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 (Security 401)"
at http://www.giac.org/registration/gsec

What is SubSeven?
Giving away control of your machine!
James Wentzel

What is SubSeven

SubSeven is a backdoor Trojan for Windows 95/98, now being referred to as a Remote Administration Tool (RAT), which allows remote users to control and retrieve information from a system[1]. The SubSeven Trojan was first discovered in May of 1999 and has had many versions released since that time[2]. When SubSeven was developed it was done to improve on the capabilities that the NetBus Trojan was lacking. The powers of SubSeven can be grouped in to three major areas. File controls, Monitoring, and Network Control. SubSeven is now becoming the most popular RAT on the internet. Unlike most RAT's SubSeven normally has an update to the server every couple of weeks and with each update, it has more features added.[3]

© SANS Institute 2000 - 2002, Author retains full rights.

The file controls of SubSeven include a huge number of utilities. Of these different utilities some of the most powerful allow the remote user the ability to transfer files to or from the remote computer. The ability to move, copy, rename or delete files off of the remote computer, the ability to erase the entire users hard drive, and the ability to Execute programs.[4] With these basic controls it gives the hacker the ability to install new versions of the Trojan onto the system, making all of the additional features that are added to the Trojan available to the hacker. These features also allow for the hacker to copy sensitive information off of the computer without the owner of the computer having any knowledge of it.

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

The Monitoring controls give the person that is remotely accessing the machine the ability to collect huge amounts of information. This information that can be gathered includes the ability to see exactly what is on the screen of the computer that is being remotely accessed. The hacker also has the ability to see all of key presses that the person using the computer types and these keystrokes can also be logged, what this means is that if a password is typed at the keyboard, the actual password will be logged. This gives the hacker the ability to collect usernames and passwords for access to other systems that the user has access to. You also have all of the capabilities as if you were using some type of package like PC-Anywhere to remotely access the computer.[5]

The Network controls have some powerful tools also. With these network tools you can see all open connections on a machine that is being accessed and the hacker can close any open connections that it wants to. One of the most powerful tools is the ability to relay off of the computer to attack another system, limiting the chance that the actual hacker will get caught and the person who's computer is being used to do scan or attack will be the one to get the blame.[6] In a recent release of SubSeven there is a new feature that is undocumented, this feature allows the machine that is running the Trojan to be used to send a huge number of ping to a Web server from numerous infected clients simultaneously causing a distributed denial of service attack. This information was gotten from research completed by the security outfit iDefense.[7]

When a hacker is creating the Trojan to be sent to an unsuspecting person, one of the features of SubSeven is the ability for it to be configured to inform the hacker by many different means that a machine has been infected and in this notification it contains all of the information that is necessary for the hacker to use the Trojan on the infected computer[8].

When configuring the SubSeven Trojan the hack can select up to 4 different notification methods that a machine has been infected. The notification methods include ICQ notification to a specific user, IRC Notification using a specific server, port and user, or an e-mail notification sending the message to a specific user relaying off of a predefined relay server. Any one of these methods can be selected or any combination of these methods can be selected. If none of these methods are selected then no notification will be sent.

© SANS Institute 2000 - 2002, Author retains full rights.

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

When configuring the SubSeven server, there are many ways to select for the SubSeven server to startup automatically on the infected computer. For these different methods to work, the installation of SubSeven modifies some key files on the infected machine. The normal files and entries that get updated are the following:

1) an entry on the "shell=" line in the SYSTEM.INI file
2) an entry on the "load=" or "run=" line in the WIN.INI file
3) In the registry "HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run"
4) In the registry "HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices"

On most of the systems that have been compromised with SubSeven, it has been found most often to be in the first location.[9]

© SANS Institute 2000 - 2002, Author retains full rights.

The full list of features offered as part of SubSeven v2.1 are:
Address book
Wwp pager retriever
Win2ip
Remote IP scanner
Host lookup
Get Windows CD-KEY
Update victim from URL
ICQ takeover
FTP root folder
Retrieve dial-up passwords along with phone numbers and usernames
Port redirect
IRC bot
File Manager bookmarks
Make folder, delete folder [empty or full]
Process manager
Text 2 speech
Clipboard manager [EDIT SERVER CHANGES]
Customizable colors
Change server ICON
Pick random port on server startup
Irc bot configuration
Restart server
AOL Instant messenger spy
Yahoo messenger spy
Microsoft messenger spy
Retrieve list of ICQ usernames and passwords
Retrieve list of AIM users and passwords
App redirect
Edit file
Perform clicks on victim's desktop
Set/change screen saver settings [Scrolling Marquee]
Restart Windows
Ping server
Compress/Decompress files before and after transfers
The matrix
Ultra fast IP scanner
IP Tool [Resolve Host names/Ping IP addresses]
Get victim's home info
    Address
    Business name
    City
    Company
    Country
    Customer type
    e-mail

© SANS Institute 2000 - 2002, Author retains full rights.

real name
state
city code
country colde
local phone
zip code

Configure Client colors
Configure menu options]add/delete pages, change names]
Automatically Display Image when downloaded [jpg, bmp]
Automatically edit files when downloaded [txt, bat]
Change port numbers for The Matrix, Keylogger and Spies
Retrieve "SubSeven message of the day"
Protect Server's port and Password once installed
Melt server when executed
Protect server settings with a password
Open Web Browser to specified location
Restart Windows [5 methods]:
- Normal shutdown
- Forced Windows shutdown
- Log off Windows user
- Shutdown Windows and turn off computer
- Reboot System

Reverse/restore Mouse buttons
Hide/Show Mouse Pointer
Control Mouse
Mouse Trail Config
Set Volume
Record Sound file from remote mic.
Change Windows Colors / Restore
Hang up Internet Connection
Change Time
Change Date
Change Screen resolution
Hide Desktop Icons / show
Hide Start Button / show
Hide taskbar / show
Open CD-Rom Drive / Close
Beep computer Speaker /stop
Turn Monitor off /on
Disable CTRL+ALT+DEL / Enable
Turn on Scroll Lock / off
Turn on Caps Lock / Off
Turn on Num Lock / Off
Connect / Disconnect
Fast IP Scanner

© SANS Institute 2000 - 2002, Author retains full rights.

