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

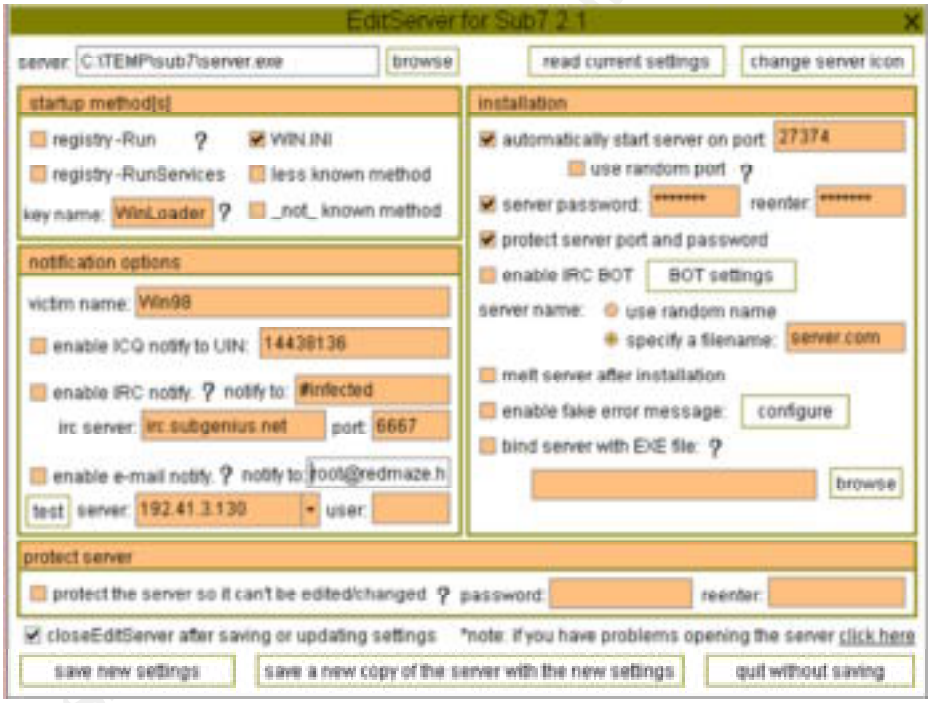
GIAC Advanced Incident Handling and Hacker Exploits
Practical Assignment for SNAP San Jose

Robert V. McMillen Jr.

SubSeven Program Documentation

SubSeven v.2.1.3 BONUS by mobman is a backdoor program that allows others to gain full access to Windows 9X systems through a network connection. The author updates the tool on a regular basis in order to stay ahead of the virus detection programs, and makes it available at http://subseven.slak.org.

The program consists of three different components: CLIENT (SubSeven.exe), SERVER (server.exe), and a server configuration utility (EditServer.exe). The client is a graphical user interface (GUI) used to connect to the server via a network/internet connection. The server is installed on the remote system, but it must be configured with the server editor prior to installation.



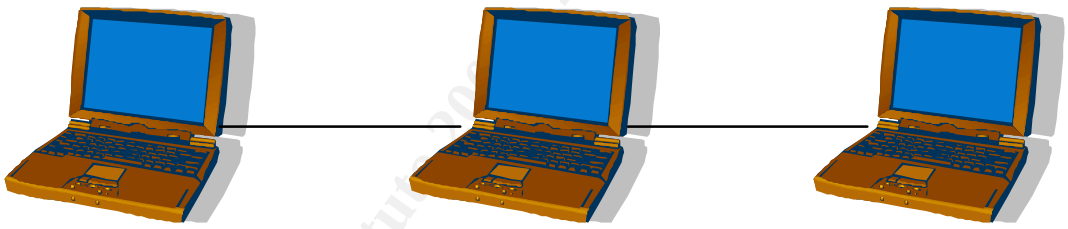
Possible Server Configuration:

- Can be configured to startup in several different ways:
  - The registry-Run option installs the server to start as an application when the user logs onto the system.
  - The registry-RunServices option installs the server to start as a service at system startup from the registry.

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

  - The Win.ini option installs the server to start at system startup or user logon from the Win.ini.
  - The less known method installs the server to start as system startup or user logon from the system.ini.
- Can be configured to notify the client of IP address changes via ICQ, IRC, or e-mail. Very useful feature when the remote system uses DHCP or a dial-up ISP.
- The TCP port the server listens on is 27374 by default, but it can be changed to any port or a random port.
- Both the listening port and the server can be password protected in order to keep other SubSeven clients from login onto the server.
- Can configure the server to delete the installation file once its been installed.
- Can bind the server with a legitimate executable file in order to hide the existence of the Trojan.
- Can configure the server so it cannot be changed at a later time.

