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
"Hacker Tools, Techniques, and Incident Handling (Security 504)"
at http://www.giac.org/registration/gcih

Sub Seven

A Risk to Your Internet Security

GCIH Incident Handling and Hacker Exploits Practical

Version 2.0

Option 2 – Support for the Cyber Defense Initiative



Submitted By Paul Ostrowski

February 4, 2002

© SANS Institute 2000 - 2005 Author retains full rights.

Table of Contents

Introduction: History of the Trojan Horse	3
Targeted Port: Internet Storm Center and the Consensus Intrusion Database	5
Malicious Worms/Trojans Running on Port 27374	5
Vulnerabilities of the SubSeven Trojan	10
The Characteristics of the SubSeven Trojan (Exploit Detail)	10
The Inner Workings of Sub7	14
How to Deploy Sub-Seven	16
Signature of the Attack	23
Identifying and Protecting an Infected System "Know Thy System"	24
Techniques for Removing Variants of the Sub7 Trojan	27
Source Code	32
Additional Info	33
Document Resources/References	35

© SANS Institute 2000 - 2005, Author retains full rights.

Introduction: History of the Trojan Horse

The origins of the word date back to the 12th century BC where, according to the Greek poet Homer, the Greeks lay siege to the well fortified city of Troy. The battle raged for 10 years until the king of Ithaca, Odysseus, came up with a plan to get the Greek army into Troy. The Greeks built an immense wooden horse and Odysseus, Menelaus, and other warriors hid inside it. After leaving the horse at the gates of Troy, the Greek army sailed away. The Trojans thought the Greeks had given up and had left the horse as a gift.

Cassandra, a priestess with psychic powers, knew the horse was trouble. She tried to warn her father, King Priam, but he wouldn't listen. A priest named Laocoon also warned the Trojans to *beware of Greeks bearing gifts*. He too was ignored and the horse was brought inside the city walls of Troy.

While the Trojans were sleeping, the Greek army's ships quietly returned. The soldiers in the horse slipped out and opened the city gates, and the Greek army quietly entered Troy. They started fires all over the city and the Trojans awoke to find their city burning and when they tried to flee, the Greek soldiers massacred them.

Today, a Trojan horse is still synonymous with deceit and nefarious functions. However, it's commonly used to describe an altered software program that appears on the surface to be benevolent in nature. In reality, it contains hidden unauthorized instructions that perform unknown and probably unwanted functions. Trojans quite often contain dangerous computer code that ultimately can be quite destructive. Many of the common Trojan horses will insert backdoor access into a compromised system and will typically send confidential information to unauthorized destinations. They can also alter the functions of the infected host so as to surrender control of common system functions to the attacker

Trojan applications are quite commonly mistaken for viruses. After infecting the unsuspecting system, a computer virus will automatically replicate itself from host to host. However, most Trojan applications will not proliferate between systems. Delivery of the Trojan file into a host can be accomplished through a variety of means, the most common being the receipt of an email containing an infected attachment.

The most common Trojan is the type classified as *Remote Administration Tool* or *RAT*. A RAT Trojan typically provides the hacker with several tools to compromise an individual's personal information. *Key logging* or *session recording* is one of the more common techniques used to acquire this information. It involves recording a victim's keystrokes into a secret file in the hopes of obtaining confidential information such as account passwords or pin numbers. The secret file can be either downloaded to the hacker using email or through a backend process built into the Trojan.

© SANS Institute 2000 - 2005 Author retains full rights.

A RAT Trojan may also possess the capabilities to alter Windows registry settings and upload/download executable files into the infected system.

A *RAT* Trojan consists of two software components commonly referred to as the *server* file and the *client* file. The server file is the component that actually infects the victim's system through an email attachment or a backend file duplication process. When the server file is opened, it will usually return a "Failed" error message. However, the server application can also arrive as a game that actually appears to install as a software component. Once the server file infects a system, it will monitor a predefined TCP port listening for IP packets destined for that port. These IP packets will originate from the *client* file located on the attacking system. The client application is designed to control and monitor the infected host running the server application. The operations that the client application can perform on the target computer will depend on the particular Trojan being implemented.

Sub7 (or sometimes referred to as *Backdoor G* or *Pinkworm*) is the epitome of the proverbial *RAT* Trojan and is quite often used for malicious intentions. The Sub 7 Trojan was written by *mobman* and ultimately enables unauthorized people access to your computer over the Internet without your knowledge.

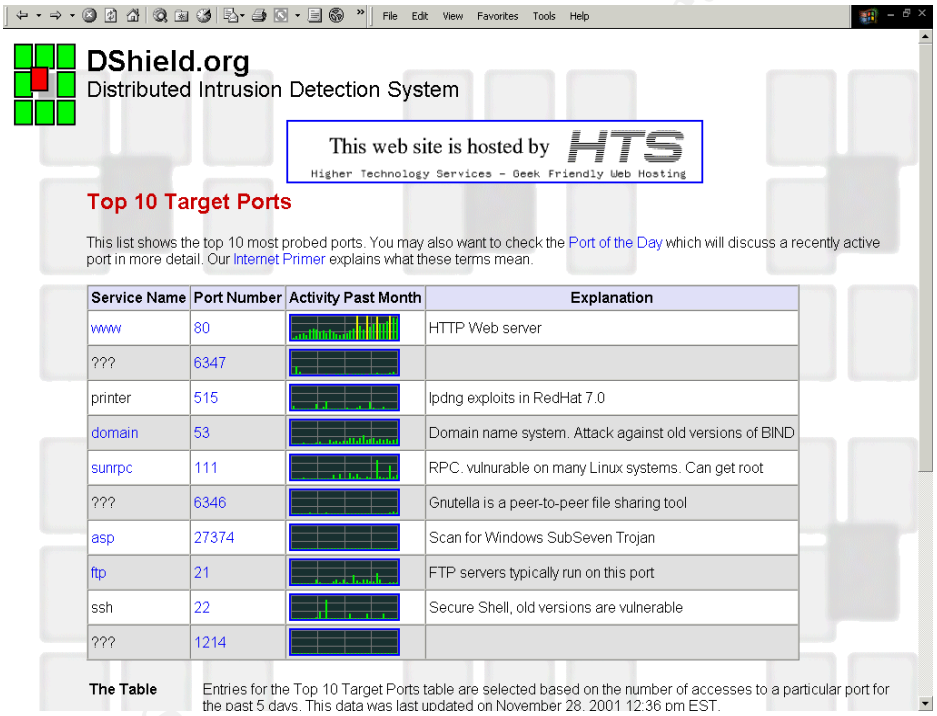
SubSeven is similar to Back Orifice that was discussed in depth during our training. Back Orifice can also be classified as a RAT Trojan in that it's comprised of two main pieces: a client application and a server application. However, there are minor differences in the exploitable capabilities between the two Trojans. The following table details those differences:

Sub7	***Back Orifice***
• Edit information in currently running programs • Show pop-up messages and dialog boxes • Hang up a dial-up connection • Open the CD-ROM tray • Edit registry information	• Lockup the target computer. • View the contents of any file on the target computer. • Write your own plugins and execute the native code of your choice in BO's hidden system process.

© SANS Institute 2000 - 2005 Author retains full rights.

Targeted Port: Internet Storm Center and the Consensus Intrusion Database

According to the latest figures compiled on November 28,2001 by the Internet Storm Center and the Consensus Intrusion Database (CID), port 27374 is one of the 10 most common ports probed for on the Internet. Port 27374 is the default port used by the client application/file of SubSeven, SubSeven 2.1 Gold, SubSeven 2.1.4 DefCon 8, and SubSeven Muie to communicate with the infected host (server application). It is also the same port used by four additional Trojan applications: Bad Blood, Ramen, Ttfloader, and Seeker.



DShield.org
Distributed Intrusion Detection System

This web site is hosted by HTS
Higher Technology Services - Geek Friendly Web Hosting

Top 10 Target Ports

This list shows the top 10 most probed ports. You may also want to check the Port of the Day which will discuss a recently active port in more detail. Our Internet Primer explains what these terms mean.

Service Name	Port Number	Activity Past Month	Explanation
www	80		HTTP Web server
???	6347		
printer	515		lpdng exploits in RedHat 7.0
domain	53		Domain name system. Attack against old versions of BIND
sunrpc	111		RPC. vulnurable on many Linux systems. Can get root
???	6346		Gnutella is a peer-to-peer file sharing tool
asp	27374		Scan for Windows SubSeven Trojan
ftp	21		FTP servers typically run on this port
ssh	22		Secure Shell, old versions are vulnerable
???	1214		

The Table Entries for the Top 10 Target Ports table are selected based on the number of accesses to a particular port for the past 5 days. This data was last updated on November 28, 2001 12:36 pm EST.

