danger from the virus, which could append itself to more than 30 different programs and execute when those applications were run. The virus opened a "back door" on PCs, leaving Port 1080 open to intruders from the Internet. It also deposited a "keylogger", a program that stores a user's keystrokes, placing personal data and passwords at risk. The malicious program attempted to shut down any antivirus software and related security programs running on a victim's computer. Finally, the software transmitted stolen passwords to 10 drop sites, all of which were located in the former Soviet Bloc. In sum, Bugbear.B did more than render harm to a computer, it was responsible for a wide array of threats to users, including economic damage, illegal surveillance, and financial theft.

V. Self-Defense Tactics

Awareness is critical when attempting to thwart Trojans. Only through a combination of credible cyber-intelligence and due diligence when managing patches on servers and clients will organizations be able thwart the threat.[22] Patch development, distribution, and installation takes time. It is important to remember that following any attack, one must take the time to investigate whether the blended threat carried a backdoor Trojan. Merely patching one's network after a successful intrusion and running an updated virus scan will not be sufficient. Next, identify and block any reverse HTTP tunnels.

Box 4: Blocking Reverse Tunnels

To block HTTP tunneling an organization needs to:

- Check access log statistics to identify the presence and endpoints of the tunnel. Typically this can be accomplished by looking for extended sessions and related data. (Note: access log statistics are not be explicitly trusted due to compromise of system integrity.)
- Implement an application level proxy and block HTTP CONNECT[1]
- Require outbound authentication on the firewall for http, https and SSL.[1] There are automated tools that sue mechanisms for reverse tunnels as well. This action does provide an easier choke point for monitoring HTTP sessions.

Maintain strong policy of use agreement with your users and punish abusers with suitable punishments according to your policy. For information flow in/out of any organization, all senior management have the responsibility of reading and understanding the Security Policy surrounding the rules[1] of electronic information flow in/out of the organization. This is most important in enabling the tunnels to stand out in a more pronounced fashion.

[21] www.MSNBC.com

[22] It is highly recommended that once a vulnerability is deemed critical by either CERT or the Vendor, one should attempt to patch it on both clients and servers within 48 hours.

The worst case scenario, as demonstrated in Bugbear, is the ability for crackers to compromise password logs. If this should occur, it is critical to mandate password changes across the entire institution. In fact, the weakest link in the security chain continues to be the end user. Many institutions hemorrhage usernames and passwords and yet many systems administrators do not notice because the entry of these passwords appear valid.

Overall, the widespread damage caused by Trojans is perpetuated as a result of insufficient access controls and weak authentication mechanisms.[23] Although not enabled with biometrics, even the most basic ATMs utilize a two-factor authentication system: a password and a physical card. Without both items, confidential data cannot be accessed at ATM terminals. No strain is placed upon the customer / user, but meanwhile security is improved. The utilization of two-factor authentication measures can greatly increase network integrity, especially when the use of biometric factors are combined with a token-based authentication system. If biometrics are properly implemented into network security schemes, the digital insider threat can be minimized exponentially.[24]

VI. Conclusion

Today's attack modus operandi have changed, and only by understanding the enemies' tactics can proper risk mitigation practices be adopted. Many worms and blended threats are illogically deemed to be nuisances because there is no evidence of a malicious payload. However the enemy should never be underestimated. No longer are hackers attempting just DDOS on network systems. Instead, they seek to steal the keys to the computer user's castle. Theft of authentication data, user identification, passwords, and other sensitive personal data through the insertion of backdoor Trojans into networks has become the exploit of choice for today's professional hacker. Increasingly, remote hackers and crackers harness the technological capabilities of powerful evolutions of malicious code so that they can, essentially, become pernicious digital insiders. More frightening, once inside a compromised system, these malicious pieces of code can act both autonomously and stealthily, escaping the notice of an organization's security controls. This is the new breed of the insider threat.

[23] Electronic Safety and Soundness: Securing Finance in a New Age. Thomas Glaessner, Tom Kellermann and Valerie McNevin. The World Bank. www1.worldbank.org/finance (click on e-security)

[24] When a token such as a biometric smartcard is properly utilized you will have a system which requires users to: a) be something (biometrics) and b) have something (smartcard).