Global Information Assurance Certification Paper

Advanced Incident Handling Practical Assignment
Option 2 – Investigation of the SubSeven Trojan (version 2.2)

Tony Samsom

Version 1.5 - April 26, 2001

Introduction

The FBI made the news late last year (1) by using a Trojan to obtain access to an alleged mobster's encrypted files. The article didn't divulge which Trojan software was used. Even so, the FBI succeeded in outlining how serious a security threat this form of malicious code can be. It appears that someone interested in computer security should become familiar with this form of exploit.

Very recently, "mobman", the author of the SubSeven Trojan, released a new version, SubSeven 2.2 beta, which is now capable of infecting Windows 2000. This paper describes my experience with the SubSeven version 2.2 beta exploit on Windows 2000.

Exploit Details

Name

SubSeven v2.2 Beta,

Variants

BackDoor-G2, BackDoor-G2.svr.gen, BackDoor-G22.svr, BackDoor.PolyDrop, Backdoor.Subseven.22.a (NAV), BackDoor/SubSeven2.2 (CAI), Badman Trojan, Serbian Badman Trojan, Sub7 v2.x, SubSeven v2.0, SubSeven v2.1, SubSeven v2.1 Gold, SubSeven v2.12, SubSeven v2.13, SubSeven v2.2 Beta , Troj_Sub7.22.d (Trend), TROJ_SUB7.MUIE , Troj_Sub7.v20 (Trend), TSB Trojan,WIN32.SubSeven.

According to the FAQ on http://subseven.slak.org, SubSeven is written in Delphi and the source code is not public domain. As a result, all direct variants should be versions of SubSeven. Copies of the current version and previous version can be downloaded from the SubSeven web site. Note that the name of the Trojan can be customized before being sent. A victim receiving a "properly configured" SubSeven Trojan will not, in general, see any of the above names.

Operating Systems:

Windows 95, Windows 98, Windows NT, Windows 2000

Protocols/Services

SubSeven uses the standard TCP/IP protocol. Default port is 27374 for version 2.2. However, SubSeven can be configured to run on any TCP port so finding infected systems in a large organization is not as simple as looking for TCP conversations on a defined port.

SubSeven has multiple methods of installation notification including email, CGI scripts on Web Server (HTTP), ICQ, IRC (Instant Messaging), and TCP/IP packets directed to a monitor provided with the SubSeven package.

Brief Description:

The SubSeven package comes with several programs: client, server, server configuration utility, and monitor. The SubSeven server is the Trojan. The client is used to control the server. The server configuration utility is used to configure server options. The monitor listens for notices from servers running on infected systems (one method of capture). Note that the infected servers must be configured to send these notices.

SubSeven has many features. Some of these features include: Screen Capture, Keyboard Logger, File Manger, FTP Server, Network Sniffer, Registry Editor, Password grabber (for Screen Saver, Cached Passwords, RAS Passwords, ICQ, etc.), Network Browser, Process Manager, ICQ Spy, Clipboard Manager, Web Cam, and Print Manager. Some "entertainment features" include the ability to flip the screen over and hide the mouse. There appears to be few things that you can do with direct access to the machine that you can't do with SubSeven and there are a few things that SubSeven can do, like keyboard logging, that are hard to do directly.

Protocol Description:

For control, the SubSeven server and client communicate over a predefined or random TCP port. Commands are issued from the client; the server processes the commands, and returns the results over this port.

For infection notification, the SubSeven Trojan can use any of the following network/application protocols:

- The Trojan can send an email to a pre-configured account
- The Trojan can use IRC, or ICQ chat
- The Trojan can send a TCP packet to a predefined address (default TCP port 27374)

- The Trojan can use the HTTP protocol (CGI script)

At the OS level, the SubSeven server itself uses various Windows API calls and a Windows device driver to provide the long list of functionality described above. Some of the OS services it uses include:

- Windows 2000 startup registry settings to restart the trojan on reboot
- Reset date and time API's to hide system file change activity
- API's to get access to keyboard messages, clipboard info, files, and screen shots.
- Drivers to get at the network stack to provide the network sniffing capability.