Malicious Worms/Trojans Running on Port 27374

In general, worms have been circulating around the Internet for quite some time and tend to be very malicious and damaging. The Morris worm (Robert Tafee Morris Jr.) is one of the more infamous worms to surface. It was released in 1989 and effectively took down the Internet for several days.

Ramen (alias: Unix/Ramen, Linux/Ramen, Elf Ramen)

Release Date: January, 2001 / Author: Unknown

Ramen is a self propagating Internet worm that infects Linux based systems

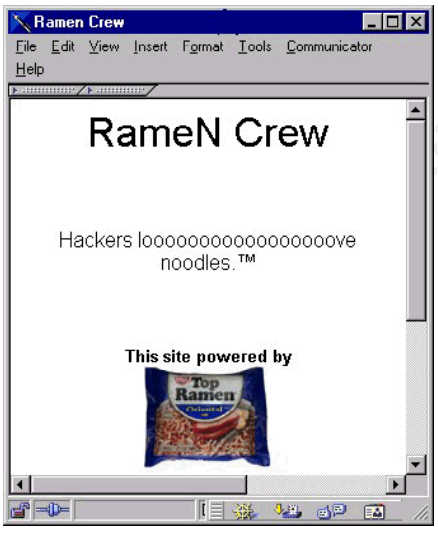
© SANS Institute 2000 - 2005 Author retains full rights.

using default installations of Red Hat (Intel) version 6.2 and version 7.0 (1st Edition). Other versions of Linux (Red Hat: 2nd Edition, non Intel, and older versions), are not vulnerable to this exploit. However, Ramen scripts can be easily modified to infect other systems running different versions of Linux and Unix. Ramen does contain routines that are designed to infect FreeBSD and SuSE computers, however, these routines are not enabled. There are two variants of the Ramen Worm – Ramen(A) and Ramen(B).

Ramen(A)

Ramen(A) infects Linux systems by exploiting vulnerabilities in the LPRng (Red Hat 7.0), wu-ftpd, (using a method called **site exec)** and rpc.stad services (Red Hat 6.2) and is designed to be easily modified by dispatching the source binaries onto a system. Once the worm compromises a host, it will implement a command to request a copy of itself from the attacking system (file:ramen.tgz) and will extract it into the following hidden directory: "/usr/src/.poop/". A shell script entitled "start.sh" is also extracted and is executed under system root privilege mode. Ramen will send an e-mail notification message to the following two accounts: gb31337@hotmail.com and gb31337@yahoo.com from the infected host.

If a web server is running on the host, the worm scans the entire system (including any mounted resources) and will replace all the "index.html" files with the following file that includes the text : *RameN Crew Hackers looooooooooooove noodles.*



Ramen removes the "/etc/hosts.deny" file and in Red Hat 6.2, will remove both the "/usr/sbin/rpc.rstatd", the "sbin/rpc.statd" and replace the "/usr/sbin/lpd" with a zero byte file within Red Hat 7.0 systems. Ramen will alter the "/etc/rc.d/rc/sysinit" file which activates the worm after the host system is started.

© SANS Institute 2000 - 2005 Author retains full rights.

Using a modified program called *syscan*, Ramen will scan a random range of class B IP subnets and will attempt to determine the version of Unix on the scanned systems by inspecting the FTP banner. It will copy a simple http application to "sbin/asp" which will establish an http server listening on port 27374 to distribute copies of the ramen.tgz file to potential hosts and will repair the vulnerable exploit(s) on the infected host. FTP services are disabled and users "ftp" and "anonymous" are added to the /etc/ftpusers directory which effectively closes the vulnerability in the wu-ftpd service.

The three exploits are addressed and fixed on Red Hat's internal web site:

Red Hat Linux 6.2: http://www.redhat.com/support/errata/rh62-errata-security.html

Red Hat Linux 7.0: http://www.redhat.com/support/errata/rh7-errata-security.html

Ramen(B)

Ramen(B) delivers a different payload then Ramen(A). Ramen(B) attempts to install a backdoor component and a variant of the Distributed Denial of Service agent called Stacheldraht onto the host system.

The worm relocates the "/bin/login" to the directory: "/usr/lib/ldliblogin.so" and will install an altered version of "login" to "/bin/login".

The "/etc/shadow" file is then sent to the individuals who originally wrote the virus and an attempt will be made to remove the event from the log entries.

The "/usr/bin/lpd" service is replace with a variant of the Stacheldraht DDOS agent and an entry is added to the "/etc/rc.d/rc.sysinit" file. This will activate the agent once the system is rebooted. A compiled program located in the "/usr/sbin/update" will kill and restart the "lpd" system process in attempt to activate the DDOS agent.

The two commands "/bin/ps" and "/bin/netstat" are moved to "/usr/lib/ldlibps.so" and "/usr/lib/ldlibns.so" and replaced with altered versions that will ultimately be disguised from the user. A cron job is created and executed monthly, "/usr/sbin/update" that is intended to kill all processes named "syncscan".

Refer to the follow site for information on how to remove the Ramen worm:
http://www.sans.org/y2k/ramen.htm

Bad Blood

Bad Blood was created in 1999 and is classified as a Remote Access / Mail Trojan that can infect Windows 95 and 98 systems utilizing Microsoft Outlook mail client. By default, Bad Blood is capable of communicating with

© SANS Institute 2000 - 2005 Author retains full rights.

the *SubSeven* Trojan on port 27374. It is also capable of establishing a communication channel with *The Thing* Trojan on port 6006 utilizing the password "badblood".

As mentioned earlier, Sub seven is probably the most prolific Trojan on the Internet. It's easy to implement and affords the hacker a vast amount of control and function. There are many different circulating variants of Sub 7 and each new version usually possess different characteristics from its predecessor. The following is one of many locations on the Internet posting the official releases of the SubSeven Trojan: http://www.sub7.org/downloads.shtml

The following is an inclusive list of known Sub Seven versions/variants complied from various web sources.

Sub Seven 1.0	Sub Seven 1.1
Sub Seven 1.2	Sub Seven 1.3
Sub Seven 1.4	Sub Seven 1.5
Sub Seven 1.6	Sub Seven 1.7
Sub Seven 1.8	Sub Seven 1.9
Sub Seven 2.0	Sub Seven 2.1 Bonus
Sub Seven 2.1 Gold	Sub Seven 2.1 MUIE
Sub Seven 2.1 MUIE unpatched	Sub Seven 2.1/2.13a-b
Sub Seven 2.2 beta	Sub Seven 2.2 beta NT Apocalypse
Sub Seven Runner.a	Sub Seven Runner.b
Sub Seven Runner.c	Sub Seven ICQ-Fix

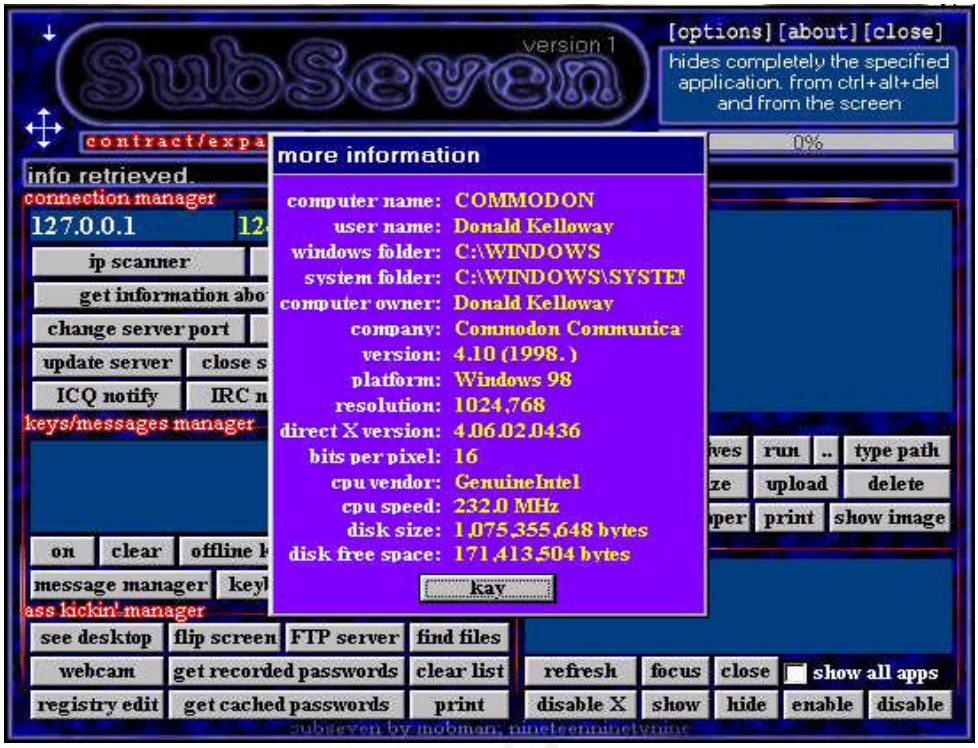
Sub Seven 2.3 (not been released) –currently being developed by Mobman

