Coping With RATs

A Look at the Problem of SubSeven and "Remote Administration Trojans

Overview

A Remote Administration Tool, or RAT, is a Trojan that when run, provides an attacker with the capability of remotely controlling a machine via a "client" in the attacker's machine, and a "server" in the victim's machine. The server in the victim "serves" incoming connections to the victim, and runs invisibly with no user interface. The clientis a GUI front-end that the attacker uses to connect to victim servers and "manage" those machines. Examples include Back Orifice, NetBus, SubSeven, and Hack'a'tack. What happens when a server is installed in a victim's machine depends on the capabilities of the trojan, the interests of the attacker, and whether or not control of the server is ever gained by another attacker -- who might have entirely different interests.

Infections by remote administration Trojans on Windows machines are becoming as frequent as viruses. One common vector is through File and Print Sharing, when home users inadvertently open up their system to the rest of the world. If an attacker has access to the hard-drive, he/she can place the trojan in the startup folder. This will run the trojan the next time the user logs in. Another common vector is when the attacker simply e-mails the trojan to the user along with a social engineering hack that convinces the user to run it against their better judgment.

Version 2.2 of SubSeven, released March 9, is more powerful and dangerous than earlier versions. For example, the new version includes expanded notification capabilities that facilitate collaboration in distributed denial-of-service attacks. Multiple attackers can be provided with a list of infected machines, which can then be directed to flood any specific target(s). The new SubSeven supports socks4 and socks5 proxies, which help attackers hide their identities. Using these proxies to cross international borders could make it more difficult to trace the source of an attack.

History of SubSeven

SubSeven has been around for just two years, with a new version available about once a month. The chronology shows this history. Each version has generally been undetectable by anti-virus products, until their scan strings were updated. With a monthly release schedule, updating defense products (such as PestPatrol or anti-virus software) monthly is clearly a good idea!

Version	Date
SubSeven 1.0	2/28/1999
SubSeven 1.1	3/7/1999
SubSeven 1.2	3/15/1999
SubSeven 1.3	3/22/1999
Subseven 1.4	3/29/1999

SubSeven 1.5	3/29/1999
SubSeven 1.6	4/17/1999
SubSeven 1.7	5/2/1999
SubSeven 1.8	5/17/1999
SubSeven Fixes	5/31/1999
SubSeven Apocalypse	6/16/1999
SubSeven 1.9	6/21/1999
SubSeven 2.1.3	6/28/1999
SubSeven 2.1.3 Bonus	6/28/1999
SubSeven 2.1.4 Defcon 8	6/28/1999
SubSeven 2.2b2	6/28/1999
SubSeven Pass	7/20/1999
SubSeven Server 2.0	9/18/1999
SubSeven 2.1	12/7/1999
SubSeven Speech	12/7/1999
Subseven Server 2.1.3 Unpacked	2/23/2000
SubSeven Server 2.1.3 M.U.I.E.	4/24/2000
Subseven Loader	6/10/2000
SubSeven 2.2 Beta 1	12/27/2000
SubSeven 2.2	3/9/2001

Extent of the Problem

How Many Users are Infected?

We don't have any procedures to quantify the pervasiveness of SubSeven, but there are many experts who are willing to guess at it. Chris Rouland, director of X-Force at ISS estimates the total number of infected machines to be in the tens of thousands. source The WildList reported SubSeven in five countries in July, 1999 source.

What Harm Can Be Caused?

A RAT like SubSeven has full power over a machine, as long as there is a live Internet connection. Because SubSeven can be controlled to retrieve a file and run it, it is extensible, and what one attacker can make it do is not necessarily what it was originally equipped to do. For instance, SubSeven could be made to retrieve a program that overwrites every byte of the hard disk repeatedly, the first time that there was no keyboard activity for an hour. Such destructive code is not part of SubSeven, but SubSeven can be made to retrieve and run such code.

Here are some of SubSeven's major capabilities:

File controls Upload or Download any file.

Move, Copy, Rename, Delete any file.
Erase hard drives and other disks
Run any program.

Monitoring Display your screen remotely as you see it locally

Log all keystrokes, including non-displaying passwords.
Open, close, and move windows
Move the mouse

Network control Monitor all open connections to and from your computer

Open and Close connections
Relay through your system to another system. An attacker can get you in trouble for an attack they per form under your identify.

