GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials: Network, Endpoint, and Cloud (Security 401)"
at http://www.giac.org/registration/gsec

Deconstructing SubSeven, the Trojan Horse of Choice

Jamie Crapanzano

Just as computers have evolved from existing as the property of a select few in corporate and governmental realms to being available to the masses for professional and private use, so have the methods and desires to misuse the technology they harness. Trojan horse programs like NetBus, Back Orifice and SubSeven have democratized hacking such that those who engage in the activity are no longer required to possess a comprehensive and often esoteric understanding of multiple operating systems, networking concepts and programming languages. The largest group of attackers, comprising over 95 percent of the hacker population, is referred to as "script-kiddies," individuals with limited knowledge of operating systems and networks. They allow precompiled programs like Trojan horses to do the work for them, which afford hackers access to other computers to pilfer files, change settings or launch denial of service attacks.[1]

What is a Trojan horse?

Trojan horses are one of the easiest weapons that hackers, particularly script-kiddies, can use to wreak havoc on the Internet. A Trojan horse is a destructive tool that operates under the guise of a valuable or entertaining program. Trojan horses can be viruses or remote control programs that provide complete access to a victim's computer. Netbus, Back Orifice and SubSeven are all examples of the latter type. Trojan horses can be installed on a computer through an email attachment intended to be opened by the victim. The fact that the Trojan is typically disguised as an appealing message or piece of software alludes to the downfall of Troy that was brought on by the invitation that the Trojans extended to well-concealed, deadly Greek warriors. As the user enjoys the attachment, infection occurs simultaneously and silently. If a remote control Trojan is installed and initialized on a system, that computer is now completely open to anyone who knows to connect to it using the Trojan horse as a server. The hacker responsible for a specific attack is not the only person who can be privy to the knowledge that a Trojan horse resides on the target computer—there are port scanners designed to find remote-control Trojans already planted on systems. Anyone who utilizes these has access to the victim's files even if he or she did not originally bestow the Trojan onto that machine.[2] A remote-control Trojan horse differs from a traditional virus in that it does not reproduce itself and spread throughout an infected system; it is an contained program designed to invisibly execute commands issued by a remote user.[3] Of all the Trojan horses available for download from the Internet and consequent deployment onto unsuspecting computers, the current Trojan of choice for misguided computer enthusiasts is SubSeven, a program written by an individual who refers to himself as Mobman.[4]

What is SubSeven?

SubSeven is a Trojan Horse used to attack computers running on a Windows 9.x platform. It's popularity stems from that fact that it is a remote-control program which allows an attacker to issue virtually any command imaginable on a compromised system, and provides many more options for attack than other Trojans like Back Orifice or NetBus. The SubSeven download is comprised of three programs: the SubSeven server, client and server editor. The

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

server is the portion that must be run on that target computer to allow the client computer (the hacker) to connect to the machine and have total access to it. The server editor (EditServer program) defines the characteristics of infection, allowing the hacker to specify whether the compromised system should send an email or ICQ notification to the attacker when the target is online, whether the program should "melt server after installation" (have the server run once and then disappear) and which ports the client should use to connect to the server (and thus which ports the server must ensure remain open while the victim is online). This customization of settings (which was introduced by Back Orifice 2000) allows the Trojan more flexibility. The function of the EditServer program is also useful when detection and/or removal of the server on the victim's machine has become imminent: the hacker can connect to the victim's machine and install a different configuration of the SubSeven server that uses alternate ports, different techniques for autostarting and/or implement a server filename that varies from that previously used. Once the attacker removes the old version of the server, he or she is able to unobtrusively continue violating the victim's computer.[5] SubSeven can be sent as an email attachment that, once executed, can display a customized message to deceive the victim and mask the true intent of the program. Infection can also occur through unprotected shares of the hard drive, when a user permits unauthorized read and write access. Such a situation allows an attacker to place the Trojan into the appropriate directories and edit the registry so that the SubSeven server is initialized every time the computer reboots.[6] In this scenario, the end-user is completely unaware that infection has occurred since he or she was not required to perform any particular action.

What does SubSeven do?

