

SUBSEVEN (ALIAS:BACKDOOR)

Commodon Communications

INTRODUCTION

SubSeven (aka Sub7 or Backdoor_G) currently affects Windows 95/98 PC's and can be a bit tricky to remove. This is because the server portion can be configured to rerun itself automatically from any of four places each time the system has been rebooted. The trojan also has two files that can be configured with any name.

As mentioned above and although the server portion can have any name, it's found in the WINDOWS directory, with one of the following:

"server.exe" (328kb)
"rundll16.exe" (328kb)
"systray.dll" (328kb)
"Task_bar.exe" (328kb)

The second file is found in the WINDOWS\SYSTEM directory, with one of the following:

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

TCP port 6711 and 6776 are used by default, but there's a third TCP port which is the port used in the establishment of the connection between the "client" and "server". This third TCP port can be configured to be anything, although it's commonly seen as TCP port 1243 or TCP port 1999.

As mentioned above, the server portion of the trojan can be configured by the hacker to rerun itself everytime the system is rebooted due to an entry in one of the four locations. Provided below, are the four locations.

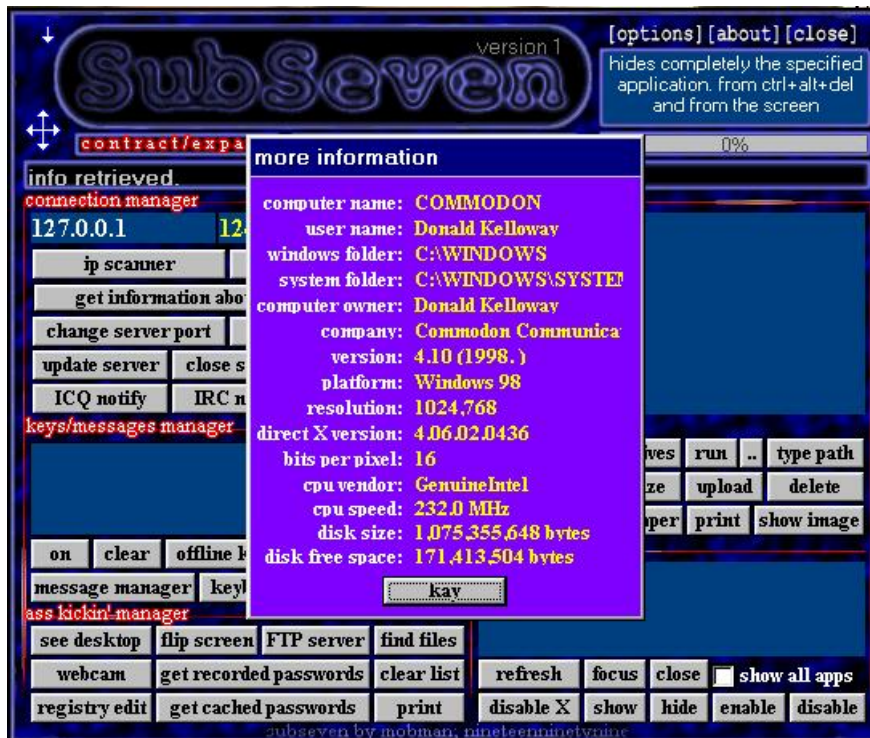
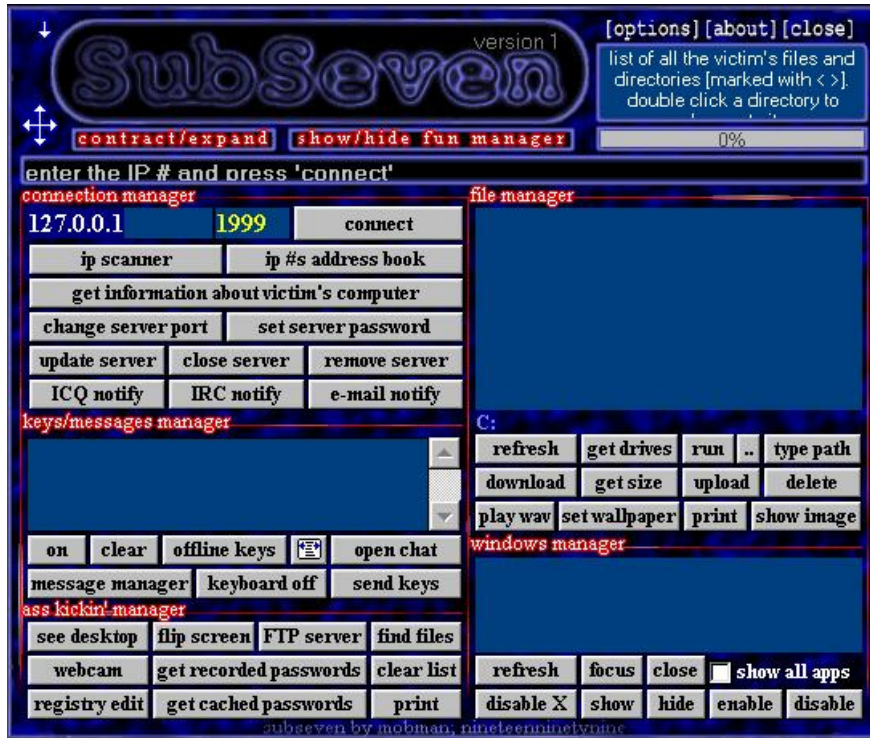
- The first, is an entry on the "shell=" line in the SYSTEM.INI file.
- The second, is an entry on the "load=" or "run=" line in the WIN.INI file.
- The third, is under:
"HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run"
- The fourth, is under:
"HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices"