DDoS with SubSeven Now a Reality!

SubSeven can be used to perform Distributed Denial of Service attacks, and has been. On March 31, for instance, we received an email reporting attacks via SubSeven's default TCP port (27374) via several dozen machines in which SubSeven was running. The actual attacker, presumably, was none of the Source IP addresses noted below.

A summary of our border, in the format below, all on TCP 27374 - all of this traffic arrived beginning 01:25:48 UTC 1 Apr 2001, and abruptly ceased at 02:22:07 UTC:

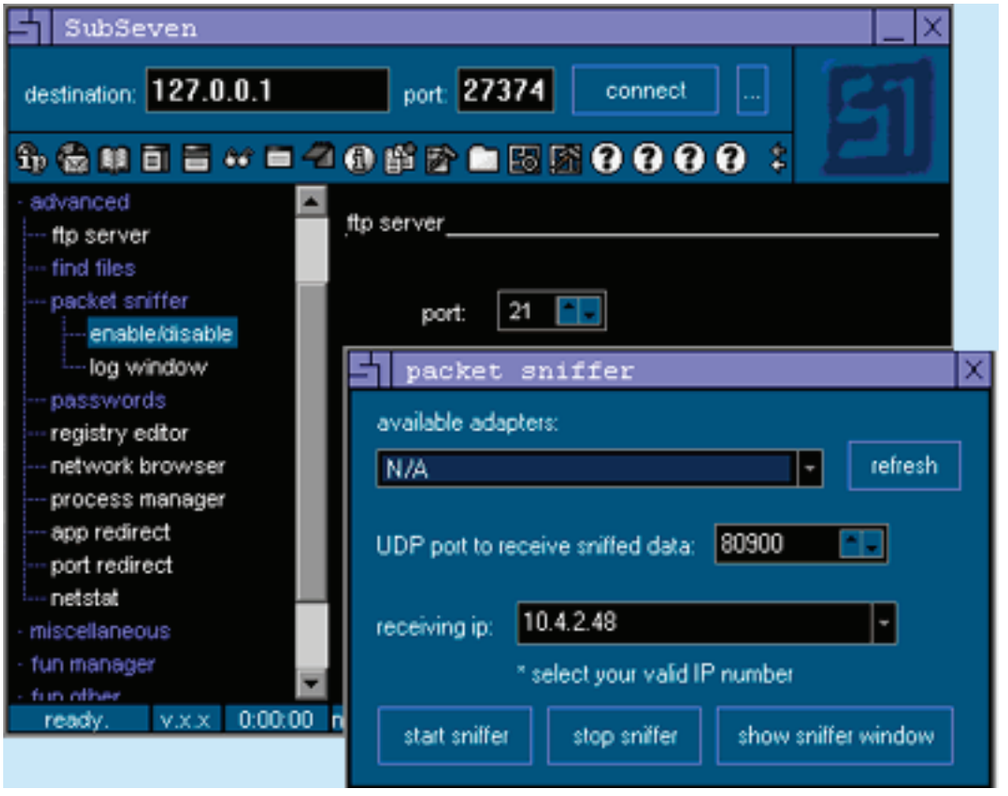
Nodes Hit	Source
83	66.24.216.220
76	65.27.22.66
70	24.191.2.106
61	65.27.22.23
59	24.176.70.54
55	64.169.39.150
54	66.31.2.197
53	66.31.172.18
51	24.188.217.0
44	24.184.187.38
43	66.31.184.236
42	66.31.9.69
30	66.24.47.47
29	66.30.8.249
29	66.30.186.174
28	66.65.84.58
24	24.191.3.157
22	66.30.26.56
20	24.112.73.20
17	152.7.48.9
16	129.237.103.214
16	128.118.213.10

15	66.30.126.166
14	152.7.39.116
13	66.65.78.227
13	164.76.172.205
11	66.31.169.178
9	131.247.226.81
6	216.184.159.159
5	24.88.88.6
3	146.151.81.87
1	24.168.241.187

The capability of performing such DDoS attacks has been present in SubSeven since a version of June, 1999. But its capabilities for such attacks have been growing. For instance, SubSeven 2.2 can use common gateway interface (CGI) scripts. Attackers can use such scripts to remotely and automatically post the IP addresses of infected machines, and later use a number of them in a co-ordinated attack on any SubSeven server.