Screen Shot of the Sub7 Client Application (source: http://www.sub7.org/help/index.shtml)

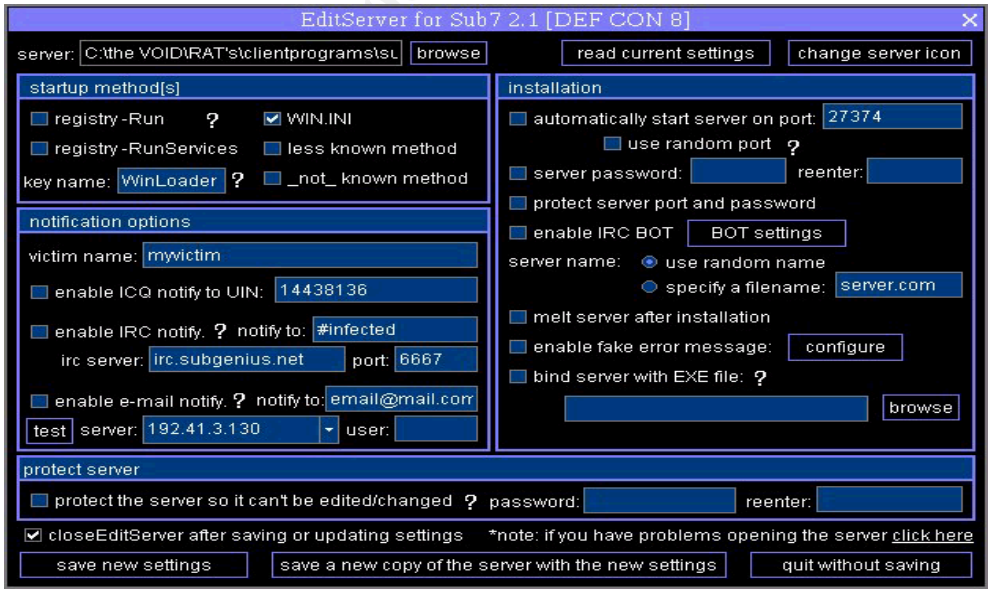


Below is a screenshot of information obtained by the Sub7's client application after it was attached to a PC that was compromised with the server application. (source: http://www.commodon.com/threat/threat-sub7.htm)

© SANS Institute 2000 - 2005 Author retains full rights.



Below is a screenshot of the "EditServer" utility. This utility allows the hacker to customize the "server" portion of the Trojan. After the server component of Sub7 has been configured, it's sent to the victim.
(source: http://www.sub7.org/help/index.shtml)



Although *Sub7* and its variants have been around for sometime, it continues to be one of the most sought after exploits on the Internet and consequently, will be the focus of this document.

© SANS Institute 2000 - 2005 Author retains full rights.

Vulnerabilities of the SubSeven Trojan

http://packetstormsecurity.nl/0001-exploits/subseven.htm

According to the following article written by Andrew Griffiths, Subseven 2.1a. is vulnerable to a buffer-overflow exploit. If the server file is instructed to execute a DOS command exceeding 315 characters in length, it will overrun a predefined buffer causing the server file to either quietly quit, crash, or overwrite system variables. In addition, all established connections to port 139 fail. Although, this appears to be an unconfirmed side affect of the vulnerability.

The SubSeven Trojan is also vulnerable to numerous dictionary attacks against the server file's password. The following is a list of tools available to remove or crack the server password: (reference: http://www.tlsecurity.net/main.htm)

SubBrute - This programs attempts to guess the SubSeven passwords by using a brute force dictionary attack against it.

SubPass - This program removes the password from ANY SubSeven server file up to and including version 1.9.

RatCracker - "Cracks" the password of the following:

- Subseven Server file up to and including version 1.9
- DeepThroat3.x
- Netbus 1.x
- Doly version 1.6 and greater

NetBuster for SubSeven is a utility which mimics the operation of an actual SubSeven server file.

Subuster - Netbuster for Subseven, behaves like a fake Subseven server.

The Characteristics of the SubSeven Trojan (Exploit Detail)

Prior to version 2.2, SubSeven was capable of infecting hosts running Microsoft Windows 95/98 operating systems. Version 2.2 of SubSeven introduced support for MS Windows NT. However, the MS Windows XP operating systems is currently immune to the current variants of SubSeven. One expects, however, the next release of the SubSeven Trojan (v2.3) will include support for Windows XP. There also exists a Unix client file version that works with SubSeven server versions 2.2 and higher. The UNIX client can be downloaded from the following site: http://website.lineone.net/~bryanrpoole/.

© SANS Institute 2000 - 2005 Author retains full rights.

There are several advisories pertaining to the SubSeven Trojan and can be found at The CERT® Coordination Center (CERT/CC): http://www.cert.org/, the National Infrastructure and Protection Center: http://www.nipc.gov/, and the Common Vulnerabilities and Exposures Database. http://cve.mitre.org/

CERT® Incident Note IN-2001-07 : Release Date: July 3, 2001 W32/Leaves: Exploitation of previously installed SubSeven Trojan Horses: http://www.cert.org/incident_notes/IN-2001-07.html

ADVISORY 01-014 "New Scanning Activity (with W32-Leave.worm) Exploiting SubSeven Victims" - June 23, 2001

http://www.nipc.gov/warnings/advisories/2001/01-014.htm

CAN-1999-0660 A hacker utility or Trojan Horse is installed on a system. http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-1999-0660++

CAN-2000-0138 A system has a distributed denial of service (DDOS) attack master, agent, or zombie installed http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2000-0138++

The server application of many of the Sub7 variants can be configured to execute from one of four system locations. The server application file associated with these variants can alter its load procedure each time the system is booted and can typically use any combination of the loading techniques listed below:

1) An entry appended after the "Explorer.exe" portion of the "shell=" line within the SYSTEM.INI file entry could signify the presence of a Trojan application. (i.e.: "shell=Explorer.exe **Task_Bar.exe**", **Task_Bar.exe** would be the server portion of the Trojan.)

2) An entry on the "load=" or "run=" line in the WIN.INI file.

The third and fourth possible locations are found within the Window's registry under one of the following two headings:
"HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run"
"HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices"

The following is a procedure for discovering the Sub7 Trojan within the Windows Registry:

Step 1.
Click START | RUN
Type REGEDIT and press ENTER

Step 2.

© SANS Institute 2000 - 2005 Author retains full rights.

In the left window, click the "+" (plus sign) to the left of the following:
HKEY_LOCAL_MACHINE
Software
Microsoft
Windows
CurrentVersion
Run

Step 3.
In the right window, identify a key with a value that loads one of the following files: "server.exe" (328kb), "rundll16.exe" (328kb), "systray.dl" (328kb), "Task_bar.exe" (328kb) as well as any other of the following files:

WINLOADER	xTnow
Win32nt	Ayespie
Win32.Bin	PowerSaveMonitor
WinCrypt	winsys32.exe
WinProtect	winsys32.exe
Win	sys32.exe

Navigate to the following key:

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices

In the right window, identify a key under the Name column that loads one of the following files:

WINLOADER	Win
Win32nt	xTnow
Win32.Bin	Ayespie
WinProtect	PowerSaveMonitor
rundll32	

Other values not included within this list may also appear. Removing these values from the registry will not prevent the programs from executing - it only prevents them from starting automatically when Windows loads.

Within many of the newer variants, the name of the actual Trojan server application can also be altered. This being the case, note the name(s) of any suspicious files referenced within the right window of REGEDIT.

Launch Windows Explorer and locate each suspicious file with an approximate size of 328Kb. Chance are you've have identified the renamed Sub7 server application file.