There appears to be no special operating system vulnerability that is exploited by SubSeven. Windows 2000 has a file system that has the ability to prevent unauthorized tampering of the registry, system files, and system directories but by default, these protections are not generally employed as they act as impediments to installing and configuring legitimate programs.

Description of Variants:

As the source code is not freely distributed, all direct variants should be modifications and improvements directly attributable to the original author of SubSeven. However, the SubSeven trojan idea is a common one and has many "competitors". These include: Back Orifice 2000, NetBus, NetSpy, etc.

Most of the Trojans have very similar capability. Back Orifice 2000 is arguably the most popular and most capable of the multipurpose Trojans. It is educational to compare SubSeven features to Back Orifice 2000 (BO2K).

Overall Structure

Both BO2K and SubSeven are client/server Trojans. The server or code that runs on the victim comes with a base executable and a set of plugins that add functionality. The base server executable for both are small, 70 to 100K bytes, and the plugins for both can add considerable size to the executable.

Similarities

Both Trojans give complete access to the victim's system and are trivial to install. With plugins, both systems allow screen snapshots, keyboard logging, access to the file system, and access to the registry. Both systems include similar nuisance features: hide the mouse, open the CD tray, etc. etc.

Differences

SubSeven authors do not claim that there is any legitimate use for SubSeven. BO2K authors justify it's existence based on BO2K's ability to do remote administration. BO2K is open source. SubSeven source code is carefully controlled by the SubSeven author. As a result, the BO2K development team is bigger and the results show.

Functionality features that BO2K has that SubSeven is lacking include easy to use remote shell capability and effective over the shoulder ability.

Network stealth features that BO2K has that SubSeven is lacking include the ability to use UDP protocol as well as TCP for network connectivity. SubSeven only uses TCP ports. Also, according to (9), an ICMP protocol plugin exists as well. SubSeven does attempt to hide the TCP port it is using somewhat by naming it in the "services" configuration file.

BO2K comes with simple and strong encryption plugins. Properly used, these tools can make BO2K invisible to high-end intrusion detection systems. SubSeven network conversations are not encrypted at present.

BO2K has the ability to remove itself from the process list. SubSeven cannot do this just yet.

SubSeven comes with a considerable number of password capturing features including tools to get ICQ, IRC, and the encrypted Windows 2000 passwords if the Windows 2000 system is still using the NT style password system (Not active directory and Kerberos). The password information is presented in a form ready for input into l0phtcrack, a very capable Windows NT password cracker.

How the Exploit Works:

The SubSeven Trojan is distributed manually. It does not appear to self-replicate so infection is accomplished through social engineering methods. Typically, an email is sent to the victim with some scheme to get him to run an attached executable although any other method of distributing executables can be used like a Web Server or FTP Server. Usually some form of social engineering is used to coerce the victim into running the SubSeven executable. For example, this description of an attempt to coerce people into installing SubSeven was taken from the description of SubSeven on (2).

> An email with an attachment called "server.exe" was spammed to Japanese computer users. The attachment claimed to be an antivirus program for a virus called Pinkworm, but it was actually a trojan called SubSeven 2.0 Server. The email was sent from a Japanese Hotmail account claiming to be from Microsoft

> Japan Service. The email requests the recipient to run the attachment called "server.exe" which will protect the computer from the Pinkworm virus. Please note that there is no virus called Pinkworm.