Get Computer Name
Get User Name
Get Windows and System Folder Names
Get Computer Company
Get Windows Version
Get Windows Platform
Get Current Resolution
Get DirectX Version
Get Current Bytes per Pixel settings
Get CPU Vendor
Get CPU Speed
Get Hard Drive Size
Get Hard Drive Free Space
Change Server Port
Set / Remove Server Password
Update Server
Close Server
Remove Server
ICQ Pager Connection Notify
IRC Connection Notify
E-Mail Connection Notify
Enable Key Logger/Disable
Clear the Key Logger Windows
Collect Keys pressed while Offline
Open Chat Victim + Controller
Open Chat among all Connected Controllers
Windows Pop-up Message Manager
Disable Keyboard
Send Keys to a remote Window
ICQ Spy
Full Screen Capture
Continues Thumbnail Capture
Flip Screen
Open FTP server
Find Files
Capture from Computer Camera
List Recorded Passwords
List Cached Passwords
Clear Password List
Registry Editor
Sent Text to Printer
Show files/folders and navigate
List Drives
Execute Application
Enter Manual Command
Type Path Manually

© SANS Institute 2000 - 2002, Author retains full rights.

Download Files
Upload Files
Get File Size
Delete File
Play *.wav
Set Wallpaper
Print .txt/.rtf file
Show image
List Visible Windows
List all active Applications
Focus on Window
Close Window
Disable X (close] button
Hide/unhide a Window from view
Enable Disable Window
Set Quality of Full Screen Capture
Set Quality of Thumbnail Capture
Set Chat font size and Colors
Set Client's User Name
Set Local 'Download' directory
Set quick help [hints]
Pre Set Target Port
Preset Server Password
Attach EXE File
Pre Set filename after installation
Pre Set Registry Key
Pre Set Auto Start Methods:
    Registry: Run
    Registry: RunServices
    Win.ini
    Less Known Method
    Not Known Method
Pre Set Fake error message
Pre Set Connection Notify Username
Pre Set Connection Notify to ICQ#
Pre Set Connection Notify to E-Mail
Pre Set Connection Notify to IRC Channel or Nickname

All of the listed features are available in version 2.1 and will be included in newer releases of the program.[10] This list is a constantly changing list as newer versions of the program become available.

If you find that your machine has been infected with SubSeven, you are not completely out of luck. SubSeven is actually very easy to remove from the system. You just need to do some very basic steps.

1) delete the virus executable file

© SANS Institute 2000 - 2002, Author retains full rights.

2) remove the virus startup entries in the registry
3) Correct the changed settings in the registry and system.ini file
4) After all is done, reboot and let the new settings take effect[11]

The best way to prevent a machine from being infected with subseven is to practice good habits. These good habits include no opening anything that you do not know the original source of. Also, you always want to have current Anti-Virus software running on your computer, what this does for you is to prevent older versions of the Trojan from infecting your computer and if your computer has been compromised when a new update becomes available it may find that your machine has been compromised. Finally, it is always a good idea to have some type of personal firewall running on your computer. I have found that the personal firewalls that prevent all outbound traffic from programs that have not been given this type of access to be the best to prevent this type of a Trojan. The only draw back to this is if the Trojan is installed with the name of an application that does have the type of access out of your computer to send the notification. However, most of these personal firewalls by default block outbound traffic from your computer on the standard ports that are used by this and many other Trojans.

---

[1] Symantec, "SunSeven 2.0 Server", 10/4/1999 http://www.symantec.com/avcenter/venc/data/sub.seven.20.html (1/19/2001)
[2] rmbox, windos.exe/sub7info, 2/7/2000, http://discussions.virtualdr.com/Forum1/HTML/007663.html (2/13/2001)
[3] The Next Generation is Now, http://www.sub7.org.uk/main.htm (2/13/2001)
[4] HackFix "SubSeven – About SubSeven" http://www.hackfix.org/subseven/about.shtml (1/19/2001)
[5] ibid.
[6] ibid.
[7] Chris Pallack, Sub7 vid Trojan can launch distributed attacks, 6/17/2000, http://www.linuxfw.org/articles/network_security_article-903.html, (2/13/2001)
[8] HackFix "SubSeven – About SubSeven" http://www.hackfix.org/subseven/about.shtml (1/19/2001)
[9] Donald F. Kelloway, "The Basics of SubSeven (aks Sub7 or Backdoor_G) http://www.commodon.com/threat/threat-sub7.htm, (1/24/2001)
[10] About SubSeven, http://www.sub7files.com/about/index.shtml (2/13/2001)
[11] rmbox, windos.exe/sub7info, 2/7/2000, http://discussions.virtualdr.com/Forum1/HTML/007663.html (2/13/2001)

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