© SANS Institute 2000 - 2005, Author retains full rights.

Sub7 can also include a second application file referenced within the WINDOWS\SYSTEM directory. This file is typically one of the following:

"FAVPNMCFEE.dll" (35kb)
"MVOKH_32.dll" (35kb)
"nodll.exe" (35kb)
"watching.dll" (35kb)

The following is a listing detailing the contents of a SubSeven version 2.1 zipped file:

SubSeven.exe (Client program – used to control Server file)
Server.exe (Server program – used to infect host)
EditServer.exe (used to configure Server file)
ICQMAPI.DLL
RawCommands.txt (Raw commands for the IRC bot script)
NewFeatures.txt
Disclaimer.txt

A description detailing the actual characteristics of each variant has been provided within this document under the heading labeled *Techniques for Removing the Sub7 Trojan*. In addition to possessing different characteristics, the server application from each variant will monitor a default TCP port. This TCP port is used to establish the connection between the "client" application and "server" application. However, the server application associated with many of the newer Sub7 variants can be configured to monitor any TCP port between the values from 1000 and 65,535. The following is an inclusive list of known default ports used by each variant of Sub7.

Port 1234:
SubSevenJavaclient,
Port 1243:
BackDoor-G, SubSeven, SubSevenApocalypse,
Port 2773/2774:
SubSeven, SubSeven2.1Gold
Port 6667:
SubSeven, SubSeven 2.1.4
Port 6711:
BackDoor-G, SubSeven,
Port 6712/6713:
SubSeven
Port 6776:
BackDoor-G, SubSeven,
Port 7000/7215:

© SANS Institute 2000 - 2005 Author retains full rights.

SubSeven, SubSeven 2.1 Gold
Port 16959:
SubSeven, SubSeven 2.1.4 DefCon 8
port 27374:
Bad Blood, SubSeven , SubSeven 2.1 Gold, Subseven 2.1.4 DefCon 8,
Sub7 Muie, Ramen, Ttfloader, Seeker
Port 27573: SubSeven
Port 54283: SubSeven, SubSeven 2.1 Gold

The Inner Workings of Sub7

Reference: Joe H. L. (Aka, Hoe, HoeBot, JoeBot, FizzBin)

SubSeven DEFCON8 2.1 was released and embedded within an executable file named "SexxxyMovie.mpeg.exe," Once the executable was launched, a copy of the server executable file was placed within the */windows* directory and was randomly renamed. The more recent versions of SubSeven (including SubSeven DEFCON8 2.1 Backdoor and later), possess the capability to notify an attacker using an IRC channel (via irc,icq.com) when a host has become infected. Many versions of SubSeven can be configured to create random file names on the infected host and have the option of listening on nonstandard ports. The standard ports for the various components of SubSeven 2.1 Gold are ICQ Spy: 54283, Key Logger: 2773, Matrix: 7215, IRC Bot: 7000. SubSeven can also be controlled using IRC commands and has even been observed launching a Denial of Service (Ping of Death) attack against targets on the Internet.

When a connection is made between the client and server application, the infected SubSeven host issues a "PWD" command. Assuming the server application was configured with a password, the client application on the hacking system will reply with a password. This is accomplished by sending a "PWDpass" command. Certain versions of the SubSeven Trojan contain a feature referred to as 'password bypass'.

Essentially, if the client application responds with a preconfigured "known" bypass password, the client application can connect to the server without providing the password configured during the setup of the server file. The Master Passwords of the distributed server file for SubSeven v. 1.9 is *predatox* and *14438136782715101980* for versions 2.1 through 2.2b. The Master Password for SubSeven DEFCON8 2.1 Backdoor is *acidphreak*.

Once connected, the server application will reply with a "connected" message that will include the time - date, year, day, and version of Sub7. An example of a typical reply would be:
connected. 12:05.59 - August 17, 2000, Thursday, version: GOLD 2.1

© SANS Institute 2000 - 2005 Author retains full rights.

connected. 12:08.13 - August 17, 2000, Thursday, version: M.U.I.E. 2.1
After the reply is received, the connection between the *server* and *client* application is considered to be complete.

Sub7's actual communication parameters between the *client* and *server* application is relatively simplistic. The actual commands are typically abbreviations of the specific function it performs. The following is a listing of Sub7 client and server application commands:

Client to Server Commands	
Disable IRC Notify	Disable ICQ Notify
Disable e-mail notify	Enabling E-Mail notify
Enabling IRC notify	Enabling ICQ Notify
Changing Port	Change Password
Removing password	Disconnect victim
Restart Server	Removing Server
Closing Server	Update server from local file
Updating from URL	Get Home Info
Get PC Info	Remote IP Scan
Key Logger	Refresh Windows

In general, SubSeven allows remote attackers to obtain cached passwords, play audio files, view webcams, and capture screenshots. The following is a list of system capabilities afforded to many of the SubSeven variants:

IP Scanner: port scanner used to scan hosts for open or listening ports
Get PC Info: obtain system info: CPU, User/computer name
Notification: technique server file will use to notify the client application
CHAT: communicate directly with the victim
Message Manager: display a message box on victim's screen
IRQ Takeover: impersonate an ICQ account

Find Files

Registry Editor

Port Redirect: map a specified TCP/UDP port to a different port
Windows Manager display list of open

Ping: used to determine if an IP host is active
Get Home Info:

Key Logger: logs actual or recorded keystrokes
The MATRIX:
Spy: receive copies of messages from ICQ/AOL IM/etc.
FTP: enable or disable FTP service on any specified port

Get Passwords: obtain cached passwords
App Redirect: execute an application on victim's system
File Manager:

Process Manager: display list

© SANS Institute 2000 - 2005 Author retains full rights.

Window's screens
processes
Text to Speech :requires support on victim's system
IRC BOT: setup IRC BOT script
Flip Screen: flip or invert the victim's screen
Browser: take control of victim's browser and enter any desired URL
Win Colors: change victims Windows desktop colors
Restart Windows: force a system shutdown

of running system
Clip Board Manager: view or clear contents of clipboard
Capture: from screen or web cam
Print: send text to victim's printers
Resolution: obtain resolution of victim's screen
Screen Saver: change the text on a marquee screen saver
Mouse: assume control of victim's mouse

Sound : record sound from victim's system ***Time/Date:***

Additional Capabilities:

Hide / show the desktop/Start Menu/Task Bar/
Open / Close the CDROM Drive
Start / Stop the speakers
Turn the monitor On / Off
Turn CTRL-ALT-DEL On / Off
Turn, Caps lock, Num lock, and Scroll Lock, On / Off

For a more complete explanation of SubSeven's capabilities, refer to the following: http://www.europe.f-secure.com/v-descs/subseven.shtml

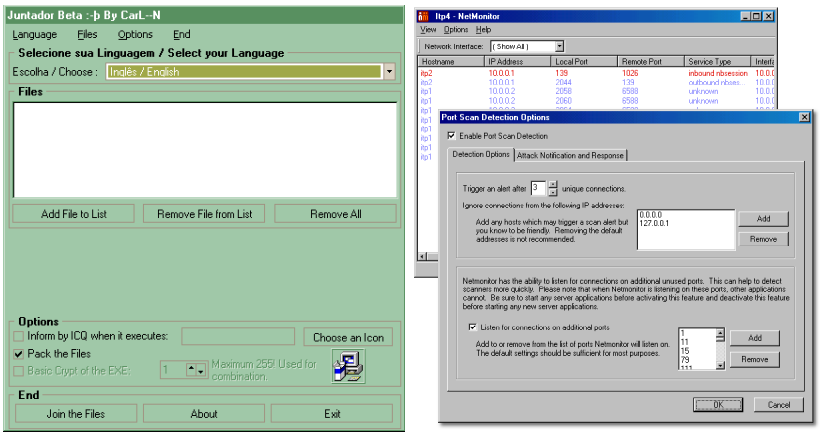
How to Deploy Sub-Seven

This section describes a procedure for infecting a target host system with Sub7 using Microsoft Instant Messenger. It was written by NËGÄTÏVË ©®ËËP and can be downloaded from the following site:
http://www.astalavista.com/trojans/library/trojans/misc/ (Trojan Hacking.ZIP)
I've taken the liberty of paraphrasing the technique as well as adding some additional material to the procedure.

Required Tools:
- MSN Instant Messenger
- Working version of Sub7 Trojan
- NeoMoniter
- A Working EXE Joiner (Juntador works well)
- A Good exe packer (Petite is good)
- ICQ
- A Few Pictures or Icons

Juntador: NeoMonitor:

© SANS Institute 2000 - 2005 Author retains full rights.