The anonymity of the attacker is preserved, in SubSeven, via SOCKS4/SOCKS5 Proxy Support. “Proxies” are intermediaries between two systems. By adding one or more hops between attacker and victim, the task of tracking an attack back to its source becomes more difficult. Information about available “open” proxies is freely traded among SubSeven users.

SubSeven can also serve as a “pre-attack” tool, gather information that might be of use in a more sophisticated attack. SubSeven can operate as a packet sniffer via a GUI, which makes its use much easier. The sniffer can be configured to collect network traffic, save this information into a log, and relay these logs.



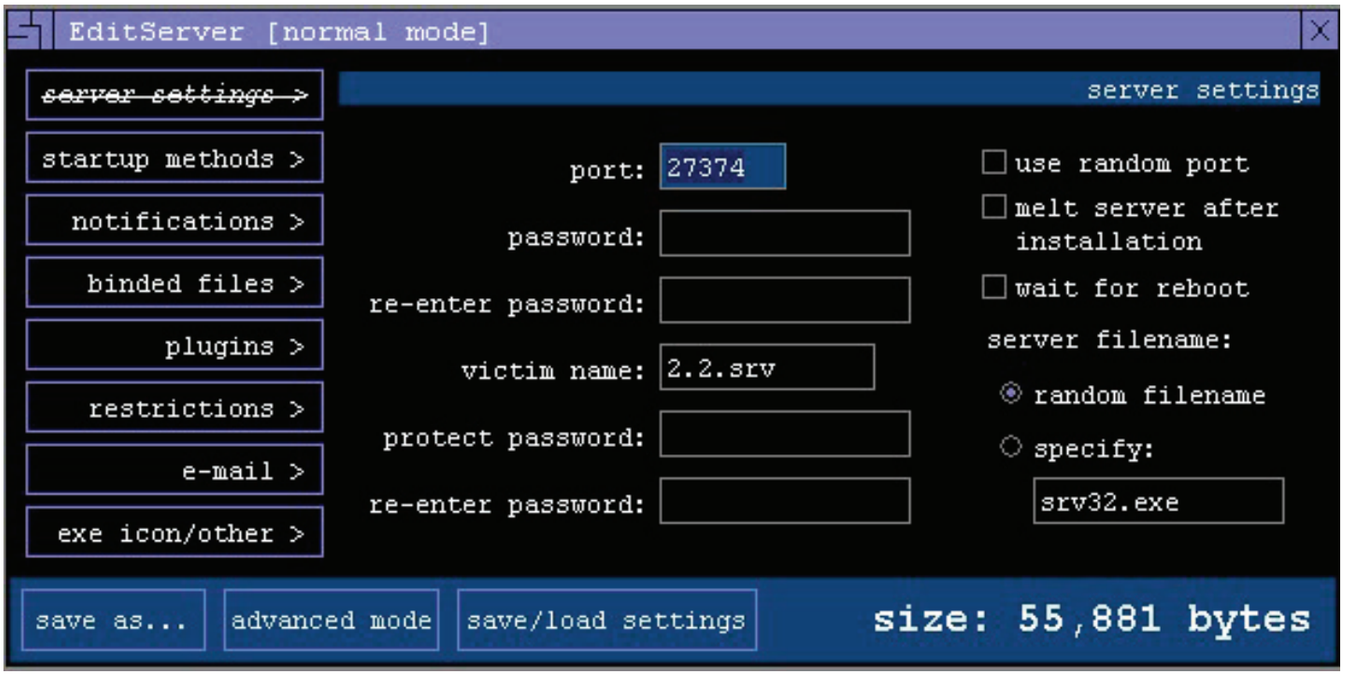
How It Happens

How the RATs Get In

There are many ways that a RAT can get into your machine. The most common RATs are distributed as mail attachments in newsgroups, particularly (for some reason), pornographic news groups. The attachment might be named: “BritneySpears.mpeg.exe” or “BritneySpears.mpeg.exe”. When a newsgroup sends out 100,000 emails with a spicy message and such an attachment, someone is sure to click on the attachment and run it. Within days of the release of SubSeven 2.2, newsgroups were used to distribute the RAT to users. Source.

