Interested in learning more about security?

SANS Institute InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

SubSeven 2.2: New Flavor of an Old Favorite

A new variation of a relatively old and powerful threat has rolled onto the Internet frontier. The latest version of an old hacker favorite offers more capabilities, functions and some very dangerous improvements. These new "improvements" make SubSeven (v 2.2) more difficult to defend against. In all types of war the rule holds true, know as much about your enemy as possible. This is the approach I have taken here. I tested SubSeven 2.2 in a lab environment on both, a typical Windows 2000 machine as well as a typical W...

Copyright SANS Institute

Author Retains Full Rights

AD

Aaron Greenlee
GSEC v 1.2e

SubSeven 2.2
New flavor of an old favorite

Introduction

A new variation of a relatively old and powerful threat has rolled onto the Internet frontier. The latest version of an old hacker favorite offers more capabilities, functions and some very dangerous improvements. These new "improvements" make SubSeven (v 2.2) more difficult to defend against. In all types of war the rule holds true, know as much about your enemy as possible. This is the approach I have taken here. I tested SubSeven 2.2 in a lab environment on both, a typical Windows 2000 machine as well as a typical Windows 98SE machine.

Background

SubSeven 1.0 was released on February 28th, 1999 (http://dark-e.com/archive/trojans/subseven/10/index.shtml). This version didn't have the ability to change its port. It was only able to listen on port 1243. That was quickly fixed. Version 1.0 was also buggy enough that other versions quickly followed. Version 1.4 was given an extensive file manager, however there still were some stability issues. Version 1.6 was the first edition to have an edit server. In version 1.8 there were four ways to infect a victim, and 3 ways to provide the port and IP address. This is also the first version to enable web cam viewing.

By version 1.9 it has some pretty serious capabilities along with some pretty silly ones. The abilities that seem rather trivial include the ability to open and close the CD-ROM drive, change the colors of the windows. It can hide things like the mouse, the taskbar, and disable the keyboard of the local machine.

It also has some potent and nasty capabilities as well. It has the ability to work as a FTP server. SubSeven can make changes to the registry, and get cached passwords. It can view, change, and close applications. It also has the ability to capture key stokes.

All of this ability in a package that is well under 500K, but the worst has only arrived now.

Version 2.2 - Infection

SubSeven usually comes as an email attachment. It has been sent under the guise of trojan removal programs, files that appear to be movie clips that most people would want to see such as BSpears_naked.mpeg.exe and every other way that is likely to slip past

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

unsuspecting end users. It can also be linked to other files that are very legitimate. The server portion of SubSeven will install in the back round while the legitimate file is taking the user's attention. The only prerequisite is that they are using any one of the Microsoft operating systems, and the Trojan is permitted to execute the installer program. From there it has its hooks in the system and configures itself to auto-start each time the computer is booted.

SubSeven has worked on Windows 9x for quite some time. It now works on NT 4.0 and 2000 as well. This opens up a whole new level of targets to aim at. Typically NT 4.0 and 2000 are used in more of a business environment. SubSeven provides such a full level of use that one compromised mobile user, fooled end user or a "neat movie clip" from a trusted friend, allows for a huge security hole to be created from which the rest of the network can be taken over piece by piece.

Installation

Installation of the server on a victim machine consists of clicking on the exe file that is the server. It is very easy to use the edit server to bind another file to the server file. In that case, the only thing that needs to be done is to click on the file bound to the exe server file and the server will install in the background. To throw victims off, you can also create an error message that is displayed when the server finishes installation. The server file can be renamed thought the edit server, or it can be a random file name as well.

SubSeven Server

SubSeven is highly configurable. It can be configured to infect in several ways, notify in several ways, and is designed in a very modular format. SubSeven's source code is not publicly available, but plug-ins can be written for it making it a moving target. To help facilitate this, rumor has it that a SDK will be released at some point.