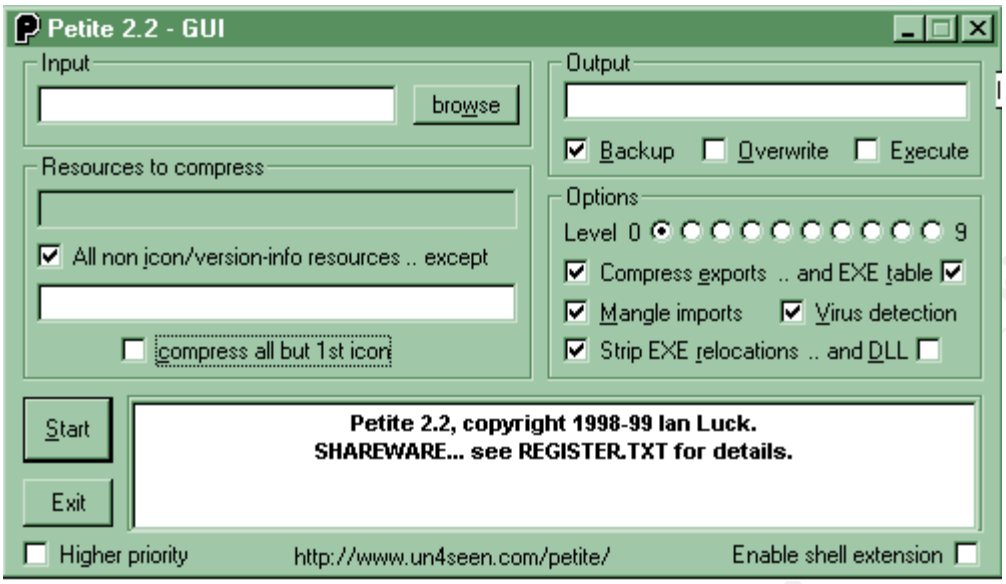


Screen shot of SubSeven version 2.1.4



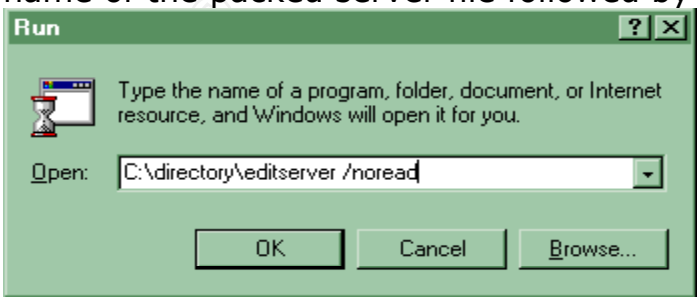
Petite Executable Compiler:

© SANS Institute 2000 - 2005 Author retains full rights.



Obtain SubSeven: http://www.sub7.org/downloads.shtml
NËGÄTÏVË ©®ËËP suggests obtaining an earlier version of sub7 (defcon8 or Bonus are good), because they are very easy to use if you are a beginner. Although, SubSeven version 2.1 is reportedly the most stable version and should be considered.
Your next step would be to obtain and install the latest version of Microsoft Instant Messenger. MSN is ultimately the program that will push the Sub Seven Server file out to your unsuspecting victim.

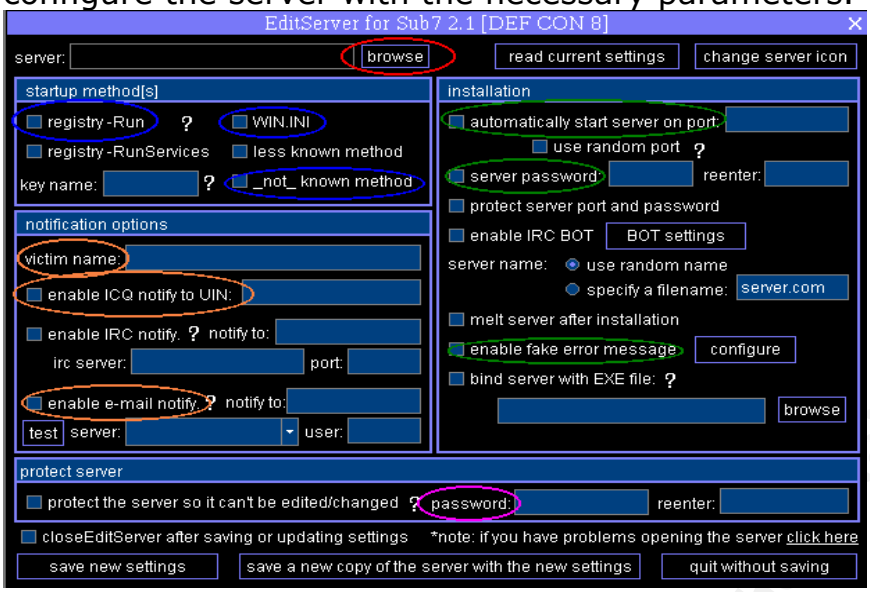
Now you need to pack and configure the server.exe file
All the commercially available anti-virus software is capable of detecting a majority of the circulating variants of the SubSeven server file. In order to bypass your targets anti-virus software, NËGÄTÏVË ©®ËËP recommends downloading an unpacked version of the server file (2.1 unpacked server) and packing it using Petite Executable Compiler. In order to reduce the size of the file, pack the file using the highest level (9). The next step is to actually configure the SubSeven packed server file.
From the <Start> menu, select <Run> and type the directory location and name of the packed server file followed by a "/noread" command.



The next step is to browse to the packed server file you created and

© SANS Institute 2000 - 2005 Author retains full rights.

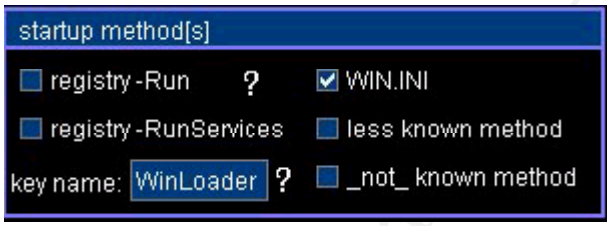
configure the server with the necessary parameters.



Edit Server for SubSeven 2.1 Defcon 8

This utility is used to customize the various configurable options within the server application. There are several options available and are listed below:

Startup Methods (Reference: http://www.sub7.org/help/index.shtml)



registry-Run

This configuration will add a key entry in the "Run" parameter under the HKEY_LOCAL_MACHINE section of the system registry.

registry-RunServices

This configuration will add a key entry in the "RunServices" parameter under the HKEY_LOCAL_MACHINE section of the system registry.

key name

Assign a name to the key assigned to the registry when utilizing one of the aforementioned techniques.

(The following screen shots were obtained from: http://www.sub7.org/help/index.shtml)

© SANS Institute 2000 - 2005 Author retains full rights.

WIN.INI

This configuration will add an entry to the run line in the WIN.INI file

less known method

This configuration will implement a less know startup technique which involves editing the system.ini file within Windows to start the server either upon system startup or when the user logs onto their system.

[boot]
shell = explorer.exe MSREXE.EXE

not known method

This configuration option will implement a supposed *not know* startup technique that involves altering the .exe file type handler in the Registry. After modifying the handler, the Trojan will continue to reload itself into memory every time an .exe file is launched on the system. Two files named MSREXE.EXE and WINDOS.EXE are added to the Windows directory and are used to initiate the server.

HKEY_CLASSES_ROOT\exefile\shell\open\command\(Default) = WINDOS.EXE

To fix the registry problem, you will need to download and launch this registry file utility. click here to download undo.reg

Notification Options (Reference: http://www.sub7.org/help/index.shtml)



Victim Name : self explanatory

Enable ICQ notify to UIN : your ICQ value

Enable IRC notify: Requires ident daemon to be bound to server file.

notify to: In this field, enter the channel name you wish the notify to come to,e.g, #infected.
irc server: Put the server address here,e.g. irc.sub7.org
port: Enter the server's port. (9 out of ten times this will be port 6667)

enable e-mail notify : enter your email address into the field labeled

© SANS Institute 2000 - 2005 Author retains full rights.

notify to: - Requires an anonymous smtp server on the Internet to relay the notification. Options include:

- mail.cfm-resources.net
- mail.ifrance.net
- mail.icqmail.com

Installation Options (Reference: http://www.sub7.org/help/index.shtml)



Port settings: value can be between (1024 and 65535)

Password settings:

- *server password:* protects server file from being compromised
- *protect server port and password:* protects the port # and password of the server from being tampered with

Enable IRC Bot: enable sub7 IRC bot script to launch on startup

Server name: references the actual name of the server file installed on the system

Melt server after installation: server file will delete itself after the initial execution

Enable fake error message: will launch a fake error message after the server file is executed

© SANS Institute 2000 - 2005, Author retains full rights.