RATs are often distributed bound with other applications, so that when you run the other application (such as WinAMP) you actually also run the RAT server. Since the RAT server installs silently, even a sharp user won’t see anything unusual. Such trojanized applications are distributed via e-mail, newsgroups, and software distribution sites.

SubSeven’s server editing tool, EditServer, allows the attacker to couple the SubSeven server with any number of additional files, and for each, to specify whether it will be executed or extracted when the combined file is run. For example, if an MP3 is bound in with the server, and set to execute, then the music of the MP3 will be played as the SubSeven server silently installs.

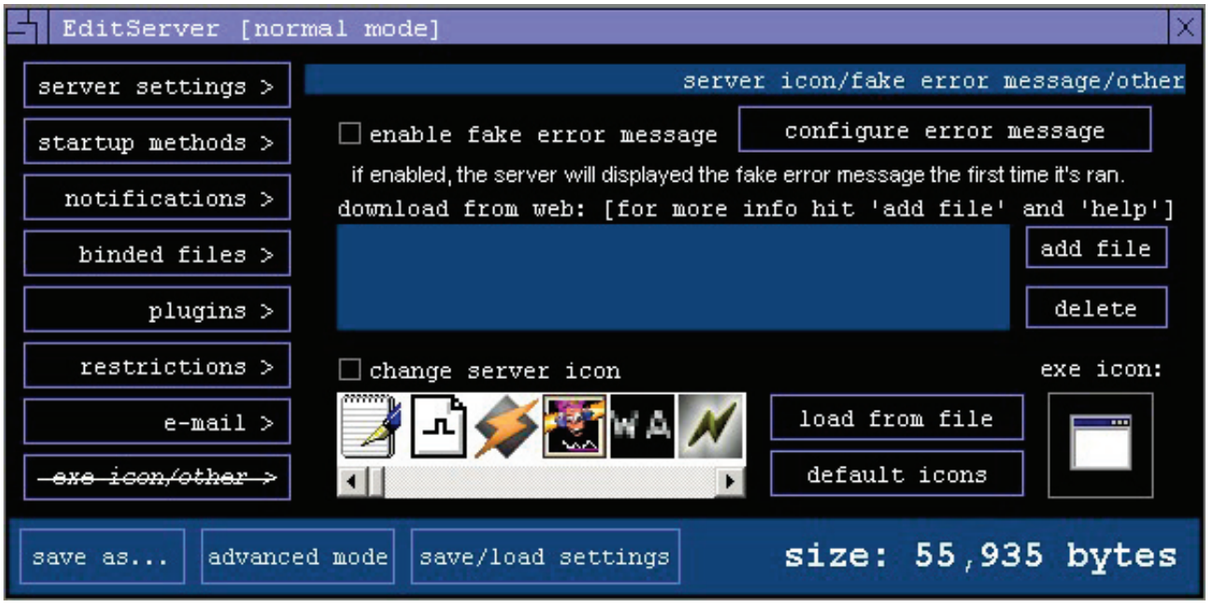


SubSeven is often distributed with WinAMP -- so often, in fact, that there are even “skins” for WinAmp after it is bound to the SubSeven Server. Here’s a screen shot of the SubSeven Server, after being bound to WinAmp.

Why RATs Don’t Get Caught

It is the Server that is distributed to a victim. The SubSeven Server can be as small as 55Kb, have any name, any icon, any size.

More Stealth: SubSeven can be configured to display a fake error message when run, to help “explain” to the user why clicking on it didn’t produce the expected result. The icon displayed can be configured (see screen shot below), as can the file size.



And More Stealth: SubSeven sends its information out via a TCP or UDP port. In the old days, the attacker would select the port to use, run EditServer to provide that info to the server, then ship the server. And in the old days, a simple tool could look at each port, see if it was in use, and hazard a guess as to what might be using it. With SubSeven 2.2, the server can be configured to listen on a random port each time it is started, and configured to notify the attacker of the port change.

Catching a RAT should be easy with an anti-virus product, but this is only in theory. A tool like SubSeven has been released far more frequently than most users update their scan strings. No variant is ever released that happens to be detectable by existing scanners/scan strings. Because users don't update their protection, they are vulnerable.