Of the systems compromised with SubSeven, it's often found to be the first location.

SUBSEVEN BASIC PROGRAM

Here is a screenshot of the client portion of the program:

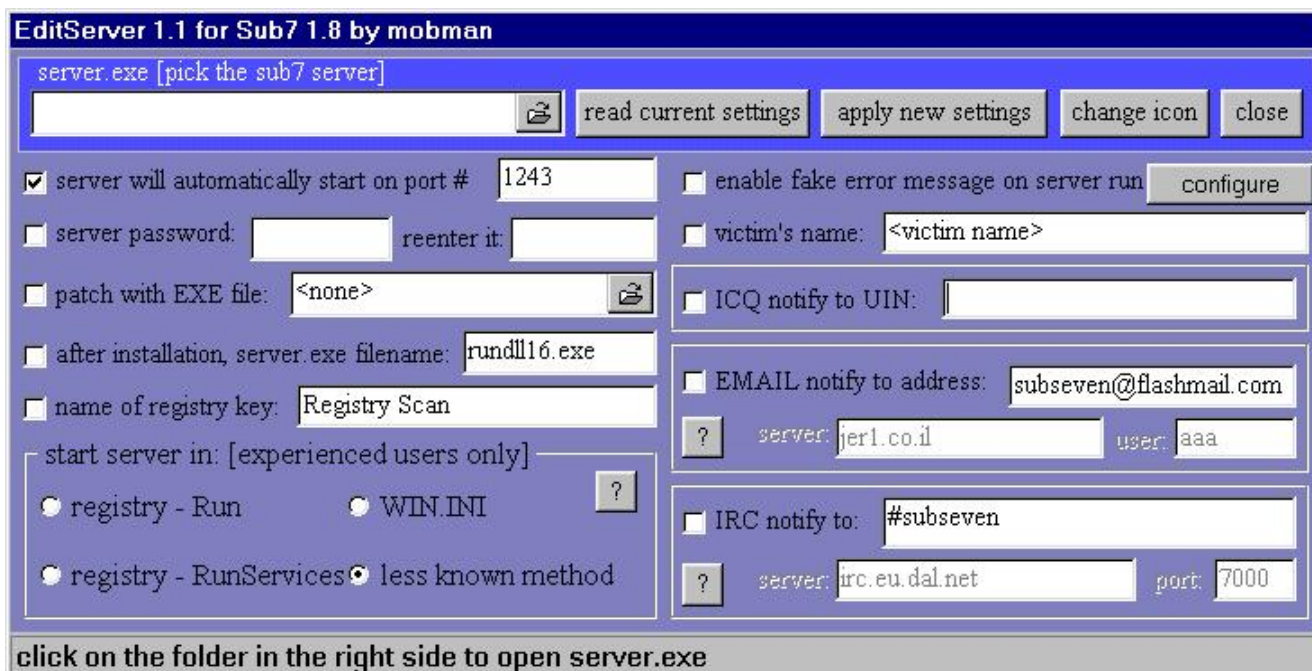
SUBSEVEN (ALIAS:BACKDOOR) Commodon Communications