System Configuration for Documentation:



Client (Attacker) Windows NT 4.0 192.168.0.2

Sniffer (Redmaze) Linux RedHat 6.1 192.168.0.1

Server (Victim) Windows 98 192.168.0.15

Server Configuration used for this documentation:

- Server Operating System: Window 98.
- Start-up Method: Win.ini.
- Victim Name: Victim.
- Notification Options: e-mail.
- Server Listening Port: 27374.
- Enabled Server Password.

The server software was installed on the victim via a floppy diskette. Tcpdump and Snort were used to analyze the program's communications.

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

Client (Attacker) Utilities:

The SubSeven Client is used to connect to the SubSeven Server. This section will explain all remote control features available to the attacker.



The IP Scanner allows the attacker to scan IP address blocks in order to find servers listening on the configured port. This utility is useful if the attacker spreads the server to multiple systems. It also allows the attacker to perform the scan from a remote SubSeven server in order to hide the identity of his system.

The get pc info provides the attacker additional information about the victim's machine.





The get home info retrieves the current user's personal information. This only works if the victim entered any of his or her personal information.

The server options window allows remote configuration of the server. It allows changes to the listening port; change or remove the password; restart, remove, or close the server; and update the server file from a local file or a website.



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



IP notify allows the attacker to remotely reconfigure the IP notification options.



The keyboard feature allows the attacker: to see what the victim is currently typing at the keyboard; to send keystrokes to the victim's system; to retrieve the victim's keystrokes while offline; and to disable the victim's keyboard.



If for some reason the attacker wants to chat with the victim, the attacker can use the chat utility. This feature opens a chat window on both the client and the server that allows chat functionality.



The matrix takes over the victim's screen and basically establishes a one-way (attacker to victim) chat session.

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



With the msg manager, the attacker can create different types of windows to appear on the victim's system. The status bar at the bottom of the SubSeven window will tell the attacker which button the victim selected from the crafted window.



Spy will allow the attacker to see the victim's ICQ, AOL instant Messenger, MSN Messenger, and Yahoo Messenger communications on the internet.



As the name implies, ICQ takeover will list and allow the attacker to takeover any existing ICQ sessions.

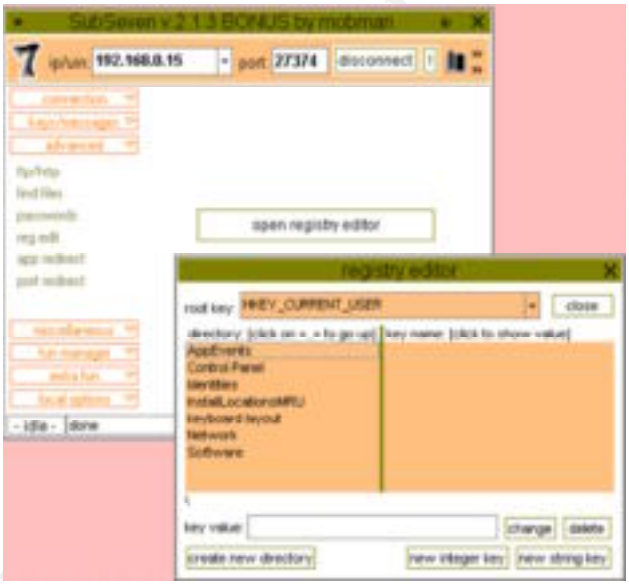


ftp/http establishes a listening ftp server on the victim. The attacker can configure the ftp server's listening port, password, and maximum number of users. The attacker can also use a web browser to view the victim's files by using the following URL: ftp://password@ip address:port

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



The passwords function checks for cached, recorded, or received passwords on the victim's system as well as retrieve dial-up, ICQ, and AOL Instant Messenger passwords.



Reg edit gives the attacker full control of the victim's registry. As you can see by the figure, the attacker can add, delete, or modify any registry key.

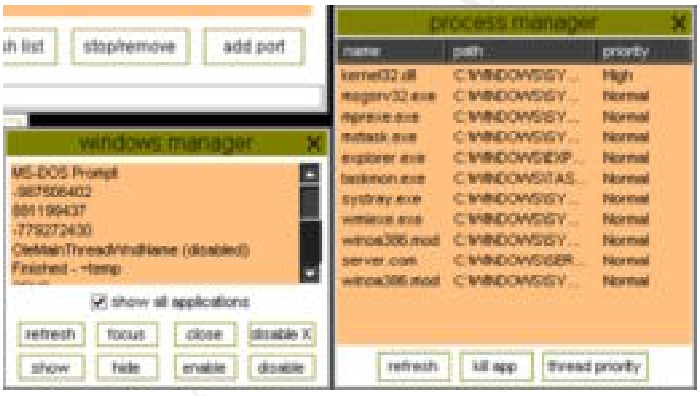


The app redirect and port redirect allow the attacker to execute applications and redirect ports on the victim's system. The output of the applications will appear on the attackers window.