When the SubSeven Server is clicked, it may create two or more copies of itself. In one test, it created sdiamd.exe and qkjsxtqx.exe in the system32 directory.

The Power of a RAT

Default Power

Passwords: SubSeven now includes options to email all pressed keys, all passwords, or passwords stored on the system (RAS, dialup, etc.). To turn on such an option, the attacker simply supplies an e-mail address to receive the information. The screen below shows how EditServer can be used to configure the server to send all passwords captured to a specified email address.

Option, Options, Options: Using the SubSeven client, the server can be made to change ports, to restart, or shut down. Using the Text to Speech capability, the attacker can type text, which will then be converted to speech in the victim's machine.

Fun Management: SubSeven includes a "Fun Manager" in the client, with many functions including:

Screen capture at controllable intervals
Webcam
Flip screen horizontally, vertically, or both
Print manager -- send any text to their printer, with control of font size and effects such as bold and un derline
Browser control -- open the victim's browser to any specified URL
Screen resolution control: get available resolutions, then change to any of those available
Change screen colors for menus, task bar, buttons, window background, etc. and restore default colors when you want.
Play tic-tac-toe with the victim
Restart the remote computer (shut down, power off, hibernate, reboot, or merely log the user off)
Mouse madness: reverse mouse buttons, hide the mouse, control the mouse, control the length of mouse trails
Read and change volume settings including wave, synth, and CD balance.
Record with their microphone for any duration, then play the recording, with control over quality
Get or set serer time/date
Show/hide desktop icons, show/hide Start button, open/close CD-ROM, show/hide clock, start/stop speaker, show/hide taskbar, turn monitor on/off.

Growing Power

SubSeven can be bound with any of the plugins (additional code modules) that have been written for it, or with any new plugins that might be created. This gives the basic SubSeven considerable extensibility. But to make it even more versatile, such plugins may be uploaded to a web site, and the server can then be instructed to

download and install them. Plugins can end in any file extension. In addition, under the control of the client, the server can be made to update itself from a file or from a URL.

The Proliferation of RATs

Over the past decade of the Internet, RATs have proliferated. SubSeven is now just one of many, including * 711 * AcidBattery * Acid Kor * Acid Shiver * Amanda * Ambush * AOL Admin * Ashley * Ass Sniffer * Asylum * Back End * Backage * BackConstruction * BackDoor * Back Orifice * Barok * Barrio * BeeOne * B.F. Evolution * Big Brother * BioNet * Bla * Blackharaz * Blade Runner * Blazer * Bo-Bo * BoFacil * BoWhack * Brain Spy * B.R.E.A.C.H. * Breach Prowler * BSDi Backdoor * Bundy * Bus Conquerer * Butt-Man * Cafeini * Cain * CC Invader * Cero * Chupacabra * Coma * Connection * Control du Sockets de Troie * ControlTotal * Crazy CD Tray * CrazzyNet * Cyber Takeover * CyberSensor * Dark Connection Inside * Deep Back Orifice * DeepThroat * Delta Source * Der Spaeher * Dial Up Raper * Donald Dick * DP Trojan * Drat * Eclypse * Edit Server for SubSeven * Enterprise * Error32 * Doly Trojan * Event Horizon * Excalibur * Executor Controller * Exploiter * Explorer * Fake Surf * File Nail * FireHacker * FireHotcker * Forced Entry * Fore * Freak 2K * FruitCake * Funny Trojan * Gaban Bus * GateCrasher * GirlFriend * Globale Project Rux * Haebu Coceda * Hack'a'Tack * Hacker_Brasil * Host Control * HVL RAT * InCommand * Indoctrination * INet Spy * Infector * Infra Trojan * Ini-Killer * Internet Connection Monitor * Intruse * IPX Control * Kaos * Khe Sanh * Kid Terror * KillSwitch * Krippled * Lamer's Death * LameSpy * Le Guardien * Logged * LRAM Kit * Mail Shtirlitz * Master's Paradise * Matrix * Millenium * MiniAsylum * MiniCommand * Mosaic * MoSucker * Nephron * Net Administrator * Net Spider * Net Trash * NetBus * NetBus Pro Cracker * NetBus Toy * NetBuster * NetController * NetDemon * Netministrator * NetMonitor * NetRaider * NetRex * NETrojan * NetSphere * NetSpy * NetTaxi * New Silencer * Nirvana * Noknok * NT Remote Controller * One Of The Last Trojans * PC Invader * PCrasher * Peanut Brittle * Phantom * Phase Zero * Phineas Phucker * Port Activator * Portal of Doom * Precursor * Priority * PrivatePort * Progenic Trojan * Project Next * Prosiak * Psycho's Nightmare * PsychWard * RAT Cracker * Rat Head * RC * Remote Administrator * Remote Boot Tool * Remote Explorer * Remote Hack * Remote Storm * Remote Windows Shutdown * Revenger * Robo-Hack * Ruler * RUX * Sanctuary * SBD * Scarab * Schwindler Trojan* Secret Service * ServeMe Trojan * Sesame Control Center * ShadowPhyre * SheepGoat * Skydance * Snid X3 * SniperNet * Sockets de Troie * Solaris Trojan * Spy * Spying King * SubSeven * SubSevenX * SubZero * Swift Remote * Syphillis * Sysmon * Tambu Dummy * TCP/IP Connector * Teman * TerrorTrojan * The Flu * The tHing * The Trojan Cow * The Unexplained * TotalRC * Toxic NetBus Ultima * Trojan First Aid Kit * Trojan Spirit * Truva Ati * Un Locked * Undetected * Valv-Net * Virtual Hacking Machine * VooDoo Doll * Vortex * WANRemote * War Trojan * Warning 2000 * WebAsylum * Web Serve CT * WinControl * WinCrash * WinS.A.T.A.N. * Xanadu * XConsole * XTCP * Y3K RAT * YAT - Yet Another Trojan *