Once SubSeven is installed, hackers can initiate attacks that range from mildly irritating to extremely detrimental. In the former category, the more notable capabilities provided by SubSeven are the ability to restart Windows on the victim's computer, reverse mouse buttons, record sound files from the microphone attached to the compromised machine, record images from an attached video camera, change desktop colors, open/close the CD-ROM drive, record screen shots of the victim's computer and turn the victim's monitor off/on. An attacker can also glean various information about a victim's computer, including the version of Windows running on the machine, the hard disk size and a listing of recorded and cached passwords. The hacker also has complete access to the victim's registry.[7] New features included in the most recent version of SubSeven (version 2.1) include an address book that facilitates checking whether a victim is presently online, a process manager feature that allows a hacker to mercilessly abort any running process on the victim's computer, a feature called "text2speech" which allows a hacker to type any text which is then spoken on the victim's computer and the ability to completely takeover a victim's ICQ account (a hacker can usurp the ability to send and receive messages as the victim, to read the victim's history, etc).[8] ICQ is an AOL subsidiary and is ranked as the most popular instant messaging service, with over 80 million members that could theoretically be affected by this addition to SubSeven.

Two of the more damaging features of SubSeven are the port redirector and the port scanner. The port redirector allows an attacker to hack into other systems by configuring ports on an already infected computer to point to new targets. This is especially useful for hackers who wish to exploit a home user's VPN (Virtual Private Network) client software (which acts as channel into the home user's corporate network), thus exposing the corporate network to attacks.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

A hacker can use the port scanning feature that is also included in SubSeven in conjunction with the port redirector—this converts the compromised machine into a personal port scanner that can be used to gain access to the corporate LAN and disguise the attacks so that they appear as if they are originating from computers belonging to trusted personnel.[9] Therefore VPN corruption, through which a hacker assumes an acceptable identity and enters what might already be a well-protected network, demonstrates that VPNs have the capability to precipitate the same hazardous results as rogue modems attached to a corporate LAN: both threaten to undermine carefully designed and implemented security measures.

Who is at risk for infection?

SubSeven is a Trojan specifically designed to enable attacks upon computers running Windows 9.x platforms. Windows is the most popular operating system for personal computers, and any such machines with access to the Internet are potential victims of hackers using SubSeven. Personal computers are also often operated by users who are less aware of security concerns and the susceptibility of a system that is on the Internet. Home users are less likely than those on a corporate LAN to adhere to a security policy addressing web access, to utilize firewall technology and to engage in port monitoring. Additionally, coinciding with the availability of a program like SubSeven and the interest of script kiddies in employing it, is the increasing popularity and availability of "always on" internet connections for the home user through cable and DSL services. This produces a potentially dangerous situation for unprotected systems; for a hacker to compromise a computer he or she must first locate it, and the chances for this occurrence are greatly increased when that computer is constantly online. While corporate systems have confronted security threats like these for some time, individuals using personal computers often do not realize the danger that "always on" connections introduce and are therefore more likely to leave their system unprotected. Features like static IP addresses only exacerbate the problem; once attackers have recognized the vulnerability of a computer, they know exactly how to return to that same system to perform additional attacks.

In terms of availability to attackers, home computers are becoming equal in level to those of private industry and government, and as average users progressively utilize their personal computers for activities such as tax preparation, online banking, stock trading and e-commerce, the amount of confidential information stored on these machines dramatically increases. The quantity of sensitive information contained on home computers contributes to their attractiveness as targets, as they hold the same promise for lucrative rewards as systems that are components of much larger enterprises. The combination of availability, private content and frequent defenseless status of home computers makes them prime targets; some hackers routinely conduct scans of certain portions of the internet searching solely for home computers to attack, regardless of their type of connection (cable, DSL or even dial-up) to the Internet.

Home computers represent an increase in the number of largely unprotected targets on the Internet, and the motives for hackers to attack them are quite clear. Computers on corporate or governmental networks are not absolved from attacks, but these machines and their users are more likely to operate according to a security policy and behind security hardware or software that serves to aid in the prevention of infection. However, without effective firewalls or adherence to an efficient security policy, every machine running the Windows 9.x operating system and interacting with the Internet is at risk for a SubSeven assault.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Prevention and Removal of SubSeven

There are a number of security measures that can be taken by the home user to avoid infection with the SubSeven Trojan horse. Sharing of the root drive should be turned off unless it is absolutely necessary. If it is necessary, authenticated access should only be permitted. Keeping anti-virus software updated is of prime importance, as these programs can usually detect the presence of the Trojan before it can do any real harm. Anti-virus software can be used to scan email attachments before they are opened to help prevent infection through email. Personal firewalls monitor the ports of a system while it is online and do not allow any suspicious traffic (including pings for the SubSeven server) to go through. Although SubSeven can operate on any ports specified by the hacker, some of the more common ports that the server is configured to use are 1243, 6711, 6712, 6713 6776, 27374. By frequently monitoring the ports on his or her system manually, a user is in a good position to recognize abnormalities when they occur and rectify the situation before excessive damage is done.