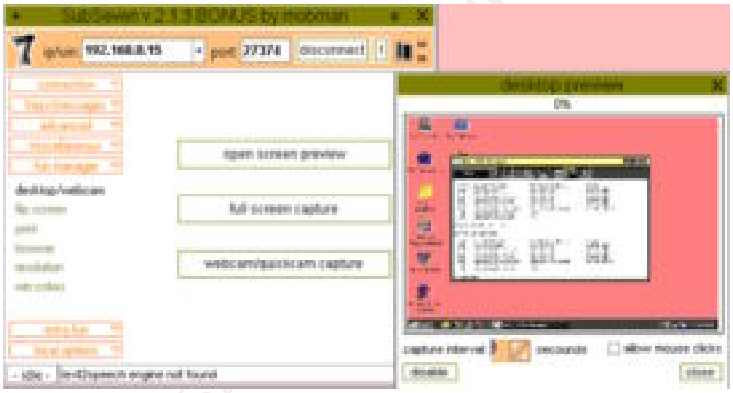
© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.



The file manager option gives the attacker full control of the victim's magnetic media. The attacker can upload, download, delete, edit, view, execute, and gather information on any file on the victim's system.



The next two options, window manager and process manager show all active windows and running processes, respectively, on the victim's system. From here, the attacker can stop, hide, or upgrade the priority of any window or process on the victim's system. Note: The SubSeven server is shown on the process manager (server.com).



The fun manager gives the attacker three very cool options. Screen preview, which can be configured to update every few seconds and allow the attacker's mouse click to execute on the victim's system. Then a next option is a full screen capture. Does not allow for continual update or mouse execution, but it gives you a full size picture of the victim's screen. Finally, if the victim has a video camera attached to the system, the attacker can retrieve live video (uses a different pre-configured port).

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



Flip screen will flip the victim's screen vertically or horizontally or both.

The print option will print attacker specified text to the victim's printer, and the browser option will start the victim's default web browser to an attacker specified URL.

As the names imply, the resolution options provides the victim's possible screen resolutions, and the win colors allows the attacker to change the default window colors on the victim's system.

The extra fun menu begins with the screen save option. If the victim has the scrolling marquee screen saver installed, this option allows the attacker to reconfigure the screen saver and execute it.





With restart win, the attacker can shutdown windows, log off the current user, shutdown the system, or reboot the system.

The mouse option really lets the attacker confuse and irritate the victim. Everything from hiding the mouse cursor to switching the mouse buttons.



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



The sound option retrieves the victim's current sound settings, and provides a limited configuration capability. However, if the victim has a microphone attacked to the system, the attacker can record and retrieve sound files of the victim.

As the name implies, the time/date option report the victim's current time and date settings. It also provides the capability to change the time and date settings on the victim's system.



The extra option toggles on or off the desktop, Start button, taskbar, CD-ROM, speaker, and monitor. It also disables the Ctrl-Alt-Del, Scroll Lock, Caps Lock, and Num Lock.

The local options allow the attacker to configure the quality of screen captures and video captures from the remote system. It allows the attacker to redefine the default folder where the screen captures and any downloaded files will be stored. And other appearance changes to the client GUI.

Program Protocol Analysis:

SubSeven accomplishes network communications by using TCP/IP. After startup, the server notifies the client by sending an e-mail, the following traffic was generated (tcpdump):

```
victim.1025 > redmaze.home.smtp: S 44331:44331(0) win 8192 <mss
    1460,nop,nop,sackOK> (DF)
redmaze.home.smtp > victim.1025: S 30637657:30637657(0) ack 44332 win 32120
    <mss 1460,nop,nop,sackOK> (DF)
victim.1025 > redmaze.home.smtp: . 1:1(0) ack 1 win 8760 (DF)
```

As you can see, SubSeven uses the victim's system to directly connect to the configured mail server. It does not use the user's e-mail application; therefore, it will not leave traces of notification on the victim system.

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

However, if your e-mail clients download their mail from a central mail server, you can use the SubSeven e-mail notification as a possible intrusion detection fingerprint. Your mail server should be the only machine establishing a connection to port 25 (SMTP).

Next, we see the attacker connecting to the victim in order to gain access (tcpdump):

```
badguy.1269 > victim.asp: S 98382:98382(0) win 8192 <mss 1460> (DF)
victim.asp > badguy.1269: S 1895687:1895687(0) ack 98383 win 8760 <mss
    1460> (DF)
badguy.1269 > victim.asp: . 1:1(0) ack 1 win 8760 (DF)
```

As you can see, it establishes a connection using TCP/IP. The majority of the communication traffic is cryptic, but passwords and answers to attacker requests are sent in plain text (snort output depicted below).