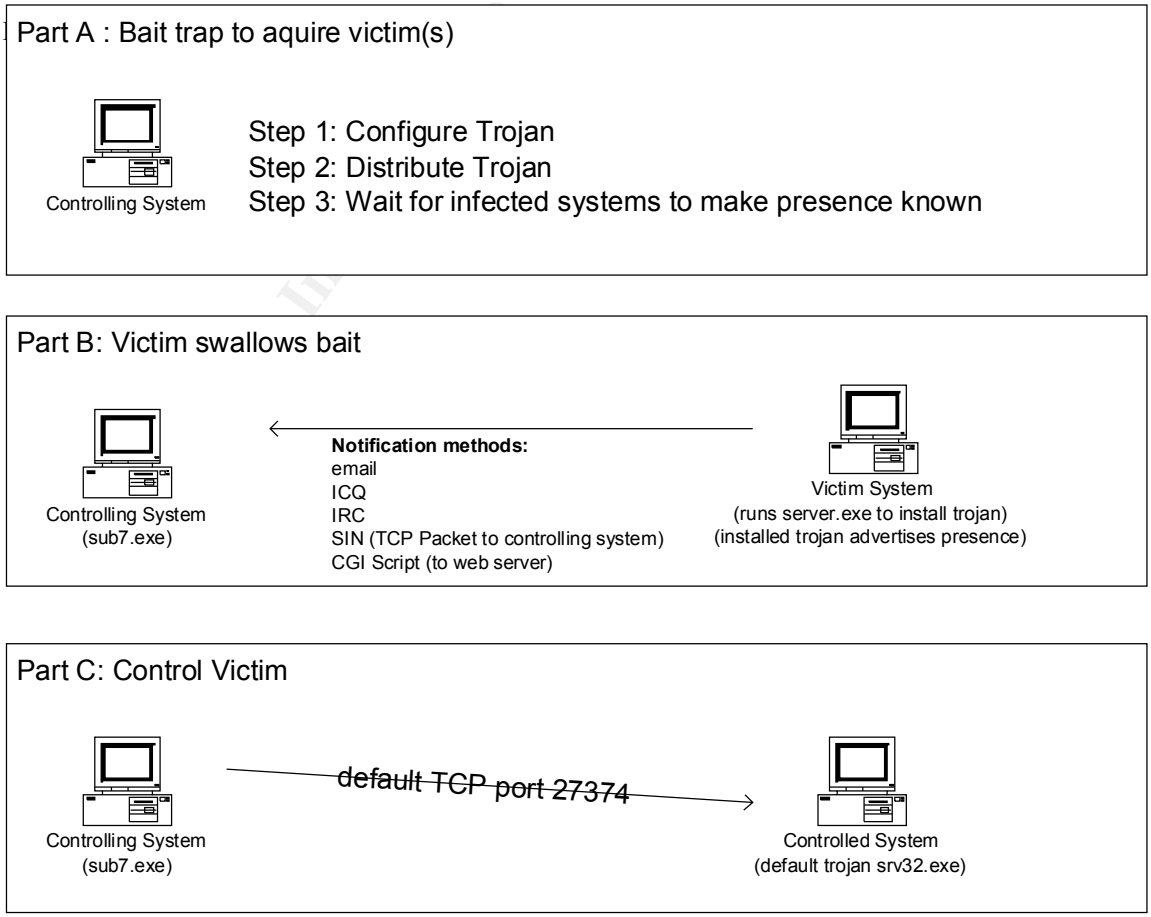
There are numerous other examples of social engineering attacks that can be adapted to distribute this trojan. Examples include: run this program to view pictures of my naked wife, run this cute game, and on and on.

The above examples concentrated on files with an .exe extension delivered through email. Other obviously dangerous file types include: .com and .vbs. However, exploits continue to be found that coerce various applications to run arbitrary code. Examples of this include buffer overflow exploits for Adobe Acrobat, and Winamp. It is wise to treat all mail attachments with suspicion.

There are other delivery mechanisms to consider as well. Executing ActiveX controls or downloading and executing code from an un-trusted website can be just as dangerous.

Diagram:

The following diagram illustrates the typical stages involved in the distribution of the SubSeven Trojan:



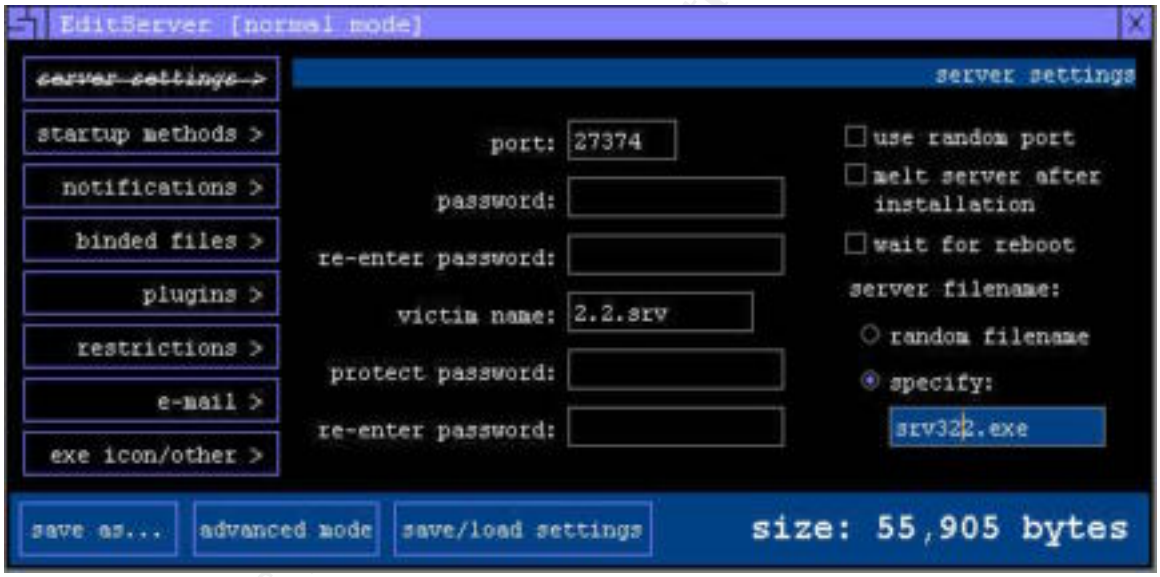
How to Use the Exploit

A brief description of the SubSeven Trojan and support programs follows:

EditServer

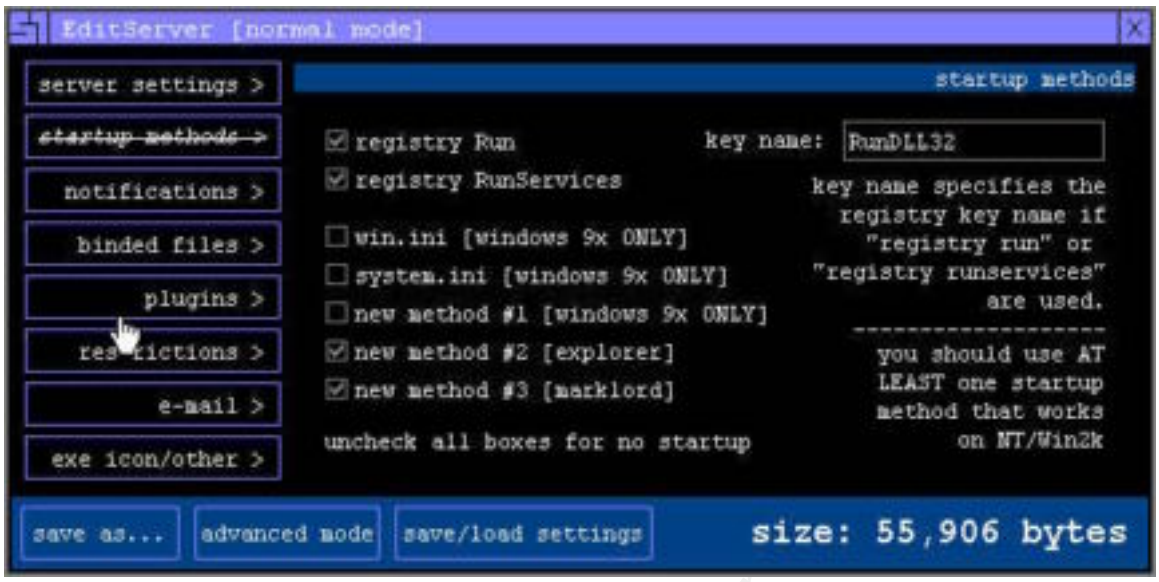
The EditServer program that comes with the SubSeven package is used to configure the SubSeven server. Options are broken into server settings, startup methods, notifications, etc. Server Settings allow choice of server TCP port, passwords etc. Note that the server filename displayed below is the name of the server when running on the victims system, not the executable to be sent.