If infection does occur, there are many programs available today that detect the presence of SubSeven and purge it from the system. To insure complete removal a user can manually eliminate the Trojan from a machine as well. The server portion of the Trojan that resides on the victimized computer consists of two files, the first of which is found in the WINDOWS directory, and the second is located in the WINDOWS\SYSTEM directory. Although these files can have any name, in the WINDOWS directory they usually take on one of the following:"server.exe" "rundll16.exe" "systray.dl" or "Task_bar.exe" and the file size is typically 328kb. In the WINDOWS\SYSTEM directory, the filename is generally one of these: "FAVPNMCFEE.dll" "MVOKH_32.dll" "nodll.exe" or "watching.dll" and the size of the file is typically 35kb. The server portion can be configured to rerun every time the system is rebooted by an entry in one of the four locations: on the "shell= " line in the SYSTEM.INI file, on the "load= " or "run= " line in the WIN.INI file, or a key with a value of one of the files mentioned above in the "HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run" or "HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices" portion of the registry. On systems containing the SubSeven Trojan, the entry is most likely found in the first location. Since the server files could technically have any name, a better technique for determining infection would be to first examine the WIN.INI, SYSTEM.INI and registry files for entries containing suspicious values, and then investigate the files referenced. This again stresses the importance of knowing one's system—such awareness affords one the ability to recognize irregularities when they are manifested.

The WIN.INI and SYSTEM.INI files can be accessed by clicking Start | Run on the Windows menu and then typing SYSEDIT and pressing enter. Click on the SYSTEM.INI file and look at the "shell=Explorer.exe" line—there should not be anything to the right of this statement. If the line looks something like "shell=Explorer.exe Task_bar.exe," Task_bar.exe is the server portion of SubSeven. Delete it from the line and save the changes. The same process should be applied to the WIN.INI file. The registry is accessed by typing REGEDIT at the Run prompt. Look for a key under the "HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run" or "HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices" directory that references any suspicious files (especially those with the previously mentioned names). Before deleting the reference, make sure that this is the SubSeven server file by checking the WINDOWS directory to ensure the file size is 328kb.[10] If it is, delete the reference

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

from the registry. Remember to also delete the actual files themselves from the WINDOWS and WINDOWS/SYSTEM directories. Once the system is cleaned, taking the previously mentioned preventative measures can help prevent future contamination.

Conclusions

The popularity of the SubSeven Trojan and the general vulnerability of many systems on the Internet, particularly those of home users, require an awareness of the dangers of being infected with this malicious program. By understanding what SubSeven is, how it works and how to defend a system against it, personal computer users are able to shift their status from that of probable victims to guardians of impermeable systems and champions of a more secure Internet.

References:

[1] Seifried, Kurt. "How To Hack: An Introduction." Sys Admin. November 2000, p.44.
[2] Williams, Jim. "Script Kiddies: The Trojan Horse Attack" URL: http://netsecurity.about.com/compute/netsecurity (2 January 2001).
[3] Hsu, Jeffrey. "Computer Viruses, Technological Poisons." Smart Computing in Plain English. October 1993, Vol 14, issue 10.
[4] McClure, Stuart and Scambray, Joel. "Security Watch: Here's a little advice to help you defeat the Internet's leading Trojan horse viruses." Infoworld. 4 December 2000, Vol. 22.
[5] Northcutt, Stephen. "Intrusion Detection Overview and Trends in Internet Attacks." Security Essentials 1. p. 4-8,9.
[6] McClure and Scambray, Infoworld.
[7] Podrezov, Alexey. "SubSeven." F-Secure Virus Descriptions. URL: http://www.f-secure.com/v-descs/subseven/htm (2 January 2001).
[8] "TL Security SubSeven Download" URL: http://www.tlsecurity.net/backdoor/subseven21.htm (2 January 2001).
[9] McClure and Scambray, Infoworld.
[10] "Threats to Your Security on the Internet - SubSeven" URL: http://www.commodon.com/threat/threat-sub7.htm (2 January 2001).

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.