Attacker Login onto the victim.

```
192.168.0.15:27374 -> 192.168.0.2:1275 TCP TTL:128 TOS:0x0 ID:35329  DF
*****PA* Seq: 0x2B3C86   Ack: 0x18090   Win: 0x2238
50 57 44 00 00 00                              PWD...

192.168.0.2:1275 -> 192.168.0.15:27374 TCP TTL:128 TOS:0x0 ID:50969  DF
******A* Seq: 0x18090   Ack: 0x2B3C89   Win: 0x2235
00 00 00 00 00 00                              ......

192.168.0.2:1275 -> 192.168.0.15:27374 TCP TTL:128 TOS:0x0 ID:51225  DF
*****PA* Seq: 0x18090   Ack: 0x2B3C89   Win: 0x2235
50 57 44 31 31 61 67 64 74 6C                  PWDtest
```

Attacker request and Victim's reply for a root directory listing.

```
192.168.0.2:1275 -> 192.168.0.15:27374 TCP TTL:128 TOS:0x0 ID:51737  DF
*****PA* Seq: 0x1809A   Ack: 0x2B3CCA   Win: 0x21F4
52 53 48 43 3A 00                              RSHC:.

192.168.0.15:27374 -> 192.168.0.2:1275 TCP TTL:128 TOS:0x0 ID:35841  DF
*****PA* Seq: 0x2B3CCA   Ack: 0x1809F   Win: 0x2229
52 53 48 30 33 33 34 34                        RSH03344

192.168.0.2:1275 -> 192.168.0.15:27374 TCP TTL:128 TOS:0x0 ID:51993  DF
******A* Seq: 0x1809F   Ack: 0x2B3CD2   Win: 0x21EC
00 00 00 00 00 00                              ......

192.168.0.15:27374 -> 192.168.0.2:1275 TCP TTL:128 TOS:0x0 ID:36097  DF
*****PA* Seq: 0x2B3CD2   Ack: 0x1809F   Win: 0x2229
43 4F 4E 46 49 47 2E 44 4F 53 0D 0A 43 4F 4D 4D  CONFIG.DOS..COMM
41 4E 44 2E 43 4F 4D 0D 0A 53 55 48 44 4C 4F 47  AND.COM..SUHDLOG
2E 44 41 54 0D 0A 46 52 55 4E 4C 4F 47 2E 54 58  .DAT..FRUNLOG.TX
54 0D 0A 4D 53 44 4F 53 2E 2D 2D 2D 0D 0A 53 45  T..MSDOS.---..SE
54 55 50 4C 4F 47 2E 54 58 54 0D 0A 3C 57 49 4E  TUPLOG.TXT..<WIN
44 4F 57 53 3E 0D 0A 4E 45 54 4C 4F 47 2E 54 58  DOWS>..NETLOG.TX
54 0D 0A 56 49 44 45 4F 52 4F 4D 2E 42 49 4E 0D  T..VIDEOROM.BIN.
0A 4D 53 44 4F 53 2E 53 59 53 0D 0A 53 55 48 44  .MSDOS.SYS..SUHD
4C 4F 47 2E 2D 2D 2D 0D 0A 44 45 54 4C 4F 47 2E  LOG.---..DETLOG.
54 58 54 0D 0A 4D 53 44 4F 53 2E 42 41 4B 0D 0A  TXT..MSDOS.BAK..
42 4F 4F 54 4C 4F 47 2E 54 58 54 0D 0A 53 59 53  BOOTLOG.TXT..SYS
```

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

```
54 45 4D 2E 31 53 54 0D 0A 49 4F 2E 53 59 53 0D  TEM.1ST..IO.SYS.
0A 3C 4D 79 20 44 6F 63 75 6D 65 6E 74 73 3E 0D  .<My Documents>.
0A 3C 50 72 6F 67 72 61 6D 20 46 69 6C 65 73 3E  .<Program Files>
0D 0A 53 43 41 4E 44 49 53 4B 2E 4C 4F 47 0D 0A  ..SCANDISK.LOG..
```

SubSeven's Signature:

SubSeven leaves several clues for a watchful system administrator to find. First, if the attacker configures the server to notify in some manner, the system administrator will see the infected system connecting to the Internet. If the network has a central mail server and does not support ICQ or IRC services, traffic from machines on the network to these ports should be an immediate alert of illegitimate network communication. Next, the server start-up configuration places several commands on the infected system. Following are SubSeven additions to the infected system (An evaluation copy of RegSnap v2.71 was used to copy and compare registry keys. It is available at http://soft4you.com):