Here is a screenshot of the client portion after information has been captured from a victim:

SUBSEVEN (ALIAS:BACKDOOR)

Commodon Communications



Here is a screenshot of the EditServer Utility to used to configure the server portion of the program:

The SubSeven backdoor was first discovered in May, 1999. First samples of this backdoor were not packed, but later some packed versions appeared which were not easy to detect with contemporary anti-virus programs that had no Win32 'Aspack' file compressor unpacking support. The backdoor is usually distributed under different names via newsgroups and e-mails.

When run, the backdoor copies itself to the Windows directory with the original name of the file it was run from or as SERVER.EXE, KERNEL16.DL, RUNDLL16.COM, SYSTEMTRAYICON!.EXE or WINDOW.EXE (names are different in different versions of SubSeven). Then it unpacks a single DLL file to the Windows System directory - WATCHING.DLL (some versions don't do this). After that the backdoor patches Windows Registry so that its main application will be run during every Windows bootup (Run or RunServices keys). Finally, it creates and modifies some other Registry keys. The backdoor can also install itself to the system by modifying either the WIN.INI or the SYSTEM.INI file.

The latest versions of the SubSeven backdoor drop a small starter program (usually WINDOS.EXE) and register it to be run when any EXE file is started in Windows. By doing this the backdoor ensures that its copy is always in the memory. For specific instructions of how to disinfect these versions please see the bottom of the page.

All the recent versions of SubSeven are supplied with a server configuration utility that allows it to customize server part capabilities - installation method, custom startup message, etc. This method was first introduced by the Back Orifice 2000 backdoor and it allows much more flexibility to backdoors.

SUBSEVEN (ALIAS:BACKDOOR)

Commodon Communications

If the SubSeven backdoor task is being active in the memory (and invisible in Task Manager), it looks for TCP/IP connections and if they are established it listens to TCP/IP ports for commands from a client part. A person who has a client part gets control over the remote system where the server part is installed.

Here's the list of 113 capabilities that the initial version of SubSeven had:

Fun Manager

1. Open Web Browser to specified location.
2. Restart Windows.
3. Reverse Mouse buttons.
4. Hide Mouse Pointer.
5. Move Mouse.
6. Mouse Trail Config.
7. Set Volume.
8. Record Sound file from remote mic.
9. Change Windows Colors / Restore.
10. Hung up Internet Connection.
11. Change Time.
12. Change Date.
13. Change Screen resolution.
14. Hide Desktop Icons / Show
15. Hide Start Button / Show
16. Hide taskbar / Show
17. Opne CD-ROM Drive / Close
18. Beep computer Speaker / Stop
19. Turn Monitor Off / On
20. Disable CTRL+ALT+DEL / Enable
21. Turn on Scroll Lock / Off
22. Turn on Caps Lock / Off
23. Turn on Num Lock / Off

Connection Manager

1. Connect / Disconnect
2. IP Scanner
3. IP Address book
4. Get Computer Name
5. Get User Name
6. Get Windows and System Folder Names
7. Get Computer Company
8. Get Windows Version
9. Get Windows Platform
10. Get Current Resolution
11. Get DirectX Version

SUBSEVEN (ALIAS:BACKDOOR)