Bind server with EXE file: attach the server file to another application to help disguise the server

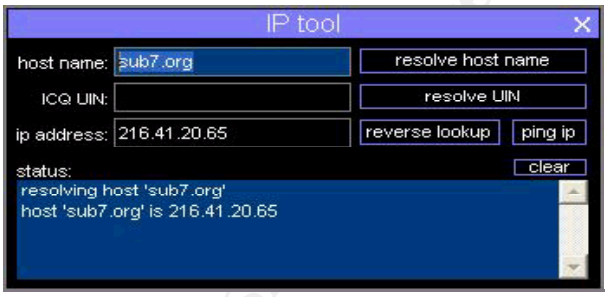
Complete the configuration by saving your settings to the file and exit from the EditServer program.NËGÄTÏVË ©®ËËP now suggests to find an old picture and using Juntador, join the picture and the server.exe file together with an extension such as .exe, .pif, .scr, .com, etc.

The HACK*:*

Load up Microsoft's Instant Messenger and NeoMonitor on your system and make note of the existing open ports and IP addresses.

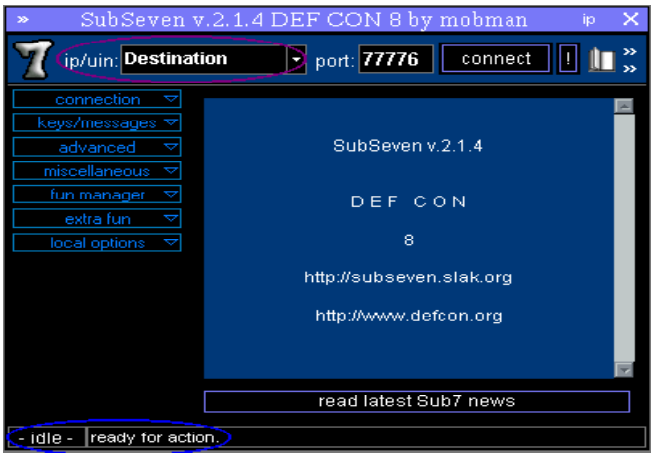
Establish a chat session with your victim and send out the infected picture. NeoMonitor should display their IP address and port#.

Another option would be to click on the ***ip*** tab located in the upper right-hand corner of the client. This assumes you already know your victim's host name or ICQ/UIN.



Open Sub7 and paste your victim's IP address into the *Destination* field.

© SANS Institute 2000 - 2005 Author retains full rights.



Once your victim opens the file, type in the port number used during the configuration of the server file and complete the connection.

Signature of the Attack

The following is an example of signature patterns used to detect SubSeven. Signature based intrusion detection systems are designed to identify malicious traffic using unique patterns matches against rules in a signature database. This particular signature is one component of a file used in conjunction with the Cipherdyne's psad; The Port Scan Attack Detector product and can be viewed in it's entirety at:
http://www.cipherdyne.com/cgi/viewcvs.cgi/psad/psad_signatures.diff?r1=1.7&r2=1.8

```
tcp any -> 1243 msg:"Possible SubSeven access"; flags: S;
tcp any -> 1243 msg:"Possible SubSeven access"; flags: S; dlevel: 2;
tcp any -> 6776 msg:"Possible SubSeven access"; flags: S;
tcp any -> 6776 msg:"Possible SubSeven access"; flags: S; dlevel: 2;
```

This signature file is configured to look for a possible SubSeven port scan on tcp ports 1243 and 6676, which are just a few of the many possible ports the SubSeven Trojan server and its variants could be configured to utilize.

The next SubSeven signature was obtained from a signature file written for **SNORT** using Perl 5.6 on a Red Hat 6.x system. **SNORT** is a Linux based intrusion detection system written Martin Roesh and is available as an open source project under the GNU public license.

```
alert tcp any 16959 -> any any (msg:"BACKDOOR-SIGNATURE - SubSeven DEFCON8 2.1 Backdoor Access!"; content: "PWD"; content:"acidphreak"; nocase;)
```

This signature is written to alert on any packets using tcp port 16959. Port 16959 is one of the two default ports used by a variant of SubSeven called DEFCON8.2.1. Unfortunately, this is only one of the many possible port used by this particular variant. The Master Password for SubSeven DEFCON8 2.1 Backdoor is *acidphreak* and the signature is designed to look for that text in the packet stream.

© SANS Institute 2000 - 2005 Author retains full rights.

Like the previous example, this signature is very specific and wouldn't detect a simple modification to the exploit. The signatures listed above are dangerous because they tend to give individuals a false sense of security. An individual may be under the impression this signature would alert on all variants of SubSeven. In reality, this particular signature is custom tailored for only one variant that in itself can be modified. (change the default port to a different value). As stated in an earlier section, the server application in many of the newer Sub7 variants can be configured to monitor any TCP port between the values from 1000 to 65,535.

Identifying and Protecting an Infected System "Know Thy System"

Trojan scanning programs are very effective at detecting hidden Trojan application files on a host system. Two highly recommended Trojan scanning programs available on the Internet are *The Cleaner* from (http://www.moosoft.com/) and *Tauscan* from Agnitum Ltd. (http://www.agnitum.com/download/tauscan.html). Both of these programs are memory resident and reside in the background of the Windows operating system. According to Moosoft's web site, *The Cleaner* is capable of detecting a total of 4043 Trojan applications. Although, a comparison chart posted on Agnitum's web site claims its product is capable of detecting 2715 Trojans and lists *The Cleaners* Trojan detecting capability at 2029.

Unfortunately, current versions of popular anti-virus software are not very reliable at detecting newer Trojan applications on an infected host. In addition, many of the newer variants are delivered as "packed" files and are not easily detected with traditional anti-virus software which may lack Win32' Aspack file compressor support. However, updating your system's Anti-virus signature file is one of the most effective techniques available to fortify a system against malicious code. Personal firewall products from Zone Alarm and Symantec will alert the user of an application's attempt to establish a network connection to the Internet. A select group of applications (i.e. Mail Client, Web Browser, Anti-Virus Live Update program) should be permitted access to the Internet. Any unknown application attempting to establish a connection should be blocked by the firewall.

The following represents a list of Anti-Virus software tested against the different variants of SubSeven and was compiled by the individuals at HackFix http://www.hackfix.org/subseven/avs.shtml

© SANS Institute 2000 - 2005 Author retains full rights.

Icon Key  Does NOT detect this version of this Trojan.  Does detect this version of this Trojan.	antidote	antivir	avg	bitdefender	ezantivirus	kaspersky	mcafee	navv	norman	pccillin	rav	cleaner	pcdoorguard	pestpatrol	tauscan	tds2
Last Updated - - MDY	11 09 01	12 28 01	12 04 01	12 09 01	12 30 01	12 30 01	12 04 01	12 06 01	12 06 01	12 09 01	12 13 01	12 26 01	12 05 01	11 30 01	12 28 01	NA 01
1.0																
1.1																
1.3																
1.4																
1.5																
1.6																
1.7																
1.8																
1.9																
1.9b																
2.0																
2.1																
2.1.3MUIE																
2.13mod																
2.1a																
2.1b																
2.1bonus																
2.1c																
2.1gold																
2.2b1																
SubStealth																

NeoMonitor from NYCSoftware can also be used as an effective tool to determine if you system is infected with a RAT Trojan application. Neomonitor will list and monitor all active/inactive connections to and from

© SANS Institute 2000 - 2005 Author retains full rights.

your system. It's capable of DNS resolving the source IP addresses and destination addresses of both the inbound and outbound connections and will also attempt to classify the connection's service type. It will also display the port the connection is using and classify it as being either in a *Listening* or *Established* state. An individual using NeoMonitor can now log and keep track of all inbound and outbound connections from their system. By paying close attention to all the ports and connections being made to and from their system, a user will be able to scrutinize suspicious connections and take appropriate action.

Obviously, the most effective measure is to not accept email attachments from unknown individuals. Trojan applications typically arrive as a .com, .exe or .bat file. Therefore, any file that is downloaded from the Internet should come from a reliable or trusted source.