- App redirect - This allows you to run commands on the victim's machine and have the output displayed on the client.
- AIM, ICQ, MSN and YAHOO spy - This allows you to see the conversation on the SubSeven client.
- Caps lock on/off
- Change resolution
- Change/view date and time
- Change volume settings
- Change windows colors
- Clipboard manager
- Control mouse
- Disable/enable ALT-CTRL-DEL
- Disable/enable keys
- File manager - This allows you to see where files are stored as well as add, remove, rename, and change their location.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

- Find files – Allows you to search for files on the victim's machine.
- Flip screen – A prank more than a serious threat that flips the screen 90, or 180 degrees.
- FTP server
- Get AIM password – Captures AIM Passwords
- Get cached passwords – Gather all passwords stored on the machine for various other programs. This takes advantage of Microsoft's desire to make password management easier for end users.
- Get home info – Gathers any personal information that has been entered into the registry. NOTE: Only about 5 percent of users actually do this according to www.Sub7files.com's FAQ.
- Get ICQ password – Captures ICQ password.
- Get pc info – Determines as much about the victim hardware as possible.
- Get RAS passwords – Captures Remote Access password.
- Get screen saver password – Captures Screen Saver password.
- Get screen shot – takes screen shot of victim's computer and sends to client.
- Hide/show clock - Most hide/show abilities are pranks for the most part.
- Hide/show desktop
- Hide/show mouse cursor
- Hide/show start button
- Hide/show task bar
- ICQ takeover – Used for hijacking a victim's ICQ account. It has the ability to read the UIN numbers on the machine. Can copy the UIN database and download it to your computer. You can then fully impersonate the victim, contact their friends and attempted to use the trusted relationship and infect them.
- Key logger – Logs all keystrokes on generated from the victim's keyboard.
- Log off, power off, reboot or shutdown windows – useful in harassing the victim as well as manually rebooting after installing other software if the need arises.
- Monitor on/off – More of a prank than anything.
- Network browser – This works like Network Neighborhood and lets you look for other machines on a LAN.
- Num lock on/off
- Open/close CD-Rom – You can open their drink holder for them if you see them get a drink via the web cam viewer.
- Packet sniffer – Works on the client machine.
- Play tic-tac-toe with server - Play tic-tac-toe against the server.
- Port redirect – Used to redirect packets to other ports in an effort to get around possible restrictions such as a weak firewall.
- Print manager
- Process manager – Allows client to view processes running on victim machine.
- Record from microphone – If the victim's computer has a microphone it can be turned on through the server and the sound directed to the client. This allows all sounds with in range of the microphone to be heard.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

- Registry manager - The registry manager allows you to edit the registry on the victim's machine.
- Scrolls lock on/off – Another prank type feature.
- Send keys
- Send message – Send message allows you to interact with the person using the compromised box. Use of this function can be a dead give away that they have been compromised. For the much less experienced user, this is also a very frightening thing if harassing messages are written or appear to be generated by the computer itself.
- Send to URL – This allows you to send log type information to a web server and display it as a web page as long as the server supports CGI.
- Show matrix – This is a prank feature. It was inspired by the movie after the same name (www.sub7files.com). It locks out the user and only shows a black screen with falling green text. The only way for the user to regain access to the machine is to reboot.
- Swap mouse buttons – Swapping the mouse buttons does just that, it makes the left button perform "right click functions". This can make new computer users think they are losing their minds.
- Text-2-speech
- View web cam – You can turn on the victim's web cam if they have one.