Server Settings:



Startup Methods:

The Startup Methods screen allows configuration of how SubSeven restarts itself when the victim reboots his/her system:



Notifications: Notifications allow configuration of the many methods this Trojan lets the originator know the victim has been infected.

Binded Files: Binded files allow addition of other executables to the server. An example would be building a zip.exe that not only unloads a series of files but also installs SubSeven.

Plugins: The base server (exe to send to victim) is about 55KB in length. Functionality like keyboard logging, packet sniffing etc. is provided through plugins or dll's. This utility allows you to bind these dll's to the base server (which can make it quite large).

The restrictions screen allows the server to be configured with restricted functionality.

e-mail: This configures the server to send back logged keys etc.

exe icon/other: This allows configuration of the server icon, allows for the display of a message when the server is installed (so the victim knows they are infected?) etc.

Additional Server Configuration

One of the main defenses to overcome in distributing SubSeven is Anti Virus Software. The SubSeven authors suggest you pack an unpacked version of SubSeven with one of the many exe packers available at http://protools.cjb.net.

Sin

Sin (sin.exe) listens on a TCP port waiting for a server to notify it that it is up and working.

Sub7

This is the client (the system that controls the server).

Server

This is the installation program. Server.exe (not usually it's real name) includes the Trojan as payload. When run, server.exe installs the Trojan.

Srv32

This is the Trojan. Generally, a random set of characters is used as the Trojan's executable name. The name "srv32" is not typical. The Trojan I configured included the keyboard logger and advanced system information plugins. Note that some of the advertised functionality is not quite working in this Windows 2000 beta version.

Using SubSeven Capabilities

Once the Server has installed Srv32, the various SubSeven features can be used to compromise a machine and it's neighbors. The keyboard logger, password grabbers, file readers, ftp etc. are very capable of getting at most if not all available information on the infected machine. As demonstrated by the FBI, a keyboard logger is effective in circumventing strong encryption software like PGP (by allowing access to the PGP passphrase). Here is an example of the keyboard logger recording keystrokes as a password gets changed through the Windows 2000 administration interface:

```
[»Set Password«]
pass111`«««««««««««hong111[Tab]pass111
[»Set Password«]
pass2111[Tab]pass2111
[»Command Prompt«]
netstat -na
[Ctrl][Alt]ipconfig
[»Command Prompt«]
ipconfig
```

If the target machine is a member of a corporate network, built in tools like the SubSeven IP scanner and Packet Sniffer can be used to gather substantial information about a compromised machine's neighbors. If the built in tools do not provide enough information, it is possible to use SubSeven to install and use other hacking tools like Nmap or Nessus. SubSeven can be used to pull all

relevant information back to the client where other hacking tools like l0phtcrack can be used. SubSeven over the shoulder capability is limited but available so it is possible to use the compromised machine to gain access to other systems in a corporate network that may not be directly accessible otherwise (for example MVS systems without IP access).

Signature of the Attack

In order to understand how SubSeven infects a Windows 2000 system I built a Windows 2000 system, performed a baseline audit, infected the system with SubSeven, and used the baseline to find some of the changes the Trojan made to the system. I also took a look at the network traffic of a quick SubSeven Client/Server conversation.

Baseline Audit

The audit tools I used to build a baseline of the system came from the base Windows 2000 system or the Windows 2000 Resource Kit and included:

netstat – A tool that shows connected and listening TCP and UDP ports.

rpcdump – Windows 2000 services and programs use dce_rpc more heavily than Windows NT. This utility lists the GUID numbers of the programs available through rpc calls.

sysdiff – An automated system installation tool that flags changes in ini files, the registry, and files on the system.

regdmp – Registry Dump utility

dir e:\winnt /s /t:c – directory listing of the winnt system

secpol.msc – This is the utility that allows configuration of what gets recorded in the security event log. The equivalent in Windows NT is the User Manager.

addusers - Dump of local users and groups (this system was not part of a domain)

tskmgr – The Windows 2000 task manager was sufficient to find (and kill) the SubSeven virus.

fc – file compare

Note that I am still looking for a good acl dump utility as I couldn't get xcacls.exe to just list acls and the other acl tools in the Windows 2000 resource kit either don't list file acls or are way to slow to be useful.

