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

“SUBSEVEN TROJAN SUMMARY”

Kelly Kester
December 19, 2000

Working at the Department of Defense Continental United States Regional Computer Emergency Response Team (DoD CONUS RCERT), my co-workers and I personally review intrusion detection logs for all government networks designated in our area of responsibility. In almost any given week, the evidence of unauthorized network probes, scans, intrusions, access attempts, and malicious logic is common place. In reference to malicious logic, our daily traffic reflects trojans activity considerably more frequent than viruses and/or worms. A trojan opens holes in your computer where anyone can access your computer. It is similar to a virus, except that it does not replicate itself. It stays in the computer doing its damage or allowing somebody from a remote site to take control of the computer. For example, if you get infected with a trojan, anyone can open your CD-ROM drive, shut down your computer, delete files, log what you are typing and lots more. One of the most common trojans we have seen lately is the SubSeven trojan, which has many aliases such as; Backdoor.Trojan, Pinkworm, BackDoor-G, BackDoor-G2.svr.21

OVERVIEW

SubSeven is one of the most popular tools on the net. It has been around for almost 1 ½ years and keeps getting better and better. 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.

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 was made to fill in the gaps left by NetBus. NetBus was the first 'point and click' trojan that made it very easy for hackers to abuse an infected system . The makers of SubSeven wanted to take this even further and give the hackers even more control than NetBus ever could.

SubSeven can do everything that NetBus can do. This includes:

- File controls
- Upload / Download
- Move, Copy, Rename, Delete
- Erase harddrives and other disks
- Execute programs
- Monitoring
- Can see your screen as you see it
- Log any/all keypresses (even hidden passwords)
- Open/close/move windows
- Move mouse

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

- Network control
- Can see all open connections to and from your computer
- Can close connections
- Can 'bounce' or relay from their system to yours, so wherever they connect, it seems as if you are doing it. This is how they prevent getting caught breaking into other computer systems and you can get in trouble!

SubSeven can also be configured to inform someone when it's infected computer connects to the internet, and tells that person all the information about you they need to use the trojan against you. This notification can be done over an IRC network, by ICQ, or by email.

HOW IT WORKS

When ran, the backdoor trojan does the following:

1) 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).

2) Unpacks a single DLL file to the Windows System directory – WATCHING.DLL (some versions don't do this).

3) After that, the backdoor patches Windows Registry so that its main application will be run during every Windows bootup (Run or RunServices keys).

4) 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 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. 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.

If the SubSeven backdoor task is active in the memory and invisible in Task Manager, it looks for TCP/IP connections. 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.

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

FIX SOLUTION

Removing SubSeven is a two-step procedure due to you having to shutdown and delete the trojan. Firstly, boot into MS-DOS mode. Do this by shutting down your computer and starting it up again. While its loading press F8 multiple times until you get a text based list. This will have an option called "Command prompt only". This is MS-DOS so move the highlighter onto that and press enter. This will load DOS and you will be prompted with ***C:***\>. You are now in DOS mode.

> Now that you're in DOS, type ***cd windows***. This will take you into the Windows directory. Now you must delete some files. You can do this by typing the following commands exactly as they appear below:
> ***del SysTra~1.Exe***
> ***del nodll.exe***
> ***del systray.exe***
> ***del kernel16.dl***
> ***del kerne132.dl***
> ***del rundll16.exe***
> ***del nodll.exe***

Note: Some files will have the error "File not Found."

Once you have done that, type ***exit***. This will take you back to Windows. Now when you run Windows, you may find errors saying some file is not found. This is due to the trojan being designed to run every time you start Windows, but since you deleted the trojan, it can't run anymore. It's now time to remove the parts added onto your computer which make the trojan start every time you boot.

Click on the ***Start*** menu, and then click on ***Run***. In run, you will be required to type in ***regedit.*** Here the Windows Registry Editor should open. This is the heart of your computer, so don't delete anything you don't need to delete. When regedit starts, you will see a file-like tree on the left-hand panel. Expand the folders to follow the path:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

At the end, click on 'Run' once, and the right hand panel should change. Look on the right of the regedit box for the following:

> ***SystemTrayIcon = "C:\WINDOWS\SysTrayIcon.Exe"***
> ***SystemTray = "SysTray.Exe"***
> ***Kernel16 = "kernel16.dl"***
> ***RegistryScan = "rundll16.exe"***

If you have any one of these, click on it once with the left mouse button, then right click on it. When the menu item appears, click on ***delete***. Once all are deleted, close regedit and reboot your computer.

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

Note: Some versions of SubSeven won't add anything to regedit, so if you don't see any of the lines above, just proceed to the next step.

Now it's time to check the ***Win.ini file***. This loads every boot and some versions of SubSeven add a line to the ***Win.ini file***. Go to the ***Start*** menu, ***Programs***, click on ***Accessories*** and then click on ***Notepad***. Notepad is a text editor and will help you to edit Win.ini. Now that you are in Notepad, click on ***File.*** A dialogue box will appear, then click ***Open***. In the Open window, navigate into the Windows directory, click on ***Win.ini*** and click open (c:\windows\win.ini). At the top of the file should be the SubSeven line, so if you see the following, delete it:

run=nodll

Click on ***File*** again and go to ***Save***. Next, click to ***File*** and ***Open*** again and select the file ***system.ini.*** This is only in one version of SubSeven, so if the following isn't there, don't worry. There should be a line in the System.ini saying "***shell=explorer.exe***". This is okay, but if it says "*shell=explorer.exe -trojan_name_here-.exe*", delete the bit saying *"-trojan_name_here-.exe*" so the line will end up as "*shell=explorer.exe*". Save the file from the File menu.

Now you have successfully removed SubSeven, but before you're finished, reboot your machine.

REFERENCES

1. Search the Encyclopedia (*define this term: trojan horse)* URL: http://www.techweb.com/encyclopedia/defineterm.cgi?sstring=trojanhorse (December 6, 2000).
2. Residential Networking (North Carolina State University). 14 August 2000. URL: http://www.ncsu.edu/resnet/security/subseven.html (December 6, 2000).
3. Sub 7, 11 December 2000. URL: http://subseven.slak.org (December 6, 2000).
4. Kelloway, Donald F. "The Basics of SubSeven (aka Sub7 and Backdoor_G" URL: http://www.commodon.com/threat/threat-sub7.htm (December 6, 2000).
5. SANS Institute Resources. " SubSeven Trojan v 1.1." URL: http://www.sans.org/newlook/resources/IDFAQ/subseven.htm (December 6, 2000).
6. Han, Wason. "SubSeven 2.0 Server" 4 October 1999 URL: http://www.symantec.com/avcenter/venc/data/sub.seven.20.html (December 6, 2000).

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