- Registry-Run start-up – The following keys were added to the registry (the program uses encryption to hide key names and values):

```
HKEY_LOCAL_MACHINE\Hardware\Data\ ðÑÐ  ÿ®-¡œ
 Value: String: ""
HKEY_LOCAL_MACHINE\Hardware\Data\ ðÑÐ  ÿ®-¡œw ž
 Value: String: ""
HKEY_LOCAL_MACHINE\Hardware\Data\ Ôwj2¶hˆh”Ä
 Value: String: ""
HKEY_LOCAL_MACHINE\Hardware\Data\"@g)
 Value: Non-ASCII string: 5A B5 0A B7 E4 DC AF 2F
HKEY_LOCAL_MACHINE\Hardware\Data\%b[
 Value: String: "¼{Žäþ÷Ô¿"
HKEY_LOCAL_MACHINE\Hardware\Data\%sI
 Value: Non-ASCII string: 0A 40 66 3F 4F
HKEY_LOCAL_MACHINE\Hardware\Data\)*~Q~ó¤ÜÇ ²„
 Value: Non-ASCII string: 1F 54 68 7B 48 01 DE
HKEY_LOCAL_MACHINE\Hardware\Data\)ln#C
 Value: Non-ASCII string: 0A 40 66 3F 4F
HKEY_LOCAL_MACHINE\Hardware\Data\)Ok.FÎ
 Value: Non-ASCII string: 0A 40 66 3F 4F
HKEY_LOCAL_MACHINE\Hardware\Data\/nFç >5ìª
 Value: String: ""
HKEY_LOCAL_MACHINE\Hardware\Data\<Se8OÞ
 Value: Non-ASCII string: 0A 40 66 3F 4F
HKEY_LOCAL_MACHINE\Hardware\Data\dr¶PM)::
 Value: String: ""
HKEY_LOCAL_MACHINE\Hardware\Data\g>V³PD1öÙÏ#
 Value: Non-ASCII string: 5E 16 39 7B 1E
HKEY_LOCAL_MACHINE\Hardware\Data\I‟ °=Õš Ç
 Value: Non-ASCII string: 5D 11 3A 7C 1A
HKEY_LOCAL_MACHINE\Hardware\Data\V fKèk ÇOú
 Value: Non-ASCII string:1F D1 93 3E 53 10 F8 8B CE C3 6B DE F3 FC CE
```

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

```
  HKEY_LOCAL_MACHINE\Hardware\Data\ZbcÔª ‰
   Value: Non-ASCII string: 1F 4B 64 3C 42
  HKEY_LOCAL_MACHINE\Hardware\Data\Š†ÃqáÆ”M©j€
   Value: String: ""
  HKEY_LOCAL_MACHINE\Hardware\Data\Œ'‘*§¡3A
   Value: Non-ASCII string: 5A 17 3C 7B
  HKEY_LOCAL_MACHINE\Hardware\Data\žü ¨"W…`î
   Value: String: ","
  HKEY_LOCAL_MACHINE\Hardware\Data\½1/B: Íe+°oùÃ
   Value: Non-ASCII string: 02 4E
  HKEY_LOCAL_MACHINE\Hardware\Data\ß$ $®5°ç¶gsMnÐ
   Value: String: "ý•ÝMÛ.¼§–"
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run\WinLoa
der
   Value: String: "sjnphmvxpiy.exe"

New file (windows directory):
    sjnphmvxpiy.exe Size: 382 371
```