Commodon Communications

12. Get Current Bytes per Pixel settings
13. Get CPU Vendor
14. Get CPU Speed
15. Get Hard Drive Size
16. Get Hard Drive Free Space
17. Change Server Port
18. Set Server Password
19. Update Server
20. Close Server
21. Remove Server
22. ICQ Pager Connection Notify
23. IRC Connection Notify
24. E-Mail Connection Notify

Keyboard Manager

1. Enable Key Logger / Disable
2. Open Key Logger in a remote Window
3. Clear the Key Logger Windows
4. Collect Keys pressed while Offline
5. Open Chat Victim + Controller
6. Open Chat among all connected

Controllers

1. Windows Pop-up Message Manager
2. Disable Keyboard
3. Send Keys to a remote Window

Misc. Manager

1. Full Screen Capture
2. Continues Thumbnail Capture
3. Flip Screen
4. Open FTP Server
5. Find Files
6. Capture from Computer Camera
7. List Recorded Passwords
8. List Cached Passwords
9. Clear Password List
10. Registry Editor
11. Send Text ot Printer

File Manager

1. Show files/folders and navigate

SUBSEVEN (ALIAS:BACKDOOR)

Commodon Communications

2. List Drives
3. Execute Application
4. Enter Manual Command
5. Type path Manually
6. Download files
7. Upload files
8. Get File Size
9. Delete File
10. Play *.WAV
11. Set Wallpaper
12. Print *.TXT*.RTF file
13. Show Image

Window Manager

1. List visible windows
2. List All Active Applications
3. Focus on Window
4. Close Window
5. Disable X (close) button
6. Hide a Window from view.
7. Show a Hidden Window
8. Disable Window
9. Enable Disabled Window

Options Menu

1. Set Quality of Full Screen Capture
2. Set Quality of Thumbnail Capture
3. Set Chat font size and Colors
4. Set Client's User Name
5. Set local 'Download' Directory
6. Set Quick Help
7. Set Client Skin
8. Set Fun Manager Skin

Edit Server

1. PreSet Target Port
2. PreSet server Password
3. Attach EXE File
4. PreSet filename after installation
5. PreSet Registry Key
6. PreSet Autostart Method:
 - Registry: Run
 - Registry: RunSevices

SUBSEVEN (ALIAS:BACKDOOR)

Commodon Communications

Win.ini

Less known method

7. PreSet Fake error message
8. PreSet Connection Notify Username
9. PreSet Connection Notify ICQ#
10. PreSet Connection Notify E-Mail
11. PreSet Connection Notify IRC Chan.
12. PreSet IRC Port
13. Change Server *.exe Icon

The author of the SubSeven backdoor calls himself Mobman. His backdoor can be considered to be one of the most advanced ones at the moment.

Subseven tries to use ICQ, IRC and different e-mail accounts to notify the author that his victims are online.

SubSeven is a trojan for the windows platform. It comes at least in two parts a client and a server. The client is used by the hacker to connect to the victim' s machine. Once the server.exe is installed on the victim's machine the hacker has full access to the victim's machine.

The zip-file I downloaded contained 3 executables:

- server.exe The real trojan, which is installed on the victim's machine
- sub7.exe The client used by the hacker to connect to his victim's machine
- EditServer.exe A configuration utility to set several configuration options on server.exe.

The EditServer.exe gives the hacker the opportunity to configure:

- the port used by server.exe
- to set a password for the server
- several other values

and most important to set some notification options, to notify the hacker when his victim(s) are online. This notification can be done using ICQ, IRC, or e-mail.

KNOWN INFORMATION ABOUT SUBSEVEN

Known TCP ports for SubSeven:

- 1243
- 6711
- 6712
- 6713
- 6776

Known TCP ports for SubSeven 2.1

- 27374

Files on an infected machine:

- server.exe

Revised December 21, 2008

SUBSEVEN (ALIAS:BACKDOOR)

Commodon Communications

- rundll1.exe
- systray.dll
- Task_bar.exe
- FAVPNMCFEE.dll
- MVOKH_32.dll
- nodll.exe
- watching.dll

Entries in configuration files:

- in system.ini:
 - an entry on the line containing "shell="
- in win.ini:
 - an entry on the line containing "load=" or "run= "
- in the registry:
 - HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\Current\Version\Run
 - HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices

To be able to connect to the victims machine the hacker needs the ip address of that machine. There are two methods to get this ip address:

1. Using ICQ - If the victim has not enabled IP Hiding in his ICQ User Profile, then the hacker can retrieve this information from the victim's profile.
2. To use the notification option of the trojan. That way the hacker is always notified when his victim(s) connect to the internet. He will even get the IP address and the port number delivered.