Trojan applications can also alter the functions of the infected host so as to surrender control of common system functions to the attacker. If your system starts exhibiting strange behaviors such as the CD ROM drive tray opening and closing, loss of control of the screen pointer, or the appearance of strange/unaccounted files in system directories, changes to the system registry or the appearance of peculiar dialogue windows containing text or keystrokes, then you are probably infected with a Trojan application and appropriate steps should be taken to clean the system. Unfortunately, the SubSeven server application registers itself as system service and will not appear in the Windows Task Manager. MyTop from CodeProject (http://www.codeproject.com/system/mytop.asp) is a utility that allows you to kill specific system processes and can be used to identify and eliminate a potential SubSeven application from your system.

Host Based Intrusion Detection products from Cisco Systems can be very effective at mitigating the risk of infection from a malicious worm or Trojan. Cisco's HIDS is based on using a combination of signature based and behavior based rule sets. Cisco's HIDS defines a set of behavior rules and bases its decision on how to treat unknown attacks on those rules.
It offers complete protection to operating systems and their resources. For the most part, system binaries should not change, many attacker tools alter system binaries to gain access to a system (backdoor root kits).
Cisco HIDS prevents the installation of root kits. It will also protect the registry keys and policies. It will protect the audit registry keys to prevent a hacker from clearing the audit log. This patented technology will also prevent the execution of the code that may have overflowed out of a buffer. It will not prevent the process from crashing, but it will prevent the execution of the malicious code which crashed the stack. For more information on Cisco's HIDS solution, refer to the following:
http://www.cisco.com/warp/public/cc/pd/sqsw/sqidsz/prodlit/wdsi_ds.htm
http://www.cisco.com/warp/public/cc/pd/sqsw/sqidsz/prodlit/sddi_ds.htm

© SANS Institute 2000 - 2005 Author retains full rights.

Techniques for Removing Variants of the Sub7 Trojan

(Source: http://www.anti-trojan.org) - *Select Trojan Info / SubSeven from the heading*

This section details the steps required for removing a majority of the SubSeven variants. Recommendation: back up the following files from your system before proceeding any further:

USER.DAT	WIN.INI
SYSTEM.DAT	SYSTEM.INI

SubSeven 1.0-1.2

These earlier versions of SubSeven were unstable and contained many bugs which prevented the system control functions from operating properly. The default TCP port used by the server application is port 1243 and was not configurable.

Removal :

Open up REGEDIT (click start , run , type REGEDIT) and navigate to the following:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

At the end, click on 'Run' and the right hand panel should change. On the right hand side of REGEDIT, look for the item titled SystemTrayIcon = "C:\WINDOWS\SysTrayIcon.Exe" Right click on the line and choose delete. Reboot, Go to Start/Find and execute a search on *systrayicon.exe* and delete all instances of this file.

SubSeven 1.3-1.4

Versions 1.3/1.4 represent improved versions of the Trojan. However, these two versions still had problems with various system control functions. TCP Port 1243 is still the default port used by the server application.

Removal :

Go to Start/Find and execute a file search for *win.ini*

After Windows finds the file, open up Windows Notepad and drag the contents of the win.ini file into the new notepad page .

Look for an entry near the top of the text with the record: *run=nodll*

Delete the text *nodll* after the entry *run*=. Close notepad and save changes .

Reboot, Go to Start/Find and execute a file search for any file named *nodll.exe* and delete it.

SubSeven 1.5

SubSeven is starting to become dangerous and more difficult to remove. The default TCP port used by the server application is still port 1243 however, the value for this port is now configurable.

© SANS Institute 2000 - 2005 Author retains full rights.

Removal
Go to Start/Find and do a file search for *win.ini*
After Windows finds the file, open up Windows Notepad and drag the contents of the win.ini file into the new notepad page .
Look for an entry near the top of the file with the
text: **run=kerne132.dl nodll**

Delete the text **kerne132.dl nodll**

Close notepad and save changes . Reboot, Go to Start/Find and execute a search for files named **nodll.exe**, **window.exe** and **winduh.dat** and delete them.

SubSeven 1.6

SubSeven has started to gain in popularity. This version is still riddled with bugs even though individuals continue to choose SubSeven over similar Trojan packages (netbus, etc.). This version uses port 1243 as the default port, however, like the previous version, this value is configurable.

Removal:
Open REGEDIT (click start , run , type REGEDIT) and follow this path
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServices
Select 'RunServices' and on the right hand panel for the key:
KERNEL16. Delete this key and reboot the system.
After windows reboots, go to Start/Find and execute a search for any file named **SysTray.exe** or **traysys.exe** and delete them. Initiate a search of the Window's system directory and scan for the following three files and delete them. (**lmdrki_33.dll**, **pddt.dat** and **rundll16.com**)

SubSeven 1.7

This version of SubSeven represents a major break-through with the introduction of the SubSeven edit server application. This application now offers more configurable options to the hacker with the release of the SubSeven edit server program with this version . This version still suffered from some minor bugs, however, Mobman continues to refine and improve his Trojan making techniques.

Removal
Open REGEDIT (click start , run , type REGEDIT) and follow this path
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServices
Select 'RunServices' and look on the right hand side panel for the key:
KERNEL16. Delete this key and reboot the system.

After windows reboots, go to Start/Find and execute a search for any

© SANS Institute 2000 - 2005 Author retains full rights.

file named **kerne16.dl** or **watching.dll** and delete them.

SubSeven 1.8

This version of Sub7 is slightly more difficult to remove.

Removal (*this is for an unedited serve file*)
Open the system.ini file in notepad and look for the following entry:
shell=Explorer.exe kerne132.dl
Delete the text **kerne132.dl** from the **shell=Explorer.exe** entry.
Close notepad, save changes and reboot .

After windows reboots, go to Start/Find and execute a search for any file named **kerne132.dl** and delete it .

SubSeven 1.9 - 1.9b

Your system will need to be booted in MS-DOS mode. When this is completed, you should be in MS-DOS looking at c:\windows\ prompt.

This version places itself at C:\windows\rundll16.exe, Simply type:
del rundll16.exe - This will delete the Trojan.
If this errors, you may need to type **attrib rundll16.exe -h**
to remove the hidden flag, then type the delete command listed above.
Type *exit* to return to Windows.

Open REGEDIT and locate the path:
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
At the end of the entry, select *'Run'* once.
On the right hand side of REGEDIT, look for the item titled
RegistryScan = "rundll16.exe"
Right click on that line only and choose delete.

Open the folders to follow the path:
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServices
At the end of the entry, select 'RunServices' once.
On the right hand side of REGEDIT, look for the item titled
RegistryScan = "rundll16.exe"
Right click on that line only and choose delete. Close REGEDIT and reboot.

SubSeven Apocalypse & SubSeven 2.0

These two versions of Sub7 utilize a new GUI for the client. Sub7 Apocalypse is less bulkier then the other previous Sub7 clients and has

© SANS Institute 2000 - 2005 Author retains full rights.

many more powerful options .

Removal (*assuming an unedited server file*)
Using a text editor, open your system.ini file and look for the following entry: **shell=Error mtmtask.dl**
Delete the text **Error mtmtask.dl** from the **shell=** entry.
Close notepad, save changes and reboot .

After windows reboots, go to Start/Find and execute a search for any file named **tmtask.dl** and delete it

SubSeven 2.1, 2.1 Gold, SubStealth, 2.1.3 MUIE and 2.1 Bonus

The easiest way to remove any of these versions is to use port listing software to detect open ports associated with specific applications. You will need to know the name of the Trojan file prior to launching the utility. Many variants of SubSeven randomize the name of the file making it more difficult to locate. The easiest way to find the name of the Trojan and the corresponding port is to use a netstat utility (NeoMonitor) or a firewall program (Zone Alarm) that shows a system's open ports.
The server application of these particular Sub7 variants can be configured to execute from one of four system locations. The server application file associated with these variants can be controlled with messages over IRC and IRQ and can alter its load procedure each time the system is booted using any of the combination of loading techniques listed below:

1) C:\Windows\Win.ini
At the top, look for two lines reading:
run=*Trojan name* load=*Trojan name*

2*)* Registry (You will need to run REGEDIT to edit the registry.)
Follow the paths using REGEDIT and find:
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServices\
each containing WinLoader = *Trojan name.* Both of these should be deleted (Right click and choose Delete.)