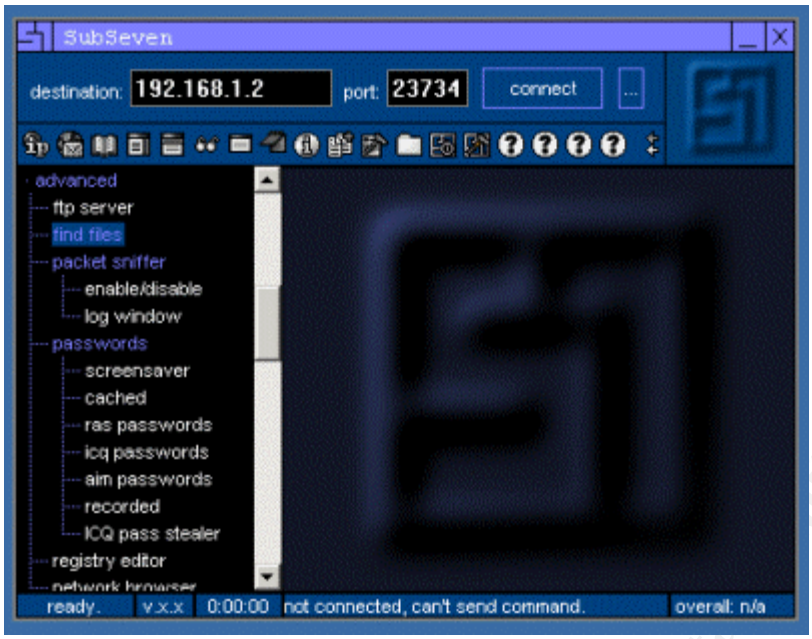
Window manager

This list of SubSeven v2.2 abilities without comments can be found at: http://dark-e.com/archive/trojans/subseven/22full/index.shtml

SubSeven Client

The SubSeven client has a very user-friendly layout. It has all the functions laid out on the left-hand column in expandable sections and an icon-based menu along the top edge of the display area. The IP address of the server the client is connected to, and the port number is just above. The client is intuitive enough to use that no skill level is needed.

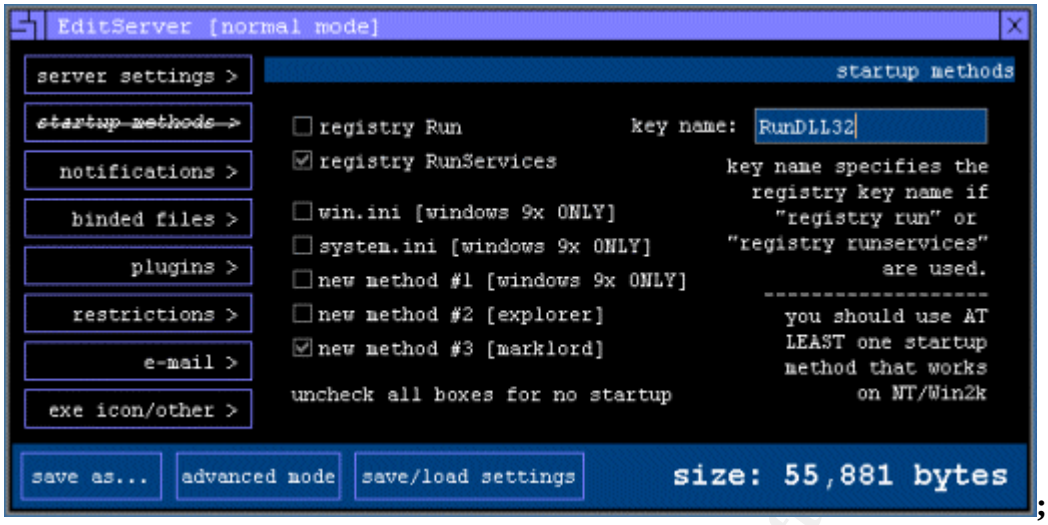
© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.



SubSeven Edit Server

The SubSeven editserver is where all the preparation takes place before a server is deployed. The editserver is used to modify the basic server and make use of its possible variations. Each time the editserver is run it creates a SubSeven server and then modifies it. It can load existing servers and modify them, as well as keep configuration files and use those to automatically force the changes on each new server created. This allows quick customization and is extremely easy to use. With the edit server, the port that each server listens on for client connections is configured, the passwords are created for both remote access, and a second password that protects the server from being edited by someone else. This means that if someone becomes infected and would like to see where the server is reporting information to, the name of the server and any other information that could be used in forensic analysis, they would need to know the protect password. The edit server also has a 3-attempt password limit, which makes brute force cracking this password extremely time consuming and unpractical. The edit server can be used to rename the exe from server.exe to anything else and can change the name of entry that goes into the registry. The methods of infection can also be chosen here as well. Most of these options work by checking boxes.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.