Netstat – Before and After

(netstat –a)

```
Comparing files netstat.before and NETSTAT.AFTER
***** netstat.before
  TCP    hef3:1025              hef3:0                 LISTENING
  TCP    hef3:netbios-ssn       hef3:0                 LISTENING
***** NETSTAT.AFTER
  TCP    hef3:1025              hef3:0                 LISTENING
  TCP    hef3:1553              hef3:0                 LISTENING
  TCP    hef3:netbios-ssn       hef3:0                 LISTENING
*****
```

The additional line (TCP hef3:1553) is our newly installed Trojan. A better look can be had with an additional switch i.e. (netstat –na) so we can now see something listening on port 27374 in this case. Note that the sysdiff results described below shows that \system32\drivers\etc\services has been changed. (Port 27374 gets a name of 1553)

```
Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1025           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:27374          0.0.0.0:0              LISTENING
  TCP    24.67.73.247:139       0.0.0.0:0              LISTENING
  UDP    0.0.0.0:135            *:*
  UDP    0.0.0.0:445            *:*
  UDP    0.0.0.0:1026           *:*
  UDP    0.0.0.0:1036           *:*
  UDP    24.67.73.247:137       *:*
  UDP    24.67.73.247:138       *:*
  UDP    24.67.73.247:500       *:*
```

Rpcdump – rpcdump did not show any changes. It appears that the SubSeven Trojan does not use COM+ just yet.

Sysdiff – sysdiff was very useful in revealing some of the Trojan's operation. Some select pieces from the sysdiff output include:

C:\

Add/change EXPLORER.EXE

E:\WINNT\system32

Add/change DIF.tmp
Add/change nmbopd.thj
Add/change pkymwem.ail
Add/change srv322.exe
Add/change vwlvqr.exe

E:\WINNT\system32\drivers\etc

Add/change services

E:\WINNT\system32\NtmsData

Add/change NTMSDATA
Add/change NTMSDATA.BAK
Add/change NTMSIDX

E:\WINNT\Tasks

Add/change SA.DAT

HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

RunDLL32: REG_SZ E:\WINNT\System32\srv322.exe

Sysdiff has provided some decent hints as to where and what was installed complements of SubSeven. Srv322.exe is the Trojan. If this is deleted, several of the changes hinted at above will restore it from some of the randomly named files now living in WINNT\SYSTEM32.

Regdmp – regdmp confirms the additional run key (HKEY_LOCAL_MACHINE\Microsoft\Windows\CurrentVersion\Run) is there and will start the SubSeven Trojan on a reboot. This turns out to be just one of several methods the SubSeven Trojan can restart itself on reboot.

Dir – The directory listing confirms the addition of the files listed above. Note that fc compares on the before and after directory listing do not show changes to explorer.exe.

Secpol.msc – Using secpol, I turned on all the auditing available before installing and exploring the SubSeven Trojan. Looking through the security logs in the event viewer, several items jumped out:

Evidence that explorer.exe is starting the Trojan (process ID chain):

A new process has been created:
New Process ID: 4264757760
Image File Name: \WINNT\explorer.exe

Creator Process ID: 4264762720
User Name: restricteduser
Domain: HEF3
Logon ID: (0x0,0x6222)

A new process has been created:
New Process ID: 4264748704
Image File Name: \WINNT\system32\lmiwplmp.exe
Creator Process ID: 4264757760
User Name: restricteduser
Domain: HEF3
Logon ID: (0x0,0x6222)

A new process has been created:
New Process ID: 4264711200
Image File Name: \WINNT\system32\srv322.exe
Creator Process ID: 4264748704
User Name: restricteduser
Domain: HEF3
Logon ID: (0x0,0x6222)

In (3), there is a description of how registry entry *"HKEY_CLASS_ROOT\exefiles\shell\open\command"* is modified to start the SubSeven server every time explorer executes a command. The sysdiff output above also shows that explorer was modified.