- Registry-RunServices start-up – The following keys were added to the registry:

```
  HKEY_LOCAL_MACHINE\Hardware\Data\ ðÑÐ  ÿ®-¡œ
   Value: String: ""
  HKEY_LOCAL_MACHINE\Hardware\Data\ ðÑÐ  ÿ®-¡œw ž
   Value: String: ""
  HKEY_LOCAL_MACHINE\Hardware\Data\ Ôwj2¶hˆh”Ä
   Value: String: ""
  HKEY_LOCAL_MACHINE\Hardware\Data\"@g)
   Value: Non-ASCII string: 5A B5 0A B7 E4 DC AF 2F
  HKEY_LOCAL_MACHINE\Hardware\Data\%b[
   Value: String: "¼{Žäþ÷Ô¿"
  HKEY_LOCAL_MACHINE\Hardware\Data\%sI
   Value: Non-ASCII string: 0A 40 66 3F 4F
  HKEY_LOCAL_MACHINE\Hardware\Data\)*~Q~ó¤ÜÇ ²„
   Value: Non-ASCII string: 1F 54 68 7B 48 01 DE
  HKEY_LOCAL_MACHINE\Hardware\Data\)ln#C
   Value: Non-ASCII string: 0A 40 66 3F 4F
  HKEY_LOCAL_MACHINE\Hardware\Data\)Ok.FÎ
   Value: Non-ASCII string: 0A 40 66 3F 4F
  HKEY_LOCAL_MACHINE\Hardware\Data\/nFç >5ìª
   Value: String: ""
  HKEY_LOCAL_MACHINE\Hardware\Data\<Se8OÞ
   Value: Non-ASCII string: 0A 40 66 3F 4F
  HKEY_LOCAL_MACHINE\Hardware\Data\dr¶PM)::
   Value: String: ""
  HKEY_LOCAL_MACHINE\Hardware\Data\g>V³PD1öÙÏ#
   Value: Non-ASCII string: 5E 16 39 7B 1E
  HKEY_LOCAL_MACHINE\Hardware\Data\I‟ °=Õš Ç
   Value: Non-ASCII string: 5C 10 3A 7C 1A
  HKEY_LOCAL_MACHINE\Hardware\Data\V fKèk ÇOú
   Value: Non-ASCII string: BD 89 0C 8C 84 35 72 E0 0F 4F 2C B9 FB
  HKEY_LOCAL_MACHINE\Hardware\Data\ZbcÔª ‰
   Value: Non-ASCII string: 1E 47 68 25
  HKEY_LOCAL_MACHINE\Hardware\Data\Š†ÃqáÆ”M©j€
   Value: String: ""
```

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

```
  HKEY_LOCAL_MACHINE\Hardware\Data\Œ'‘*§¡3A
   Value: Non-ASCII string: 5A 17 3C 7B
  HKEY_LOCAL_MACHINE\Hardware\Data\žü ¨"W…`î
   Value: String: ","
  HKEY_LOCAL_MACHINE\Hardware\Data\½1/B: Íe+°oùÃ
   Value: Non-ASCII string: 02 4E
  HKEY_LOCAL_MACHINE\Hardware\Data\ß$ $®5°ç¶gsMnÐ
   Value: String: "ý•ÝMÛ.¼§-"
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices\WinLoader
   Value: String: "wsukvbgpy.exe"
```

New file (windows directory):

```
    wsukvbgpy.exe Size: 382 371
```

- Win.ini start-up - Adds the following keys to the registry and the following line to the [windows] block in the Win.ini file: **run=server.com**. Note: the attacker can rename the file name.

New keys:

```
  HKEY_LOCAL_MACHINE\Hardware\Data\ ðÑÐ  ÿ®-¡œ
   Value: String: ""
  HKEY_LOCAL_MACHINE\Hardware\Data\ ðÑÐ  ÿ®-¡œw ž
   Value: String: ""
  HKEY_LOCAL_MACHINE\Hardware\Data\ Ôwj2¶hˆh”Ä
   Value: String: ""
  HKEY_LOCAL_MACHINE\Hardware\Data\"@g)
   Value: Non-ASCII string: 5A B5 0A B7 E4 DC AF 2F
  HKEY_LOCAL_MACHINE\Hardware\Data\%b[
   Value: String: "¼{Žäþ÷Ô¿"
  HKEY_LOCAL_MACHINE\Hardware\Data\%sI
   Value: Non-ASCII string: 0A 40 66 3F 4F
  HKEY_LOCAL_MACHINE\Hardware\Data\)*~Q~ó¤ÜÇ ²„
   Value: Non-ASCII string: 1F 54 68 7B 48 01 DE
  HKEY_LOCAL_MACHINE\Hardware\Data\)ln#C
   Value: Non-ASCII string: 0A 40 66 3F 4F
  HKEY_LOCAL_MACHINE\Hardware\Data\)Ok.FÎ
   Value: Non-ASCII string: 0A 40 66 3F 4F
  HKEY_LOCAL_MACHINE\Hardware\Data\/nFç >5ìª
   Value: String: ""
  HKEY_LOCAL_MACHINE\Hardware\Data\<Se8OÞ
   Value: Non-ASCII string: 0A 40 66 3F 4F
  HKEY_LOCAL_MACHINE\Hardware\Data\dr¶PM)::
   Value: String: ""
  HKEY_LOCAL_MACHINE\Hardware\Data\g>V³PD1öÙÏ#
   Value: Non-ASCII string: 5E 16 39 7B 1E
  HKEY_LOCAL_MACHINE\Hardware\Data\I‟ °=Õš Ç
   Value: Non-ASCII string: 5C 11 3B 7C 1A
  HKEY_LOCAL_MACHINE\Hardware\Data\V fKèk ÇOú
   Value: Non-ASCII string:4C AB 30 38 C9 9F 02 D3 90 F9 F8 43 49 6B F7
  HKEY_LOCAL_MACHINE\Hardware\Data\ZbcÔª ‰
   Value: Non-ASCII string: 09 4B 73 3B 5E 1C
  HKEY_LOCAL_MACHINE\Hardware\Data\Š†ÃqáÆ”M©j€
   Value: String: ""
```