Download Sites

RATs are widely available. SubSeven, for instance, is available from dozens of sites. RAT Removal

Removing a RAT is not straightforward, because the RAT server will normally be running as a service, and cannot be deleted. The trick is to identify the RAT as a file, then identify the process that invokes the RAT (such as a registry entry on line in an ini file), remove the invocation process, reboot the machine, and now remove the RAT.

There are seven possible processes by which SubSeven can be invoked. One or more of these methods might be configured, so all must be checked.:

Method	Notes
registry Run	Default keyname is RunDLL32, but any may be used. You'll find a registry entry like HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run with a Key Name of RunDLL32 and a value of D:\WINNT\System32\sdiamd.exe (or whatever your system directory is, and whatever the name of the SubSeven server.)
registry RunServices	Default keyname is RunDLL32, but any may be used.
win.ini [Win9x only]	In NT/2K, no entry will be created in win.ini
system.ini [Win9x only]	In NT/2K, no entry will be created in system.ini
"new method #1" [Win9x only]	
"new method #2 [explorer]"	HKEY_CURRENT_USER: Software\Microsoft\Internet Explorer\Explorer Bars\{C4EE31F3-4768-11D2-BE5C-00A0C9A83DA1}\FilesNamedMRU may hold three keys named 000, 001, and 002, whose values are, respectively, qkjs*.exe, sdiamd.exe, and rege There may be another identical entry *3 keys) at HKEY_USERS\S-1-5-2-83952215-1935644697-1343024091-500\Software\Microsoft\Internet Explorer\Explorer Bars\C4EE31F3-4768-11D2-BE5C-00A0C9A83DA1}\FilesNamedMRU
"new method #3 [marklord]"	

References

SubSeven From the SaferSite Pest Info Database.
Experts warn of new hacking tool. James Middleton. March 12, 2001 VNU Business Publishing Limited
Hacker unleashers updated backdoor program InfoWorld. March 15, 2001 Douglas F. Gray.
Mutations make new SubSeven virus riskier. CNET News.com Staff March 15, 2001
Security Experts Warn of Updated Trojan So-called backdoor program SubSeven could infect your PC and use it as launching pad for later attacks. Douglas F. Gray, IDG News Service Tuesday, March 13, 2001
"SubSeven DEFCON8 2.1 Backdoor" Trojan. ADVISORY 00-056 National Infrastructure Protection Center (NIPC). Overview