Another hint that SubSeven may be hiding it's tracks:

Privileged Service Called:
Server: Security
Service: -
Primary User Name: Administrator
Primary Domain: HEF3
Primary Logon ID: (0x0,0x621B)
Client User Name: -
Client Domain: -
Client Logon ID: -
Privileges: SeSystemtimePrivilege

Addusers – addusers showed no changes

Taskmgr – Control Alt Delete on Windows 2000 allows access to the task manager. It shows the active processes including our Trojan "srv322.exe". However, on a typical Windows 2000 box there are 20 or more processes running. It is unlikely our Trojan would be discovered by casual observation.

Network Signature

A look at the packets moving between SubSeven client and server shows a typical unencrypted TCP conversation. Here are the first few packets of the start of conversation complements of Windump.exe. This particular setup included setting the TCP port on 13169 and setting a password on the SubSeven Server.

```
21:27:27.569261 IS~HEF2.1058 > hef3.13169: S 3808346148:3808346148(0) win 16384
<mss 1460,nop,nop,sackOK> (DF)
0x0000   4500 0030 0870 4000 8006 2de3 1843 49f8        E..0.p@...-..CI.
0x0010   1843 49f7 0422 3371 e2fe c024 0000 0000        .CI.."3q...$....
0x0020   7002 4000 a3f3 0000 0204 05b4 0101 0402        p.@.............
21:27:27.569804 IS~HEF2.1058 > hef3.13169: . ack 879101830 win 17520 (DF)
0x0000   4500 0028 0871 4000 8006 2dea 1843 49f8        E..(.q@...-..CI.
0x0010   1843 49f7 0422 3371 e2fe c025 3466 0786        .CI.."3q...%4f..
0x0020   5010 4470 904b 0000 0000 0000 0000             P.Dp.K........
21:27:27.605306 IS~HEF2.1058 > hef3.13169: P 0:36(36) ack 13 win 17508 (DF)
0x0000   4500 004c 0872 4000 8006 2dc5 1843 49f8        E..L.r@...-..CI.
0x0010   1843 49f7 0422 3371 e2fe c025 3466 0792        .CI.."3q...%4f..
0x0020   5018 4464 ee6e 0000 5061 7373 776f 7264        P.Dd.n..Password
0x0030   2068 6f6e 6731 3131 0d0a 5061 7373 776f        .hong111..Passwo
0x0040   7264 2068 6f6e 6731 0d0a 0d0a                  rd.hong1....
```

How to Protect against it

Current versions of SubSeven are generally caught by the more popular anti virus products with up to date virus signature files. The best first defense is to keep your anti virus software up to date. The newest version SubSeven, or versions specially constructed to avoid current anti virus signatures can get by this one layer of defense. A list of countermeasures that should keep most systems safe include:

- Don't execute code or look at attachments from unknown sources.
- Keep your OS and application software patches up to date.
- For Windows 2000, use a "locked down" system configuration. If there is no write access to system files and directories, or the registry, SubSeven will not install.
- Install virus software and keep the software and signature files up to date.
- Install a personal firewall and configure it to only allow known applications and ports out. If you use a network level firewall with an Intrusion Detection component, keep these signature files up to date.
- For critical systems, a baseline audit and regular follow-up audits should expose variants of SubSeven or other malicious code that evades current firewall, intrusion detection, or virus scanning software.
- At my current contract, Internet access is only allowed after authentication on the Firewall, and high TCP ports are not generally open. This policy will catch SubSeven Trojans on internal systems just as long as the

client/server conversation attempted to go through the firewall. (The firewall logs are scanned regularly for this kind of activity)

There are two major classes of personal firewalls; application level, and network level firewalls. Application level firewalls like ZoneAlarm by ZoneLabs need to be configured to allow srv32.exe access to the network. Network level firewalls like LockDown 2000 scan the network traffic and watch for signatures of viruses (like an Intrusion Detection System), Other network level firewalls allow the user to restrict which TCP and UDP ports are available for use. Both types of firewalls can be effective in at least identifying that SubSeven is present. An interesting note in the SubSeven "faq" discusses the effectiveness, or lack thereof, of some of the above defenses. Apparently, several "victims" have said yes when their application level firewall software asked if it was OK to let SubSeven have access to the Internet. User education is one major component of keeping systems safe.