3) Edit the C:\Windows\System.ini file
In the System.ini file, the line containing:
shell=explore.exe *Trojan name* should be changed to
shell=explore.exe
(Simply remove the Trojan named key from the end of the line)

4) Registry (.exe file type handler)
This configuration option will implement a supposed *not know* startup technique that involves altering the .exe file type handler in

© SANS Institute 2000 - 2005 Author retains full rights.

the Registry. After modifying the handler, the Trojan will continue to reload itself into memory every time an .exe file is launched on the system. To fix the registry problem, you will need to download and launch this registry file utility to repair your registry. click here to download undo.reg

SubSeven Defcon8 (2.1)

This version of SubSeven was released at the Defcon convention in Las Vegas and has been distributed on Usenet news groups with an executable filename of "SexxxyMovie.mpeg.exe. The server file was recompiled and the default port used by this version of SubSeven can be either 6667, 16959, 27374 and can be randomly changed.

Removal

Refer to the removal instructions for SubSeven 2.1

SubSeven 2.2-Beta 1 & Beta2

According to an alert issued by Internet Security Services, SubSeven Version 2.2 added some additional capabilities to the Trojan application which include a GUI packet sniffer, support for proxies (Sock4/5), the ability of the server-client Trojan application to communicate on any random port, and CGI based notification capable of sending information about infected hosts to web sites. This version of the Trojan can be configured to eavesdrop on the victim using the infected host's microphone and can even spy on the victim if the infected system is configured with a Web-cam. The SubSeven server is still relatively small: 54,5KB.

Removal

Open REGEDIT (click start , run , type REGEDIT) and follow this path
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
Select 'Run' and look on the right hand side panel for the key:
`Loader = "c:\windows\system\***"` *** represents a random name assigned to the server, make note of it and Delete this key.

Open REGEDIT (click start , run , type REGEDIT) and follow this path
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServices
Select 'RunServices' and look on the right hand side panel for the key:
`Loader = "c:\windows\system\***"` *** represents a random name assigned to the SubSeven server file. Within many of the newer variants, the name of the actual Trojan server application can also be altered. This being the case, note the name(s) of any suspicious files referenced within the right window of REGEDIT and Delete this key and reboot your PC.

Go to Start/Find and do a file search for *win.ini*

© SANS Institute 2000 - 2005 Author retains full rights.

After Windows finds the file, open up Windows Notepad and drag the contents of the win.ini file into the new notepad page .
Look for an entry near the top of the file with the text: **run=******.**
The ***** represents a name value assigned to the server, make note of it and Delete only this text after the line **run=**
Close notepad and save changes .

Go to Start/Find and do a file search for *system.ini*
After Windows finds the file, open up Windows Notepad and drag the contents of the *system.ini* file into the new notepad page .
Look for an entry near the top of the file with the text: **shell=explorer.exe *******
The ***** represents a random name assigned to the server, make note of it and Delete only this text after the line **shell=explorer.exe**
Close notepad and save changes .

Close notepad and save changes . Reboot, Go to Start/Find and execute a search for name of the SubSeven server file represented by the ******* in the above procedure and delete it.

SubSeven 2.3 beta –Not Released

According to IT-Networks (http://www.it-networks.org.uk/article.php?sid=571&mode=&order=0&thold=0), an application claiming to be a pre-beta version of Sub Seven 2.3 was released on the Internet. In reality, this application is another backdoor Trojan that simply connects to an IRC server (irc bot dropper). For more information, refer to the next section.

NOTE: If the techniques listed above do not remove the server file from your system, then the file was probably configured using the *"less known method"* option. The technique for removing the Trojan from your system is to delete two files stored in the Windows directory named MSREXE.EXE WINDOS.EXE. (if it exists).

Source Code

According to the information documented at the following web site: http://www.simovits.com/trojans/tr_data/y1660.html, the Delphi source code for SubSeven is decompiled and available. However, after an exhaustive search, I was unable to obtain the source code for the SubSeven Trojan and would welcome any suggestions that would help in identifying a source for the code.

Additional Info

(source: http://www.f1-help.com/virus.htm)

An email with an attachment called "server.exe" was spammed to Japanese

© SANS Institute 2000 - 2005 Author retains full rights.

computer users. This attachment claimed to be an antiviral program for a virus called Pinkworm, but it was actually the SubSeven 2.0 Trojan server file. This email was sent from a Japanese Hotmail account claiming to be from Microsoft Japan Service and requested the recipient to run an attachment called "server.exe". It claimed to offer protection from the Pinkworm that is an alias for the Sub7, Backdoor.Trojan, and BackDoor-G2.svr.21 Trojan application.

(source: http://news.zdnet.co.uk/story/0,,t269-s2088985,00.html)

According to security experts, a video file claiming to be footage of the execution of Oklahoma City bomber Timothy McVeigh was discovered to contain the backdoor Trojan called SubSeven. The video file appeared on the Internet several hours after the execution and lured unsuspecting users to download and launch the malicious program. The Web page containing the Trojan, known as a "SubSeven," is no longer up, said Russ Cooper, surgeon general for security services provider TruSecure and editor of the NTBugTraq email list.

January 18 2002: According to IT-Networks (http://www.it-networks.org.uk/article.php?sid=571&mode=&order=0&thold=0), an application claiming to be a pre-beta version of Sub Seven 2.3 was released on the Internet. In reality, this application is a different backdoor Trojan that simply connects to an IRC server (irc bot dropper). After infecting a host, two files (hh2.exe and windows.exe) are created and inserted into the *windows* directory. The server file is an IRC bot script that connects back to an IRC server in an attempt to infect the system with additional bot scripts. The other file alleges to be the editserver for the Trojan and will even present a non functioning Subseven GUI claiming to be the utility for the 2.3 version of the Sub Seven Trojan. It is also rumored to attempt to exploit the UPnP vulnerability recently discoverd in many of the Windows operating systems.

Alias: Backdoor.EEYE.b (KAV), Win32.Plugbot (InnoculateIT)

To Obtain Additional Information on Sub7:

http://www.astalavista.com/trojans/library/trojans/sub7/CompleteGuide_Sub7.shtml

http://www.symantec.com/avcenter/venc/data/backdoor.SubSeven.html

To Obtain the Sub7 Trojan Application:

http://209.100.212.5/cgi-bin/search/search.cgi?searchvalue=sub+seven&%5Bsearch%5D.x=5&%5Bsearch%5D.y=1

http://astalavista.box.sk/cgi-bin/robot?srch=sub+seven+&submit=+search+

© SANS Institute 2000 - 2005 Author retains full rights.

http://a99download.ovh.org:82/pages/Ratings/

http://www.sub7.org/downloads.shtml

To Obtain the Ramen Worm Application:

http://www.tlsecurity.net/cgi-bin/download.cgi?virus/Ramen.tgz

© SANS Institute 2000 - 2005, Author retains full rights.

Document Resources/References

http://www.royalty.nu/legends/Troy.html

http://www.commodon.com/threat/threat-sub7.htm *(currently under re-construction)*

http://news.zdnet.co.uk/story/0,,t269-s2085003,00.html

http://vil.mcafee.com/dispVirus.asp?virus_k=10171

http://xforce.iss.net/alerts/advise65.php

http://www.symantec.com/avcenter/venc/data/backdoor.subseven.html

http://209.100.212.5/cgi-bin/search/search.cgi?searchvalue=sub+seven&%5Bsearch%5D.x=5&%5Bsearch%5D.y=1

http://www.astalavista.com/trojans/library/trojans/sub7/CompleteGuide_Sub7.shtml

http://www.astalavista.com/trojans/library/trojans/misc/ *(Select Trojan Hacking ZIP File)*

http://www.anti-trojan.org/page17.html *(Select Trojan Info / SubSeven from the heading)*

http://www.bsoft.swinternet.co.uk/trojans/sub7.htm

http://www.cultdeadcow.com/tools/bo.html

http://www.sub7.org/help/index.shtml

http://www.hackfix.org/subseven/fix2.2.shtml

http://www.europe.f-secure.com/v-descs/ramen.shtml

http://www.nipc.gov/warnings/advisories/2000/00-056.htm

http://www.net-security.org/cgi-bin/dlhp.cgi?url=http://hwa-security.net/

http://www.megasecurity.org/Info/ramen_worm.txt

http://www.blackcode.com/trojans/details.php?id=134

http://neworder.box.sk/showme.php3?id=3871

http://dark-e.com/archive/trojans/subseven/21defcon/index.shtml

© SANS Institute 2000 - 2005, Author retains full rights.