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

```
HKEY_LOCAL_MACHINE\Hardware\Data\Œ'‘*§¡3A
 Value: Non-ASCII string: 5A 17 3C 7B
HKEY_LOCAL_MACHINE\Hardware\Data\žü ¨"W…`î
 Value: String: ","
HKEY_LOCAL_MACHINE\Hardware\Data\½1/B: Íe+°oùÃ
 Value: Non-ASCII string: 02 4E
HKEY_LOCAL_MACHINE\Hardware\Data\ß$ $®5°ç¶gsMnÐ
 Value: String: "ý•ÝMÛ.¼§-"
```

New file(windows directory)

```
ejywtrgoeou.exe Size: 382 371
```

- Less known method start-up – Adds the following keys to the registry and changes the following line to the [boot] block in the System.ini file: **shell=Explorer.exe** to **shell=Explorer.exe server.com**. Again, the attacker can change the file name.

```
HKEY_LOCAL_MACHINE\Hardware\Data\ ðÑÐ  ÿ®-¡œ
 Value: String: ""
HKEY_LOCAL_MACHINE\Hardware\Data\ ðÑÐ  ÿ®-¡œw ž
 Value: String: ""
HKEY_LOCAL_MACHINE\Hardware\Data\ Ôwj2¶hˆh”Ä
 Value: String: ""
HKEY_LOCAL_MACHINE\Hardware\Data\"@g)
 Value: Non-ASCII string: 5A B5 0A B7 E4 DC AF 2F
HKEY_LOCAL_MACHINE\Hardware\Data\%b[
 Value: String: "¼{Žäþ÷Ô¿"
HKEY_LOCAL_MACHINE\Hardware\Data\%sI
 Value: Non-ASCII string: 0A 40 66 3F 4F
HKEY_LOCAL_MACHINE\Hardware\Data\)*~Q~ó¤ÜÇ ²„
 Value: Non-ASCII string: 1F 54 68 7B 48 01 DE
HKEY_LOCAL_MACHINE\Hardware\Data\)ln#C
 Value: Non-ASCII string: 0A 40 66 3F 4F
HKEY_LOCAL_MACHINE\Hardware\Data\)Ok.FÎ
 Value: Non-ASCII string: 0A 40 66 3F 4F
HKEY_LOCAL_MACHINE\Hardware\Data\/nFç >5ìª
 Value: String: ""
HKEY_LOCAL_MACHINE\Hardware\Data\<Se8OÞ
 Value: Non-ASCII string: 0A 40 66 3F 4F
HKEY_LOCAL_MACHINE\Hardware\Data\dr¶PM)::
 Value: String: ""
HKEY_LOCAL_MACHINE\Hardware\Data\g>V³PD1öÙÏ#
 Value: Non-ASCII string: 5E 16 39 7B 1E
HKEY_LOCAL_MACHINE\Hardware\Data\I‟ °=Õš Ç
 Value: Non-ASCII string: 5C 11 3A 7D 1A
HKEY_LOCAL_MACHINE\Hardware\Data\V fKèk ÇOú
 Value: Non-ASCII string: 87 B6 78 19 E7 DB 54 8F E5 93 D5 19 E1 BB
        A3 20 FA
HKEY_LOCAL_MACHINE\Hardware\Data\ZbcÔª ‰
 Value: Non-ASCII string: 1B 55 61 28 45
HKEY_LOCAL_MACHINE\Hardware\Data\Š†ÃqáÆ”M©j€
 Value: String: ""
HKEY_LOCAL_MACHINE\Hardware\Data\Œ'‘*§¡3A
 Value: Non-ASCII string: 5A 17 3C 7B
```

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

```
  HKEY_LOCAL_MACHINE\Hardware\Data\žü ¨"W…`î
   Value: String: ","
  HKEY_LOCAL_MACHINE\Hardware\Data\½1/B: Íe+°oùÃ
   Value: Non-ASCII string: 02 4E
  HKEY_LOCAL_MACHINE\Hardware\Data\ß$ $®5°ç¶gsMnÐ
   Value: String: "ý•ÝMÛ.¼§-"
New file(windows directory)
  wtkdoncrgdbvl.exe Size: 382 371
```