I don't believe that it is possible for Microsoft for help in preventing SubSeven or it's equivalent from being capable of being written. The Windows 2000 capabilities that SubSeven uses are also used by legitimate software vendors. For example: "SnagIt" by TechSmith corp., "PC-Anywhere" by Symantec, or any Anti Virus software. I doubt that Microsoft could provide the capability to write these products without also providing the hooks needed to write SubSeven or it's equivalent.

Audit Lessons Learned

It was very useful for me to gain some practical experience with system auditing while trying to get a handle on what SubSeven was doing to my system. Because I chose to work with Windows 2000 instead of Windows NT, the audit recommendations in (6) were not directly applicable and I had to look for comparable tools on the new OS. Going through the audit emphasized several key points about systems auditing. Lessons learned included:

- Choosing what tools to use to collect and analyze system information is both important and difficult to get right without trial and error.
- Having a sound understanding of what data can be collected and what to collect is important and again, practice will help get this part right.
- A basic understanding of how systems work is essential, as much of the information collected is not relevant and skill is required in finding the "relevant bits" when analyzing an incident.
- Audit procedures are good at flagging that malicious code is present. Audit procedures are, in general, not good at undoing the damage. Due to limitations on what information can be collected, complete information on what malicious code has done is unlikely to exist after the fact.

When I checked the anti virus centers (2,3,4) for a description of the SubSeven virus, I found descriptions of the addition of registry keys and other system changes that I did not see with my audit. Possibly differences between Windows 95,98, NT and the Windows 2000 audit I performed could explain this. More likely, I missed a few details in the massive amount of information I collected Even though my audit methods were incomplete and arguably flawed; they did flag the presence of the malicious code.

Conclusions

SubSeven and other examples of this class of malicious code can easily be used to compromise the integrity of Windows systems. Due to the capabilities of SubSeven, once a system is infected, there is little information that the infected system contains that can't be accessed using the Trojan. The availability and ease of use of SubSeven make it a useful tool for even unsophisticated users. Luckily, preventative measures like the use of up to date anti viral software, personal firewalls, personal and enterprise Intrusion Detection Systems, regular system audits, and especially user education can substantially reduce the risk of infection.

System audits are one tool that can be used to detect the presence of SubSeven and other malicious code. Audits also have the quality that they are relatively effective even when malicious code is new enough or different enough to evade current Intrusion Detection and Anti Virus software. Unfortunately, audits are not trivial. Preparation, skill and therefore cost is involved. However, like any security measure, if the information being protected is valuable enough, audits are worth the cost.

Source Code / Pseudo Code

The source code for SubSeven is not publicly available. However, recreating SubSeven would be possible, just a huge amount of work. The Windows 2000 resource kit comes with a tool that allows monitoring of system API calls. Back Orifice 2000 (www.bo2k.com) comes with source and analyzing this source would probably reveal many of the techniques that SubSeven uses for obtaining screen shots, keystrokes etc. A dis-assembler like "softice" (softice.tsx.org) will allow instruction-by-instruction analysis of programs. Also, sniffing the conversation between SubSeven client and server would provide a good understanding of the command set the client uses to control the server.

Additional Information:

1. GIAC weekly news bites archive URL: FBI Uses Keystroke Surveillance : Story 2

2. Symantec Corp Anti Virus Center URL: http://www.symantec.org/avcenter

3. McAfee Virus Information URL: http://www.mcafee.com

4. Computer Associates Virus Information URL: http://ca.com/virusinfo/

5. Cert (Computer Emergency Response Team) URL: http://www.cert.org

6. Chris Benton, "Basic Windows NT Auditing", SANS Level 1 version 1.1, edited by K Rosenthal.

7. SubSeven: www.subseven.ws, or http://www.sub7files.com - Download site for Trojan, admin tools, faq's etc.

8. Microsoft Knowledge Base: "Q270035 – How to Modify the List of Programs that Run When You Start Windows"

9. Eric Cole and Ed Skoudis, "Computer and Network Hacker Exploits – Part 11, Backdoors, Trojans, and RootKits, SANS GIAC Level 2