;

Sin – The ear to the ground

Sin is the program that listens for pre-configured SubSeven servers to announce that they are online. A pre-configured server can send the IP address, server name and port that it is listening on to Sin. This works with the random port feature that allows SubSeven to use a different port each time, increasing its stealth. The only catch to this is it reports to a static IP address. When a server connects it shows in green the server name, port and victim name if fully configured. All that is needed to do at this point is to double click on it and the connection is established. Sin.exe is included in the ss22.zip file.

Methods of Detection

Most Anti-virus software will detect SubSeven 2.2 as well as the client and edit server. Manual detection also includes recognizing some of SubSeven's abilities as well as a seeing unknown ports open while running netstat and investigating them. SubSeven is designed not to show up when listing processes or programs running. This makes having a known base line of normal operation for each machine all the more important.

Removal

Removal in my test of Norton Anti-virus 2001 consisted of identifying the infected files and quarantining them. However, the registry will still need a human eye to make the changes back to pre-infection state in most cases. I strongly recommend writing down the infected file names. This will make finding the affected registry keys easier.

Removal directions are have been basically standardized. I have included the removal instructions found at http://members.tripod.lycos.nl/brouw039/remsubseven22.html. Some of these steps can be skipped if the files are first found by anti-virus software.

Step 1.
Click Start > Run and type Regedit.
Follow the paths using regedit and find:

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

HKEY_LOCAL_MACHINE
Software
Microsoft
Windows
CurrentVersion
Run
In the right window, look for look for the item titled:
Loader = "c:\windows\system*"**
The *** will be a random file name. Write this down as it is the Sub7 server!
Right click on that line and choose delete.
Step 2.
Follow the paths using regedit and find:
HKEY_LOCAL_MACHINE
Software
Microsoft
Windows
CurrentVersion
RunServices
In the right window, look for look for the item titled the same as above:
Loader = "c:\windows\system*"**
Right click on that line and choose delete.
Step 3.
Exit the Registry.
Step 4.
Click Start > Run and type Sysedit.
Open the file Win.ini. Near to the top you will see a line with:
run=
If you see a path pointing to the Sub7 server here as well, delete it so the line only reads:
run=
Save and close file Win.ini.
Open the file System.ini. Look for a line starting with:
Shell=explorer.exe
If the Sub7 server name is after this, remove that file name so the line reads exactly:
Shell=explorer.exe
Save and close file System.ini.
Step 5.
Exit Sysedit and reboot your computer.
Step 6.
Click Start > Find/Files or Folders. Search all drives for files with the name "***". The random file you have found as the Sub7 server. Delete them all and empty your recycle bin.
Step 7.
Reboot your computer.

Synopsis

In my testing I was not able to make a server actually listen for remote connections. It did make the expected changes in the registry, win.ini and system.ini files. I used netstat, a firewall and a packet sniffer to verify that it was not working and verify that the client was. I tried installing the SubSeven server on both a Windows 98SE machine as well as

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

a Windows 2000 machine. In my research I found a newsgroup about SubSeven 2.2 where several people complained about the same results. It is my belief that SubSeven 2.2 in its current state does not work or there are many more broken versions floating around than working ones. Mobman, the author of SubSeven is more than likely making the required fixes to get it working. I also found an opinion regarding this that stated the client is the actual trojan and the people who think they are so clever, are the actual victims, and that Mobman and possibly a small faction of people are the truly clever ones.

Regardless of what the actual situation, this only proves that the stakes are steadily climbing in the world of computer security.