It is claimed in the description of SubSeven that most Antivirus Software won't be able to detect newer versions of it. Have a look in your registry whether the strings SubSeven, "Sub Seven" or "Sub 7" are found. If yes, your machine got infected. If no, well that does not mean that your machine is not infected, since the hacker can set the values used in the registry with the EditServer.exe. The server.exe can be removed using the file client.exe. If you downloaded and extracted the zip-archive of the subseven-trojan do not click on the file server.exe. Otherwise you will have infected your machine.

DETECTING SUBSEVEN ON THE NET

The following attack patterns for the NIDS *snort* can be used to recognize SubSeven network activity:

```
alert tcp $HOME_NET 1243 -> !$HOME_NET any (msg:"
TROJAN ACTIVITY-Possible Subseven"; flags:SA;)
alert tcp any any -> any any (msg:"TROJAN ACTIVITY-Possible
SubSeven access"; content:"connected. time/date"; flags:PA;)
alert tcp !$HOME_NET any -> $HOME_NET 6776 (msg:"TROJAN ATTEMPT-
SubS even access"; flags:S;)
alert tcp !$HOME_NET any -> $HOME_NET 6711 (msg:"TROJAN ATTEMPT-
Deep Throat/SubSeven"; flags:S;)
alert tcp !$HOME_NET any -> $HOME_NET 1243 (msg:"TROJAN ATTEMPT-
```

SUBSEVEN (ALIAS:BACKDOOR)

Commodon Communications

Subseven"; flags:S;)

REMOVING SUBSEVEN

Disinfection of SubSeven is performed automatically by FSAV. You might need to restart your system to complete the disinfection of a locked server part of SubSeven that cannot be removed while it is active in Windows. Note that earlier versions of FSAV might not clean the "EXE-file startup" Registry entry, which is used by the latest SubSeven versions to re-install itself back to the system every time an EXE file is run. So, if you are still having problems with this registry key even after the disinfection and if you are unable to start EXE files in Windows, please download and run the special file from our ftp site, which will solve this problem:

<ftp://ftp.europe.F-Secure.com/anti-virus/tools/s7disinf.reg>

You need to run (double-click or press 'Enter' when the cursor is placed on the file) the S7DISINF.REG file from Windows Explorer after you have downloaded it. Note that the .REG extension might not be visible if you do not have 'Show All Files' option on. Alternatively you can click on the 'Start' button, then on the 'Run' menu and either input the location of the S7DISINF.REG file manually (for example, C:\S7DISINF.REG) or to find it with the 'Browse' button. After you have entered the location, you need to click on the 'Ok' button and the REG file will be run which will solve your SubSeven problem. If you have problems locating or running the downloaded file, please consult a more experienced computer user.

You can also use a free version of F-Prot for DOS to remove SubSeven from an infected system. In this case you will have to perform disinfection from pure DOS. It is advised to run the above shown REG file before exiting Windows.

<ftp://ftp.europe.F-Secure.com/anti-virus/free/>

<ftp://ftp.europe.F-Secure.com/anti-virus/updates/f-prot/dos/>

All SubSeven components (files) should be deleted from an infected system for successful disinfection.

To Remove SubSeven Manually:

1. Edit SYSTEM.INI
If you find the line shell=Explorer.exe Task_Bar.exe, remove the Task_Bar.exe entry. Ave SYSTEM.INI
2. Edit win.ini and look at the lines containing run= and load=. If you find one of the files listed above, remove this entry (entries).
3. Start the regedit.exe and search for the files listed above. If you find an entry with one of the files, remove it.
4. Reboot