- _not_known method start-up – Modified and added the following registry keys:

```
Modified key
  HKEY_LOCAL_MACHINE\Software\CLASSES\exefile\shell\open\command\@
   Old value: String: ""%1" %*"
   New value: String: "umapwsoap.exe "%1" %*"

New keys
  HKEY_LOCAL_MACHINE\Hardware\Data\ ðÑÐ  ÿ®-¡œ
   Value: String: ""
  HKEY_LOCAL_MACHINE\Hardware\Data\ ðÑÐ  ÿ®-¡œw ž
   Value: String: ""
  HKEY_LOCAL_MACHINE\Hardware\Data\ Ôwj2¶hˆh”Ä
   Value: String: ""
  HKEY_LOCAL_MACHINE\Hardware\Data\"@g)
   Value: Non-ASCII string: 5A B5 0A B7 E4 DC AF 2F
  HKEY_LOCAL_MACHINE\Hardware\Data\%b[
   Value: String: "¼{Žäþ÷Ô¿"
  HKEY_LOCAL_MACHINE\Hardware\Data\%sI
   Value: Non-ASCII string: 0A 40 66 3F 4F
  HKEY_LOCAL_MACHINE\Hardware\Data\)*~Q~ó¤ÜÇ ²„
   Value: Non-ASCII string: 1F 54 68 7B 48 01 DE
  HKEY_LOCAL_MACHINE\Hardware\Data\)ln#C
   Value: Non-ASCII string: 0A 40 66 3F 4F
  HKEY_LOCAL_MACHINE\Hardware\Data\)Ok.FÎ
   Value: Non-ASCII string: 0A 40 66 3F 4F
  HKEY_LOCAL_MACHINE\Hardware\Data\/nFç >5ìª
   Value: String: ""
  HKEY_LOCAL_MACHINE\Hardware\Data\<Se8OÞ
   Value: Non-ASCII string: 0A 40 66 3F 4F
  HKEY_LOCAL_MACHINE\Hardware\Data\dr¶PM)::
   Value: String: ""
  HKEY_LOCAL_MACHINE\Hardware\Data\g>V³PD1öÙÏ#
   Value: Non-ASCII string: 5E 16 39 7B 1E
  HKEY_LOCAL_MACHINE\Hardware\Data\I" °=Õš Ç
   Value: Non-ASCII string: 5C 11 3B 7C 1B
  HKEY_LOCAL_MACHINE\Hardware\Data\V fKèk ÇOú
   Value: Non-ASCII string: FC 01 1D FF C3 72 73 AD 0F 99 66 65 A5 8C
  HKEY_LOCAL_MACHINE\Hardware\Data\ZbcÔª ‰
   Value: Non-ASCII string: 0D 40 7E 3E 48
  HKEY_LOCAL_MACHINE\Hardware\Data\Š†ÃqáÆ”M©j€
   Value: String: ""
  HKEY_LOCAL_MACHINE\Hardware\Data\Œ'‘*§¡3A
   Value: Non-ASCII string: 5A 17 3C 7B
  HKEY_LOCAL_MACHINE\Hardware\Data\žü ¨"W…`î
   Value: String: ","
```

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

```
HKEY_LOCAL_MACHINE\Hardware\Data\½1/B: Íe+°oùÃ
 Value: Non-ASCII string: 02 4E
HKEY_LOCAL_MACHINE\Hardware\Data\ß$ $®5°ç¶gsMnÐ
 Value: String: "ý•ÝMÛ.¼§-"
```

New files (windows directory):

```
aatrbdxugj.exe Size: 382 371
umapwsoap.exe Size: 10 769
```

SubSeven Countermeasures:

The first, and possibly the most preventive countermeasure, is a statefull firewall. With rules to allow only inbound traffic initiated by the legitimate network, the attacker will not be able to establish a connection to an infected system.

Anti-viral software companies regularly publish new virus definitions. In order to find compromised systems or infected files, establish a procedure for downloading and updating existing anti-viral software weekly (new versions of SubSeven exist every couple of weeks that current virus definitions will not identify).

If possible, acquire a tool such as RegSnap, that allows the system administrator to take a system "snap shot" prior to installing the system on the network. Then, regularly, take new "snap shots" and compare them to the initial "snap shot" in order to find illegitimate additions or modifications to the registry. Some of these programs also include changes to system files which may indicate illegitimate modifications.

The operating system itself can tell if something is amiss. Running **netstat –na** will display all listening ports and established connections. The following netstat output line gives SubSeven away:

Proto	Local Address	Foreign Address	State
TCP	0.0.0.0:27374	0.0.0.0:0	LISTENING

Note: The listening port is configurable by the attacker, but it will still be listening at IP 0.0.0.0. Another place to check is the process list. The attacker can configure the process name, but the system administrator should be familiar with legitimate processes and be able to identify the illegitimate process.

Finally, monitor network traffic to ensure legitimate network communications. If specific systems on the network, other than actual mail servers, are connecting to remote mail servers, the system may be infected. The same procedure applies to ICQ and IRC. These services are used by SubSeven to notify the attacker of system startup and IP address changes.

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