References

1. http://dark-e.com/archive/trojans/subseven/10/index.shtml (April 13, 2001)
2. www.sub7files.com (Site has been taken down) (April 13, 2001)
3. http://members.tripod.lycos.nl/brouw039/remsubseven22.html (May 18, 2001)
4. http://www.tlsecurity.net/news/ (May 17, 2001)
5. http://www.infowar.com/iwftp/xforce/advise73.shtml (May 18, 2001)
6. http://subseven.slak.org (Site has basically been taken down.) (April, 13 2001)
7. http://www.symantec.com/avcenter/venc/data/backdoor.subseven.22.a.html (May 18,2001)

© SANS Institute 2003, Author retains full rights

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Last Updated: August 23rd, 2017

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Tampa - Clearwater 2017	Clearwater, FLUS	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS Network Security 2017	Las Vegas, NVUS	Sep 10, 2017 - Sep 17, 2017	Live Event
SANS Dublin 2017	Dublin, IE	Sep 11, 2017 - Sep 16, 2017	Live Event
SANS Baltimore Fall 2017	Baltimore, MDUS	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Copenhagen 2017	Copenhagen, DK	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS London September 2017	London, GB	Sep 25, 2017 - Sep 30, 2017	Live Event
Data Breach Summit & Training	Chicago, ILUS	Sep 25, 2017 - Oct 02, 2017	Live Event
Rocky Mountain Fall 2017	Denver, COUS	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS SEC504 at Cyber Security Week 2017	The Hague, NL	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Oslo Autumn 2017	Oslo, NO	Oct 02, 2017 - Oct 07, 2017	Live Event
SANS DFIR Prague 2017	Prague, CZ	Oct 02, 2017 - Oct 08, 2017	Live Event
SANS Phoenix-Mesa 2017	Mesa, AZUS	Oct 09, 2017 - Oct 14, 2017	Live Event
SANS October Singapore 2017	Singapore, SG	Oct 09, 2017 - Oct 28, 2017	Live Event
SANS AUD507 (GSNA) @ Canberra 2017	Canberra, AU	Oct 09, 2017 - Oct 14, 2017	Live Event
Secure DevOps Summit & Training	Denver, COUS	Oct 10, 2017 - Oct 17, 2017	Live Event
SANS Tysons Corner Fall 2017	McLean, VAUS	Oct 14, 2017 - Oct 21, 2017	Live Event
SANS Tokyo Autumn 2017	Tokyo, JP	Oct 16, 2017 - Oct 28, 2017	Live Event
SANS Brussels Autumn 2017	Brussels, BE	Oct 16, 2017 - Oct 21, 2017	Live Event
SANS Berlin 2017	Berlin, DE	Oct 23, 2017 - Oct 28, 2017	Live Event
SANS San Diego 2017	San Diego, CAUS	Oct 30, 2017 - Nov 04, 2017	Live Event
SANS Seattle 2017	Seattle, WAUS	Oct 30, 2017 - Nov 04, 2017	Live Event
SANS Gulf Region 2017	Dubai, AE	Nov 04, 2017 - Nov 16, 2017	Live Event
SANS Miami 2017	Miami, FLUS	Nov 06, 2017 - Nov 11, 2017	Live Event
SANS Amsterdam 2017	Amsterdam, NL	Nov 06, 2017 - Nov 11, 2017	Live Event
SANS Milan November 2017	Milan, IT	Nov 06, 2017 - Nov 11, 2017	Live Event
Pen Test Hackfest Summit & Training 2017	Bethesda, MDUS	Nov 13, 2017 - Nov 20, 2017	Live Event
SANS Paris November 2017	Paris, FR	Nov 13, 2017 - Nov 18, 2017	Live Event
SANS Sydney 2017	Sydney, AU	Nov 13, 2017 - Nov 25, 2017	Live Event
SANS San Francisco Fall 2017	OnlineCAUS	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced