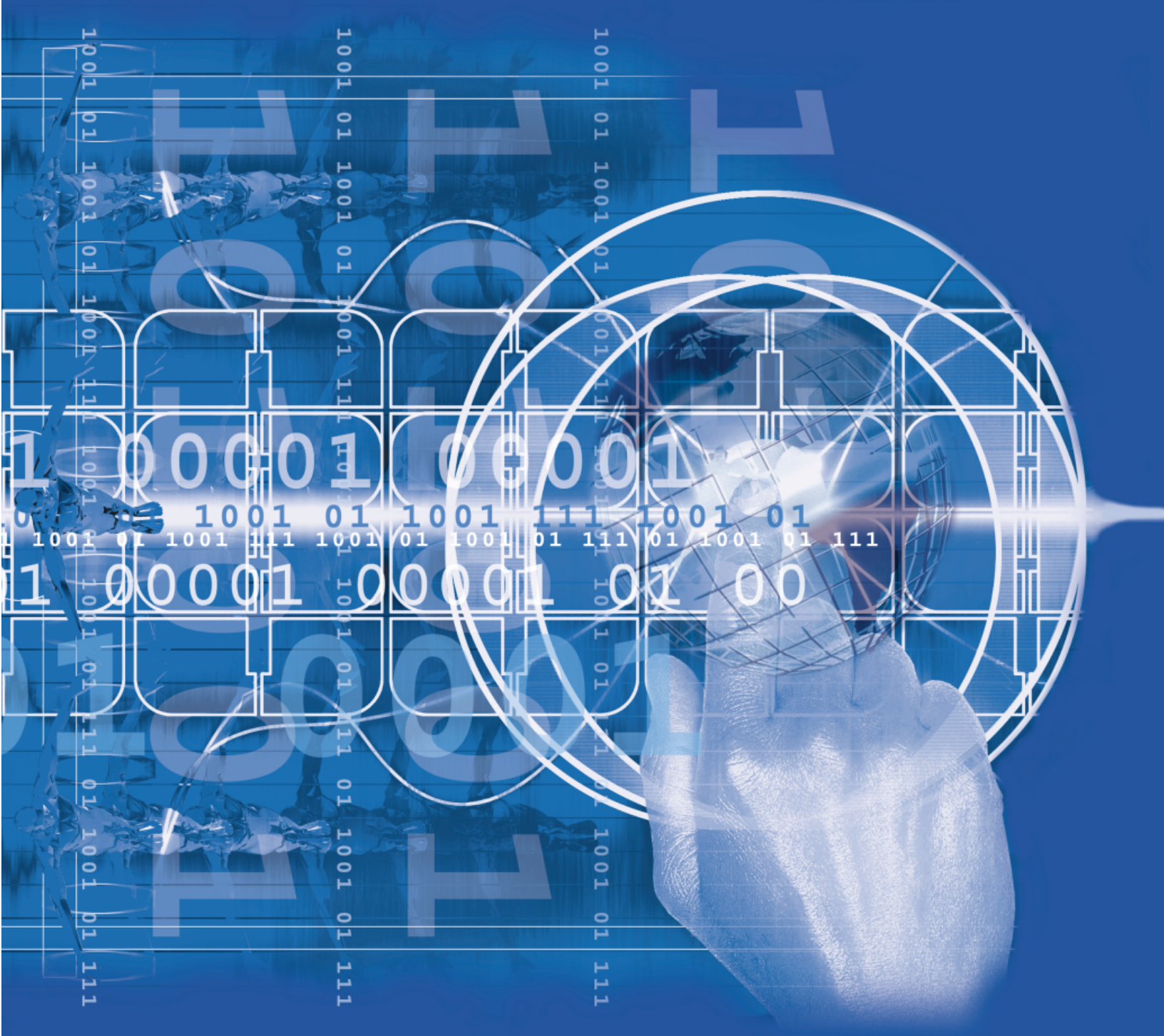
iDEFENSE™

The Power of Intelligence



Analysis of SubSeven.Trojan Distributed Attack Feature

iDEFENSE™
The Power of Intelligence

iDEFENSE Analyzes Feasibility of Distributed Attacks using SubSeven

Much attention has been focused recently on SubSeven, a Trojan horse "hacker tool" in wide circulation around the Internet. iDEFENSE security engineers obtained copies of SubSeven variants associated with recent miscreant activity and performed detailed forensic tests in a controlled environment. Based on our analysis of these SubSeven variants, it is evident that they can be used to launch distributed ping flood attacks from compromised machines around the Internet. As with all flooding activity, the effect of this attack depends directly on the characteristics of the specific target host, as well as on the available bandwidth from the compromised hosts to the Internet and from the Internet to the target. Our analysis of this SubSeven functionality has been confirmed by HeLLfiReZ, one of the authors of SubSeven.

1. Chronology of SubSeven

SubSeven (http://subseven.slak.org/) is a "remote administration tool" that allows an attacker to remotely control a compromised Windows 95/98 system. Version 1.0 appeared in late February 1999, and was followed by versions 1.1 through 2.1. These versions are compatible with Windows 95/98 systems only. The current version is SubSeven 2.1 Bonus, which was released in early June 2000. SubSeven 2.2 Beta #1 is already available, as well as a beta version of an NT-compatible SubSeven server (http://subseven.slak.org/beta/). A new Java-based client is also available, which only works with SubSeven 2.2 servers (http://www.sub7java.com/). SubSeven is referred to as BackDoor-G by some anti-virus vendors.

SubSeven is a feature rich application, comparable in quality to various commercial products, although many may resent this comparison. The later SubSeven versions (since version 1.7 or so) have been very reliable—during the hundreds of hours of research for this paper, no significant software errors or crashes were observed. SubSeven also contains features that most commercial remote administration tools do not have. This includes the ability to open and close the CD tray, play sounds, invert the screen image, lock the keyboard, log all keystrokes, monitor ICQ and IRC chats, and grab cached passwords. This is the type of "non-legitimate" functionality that many people point to when classifying SubSeven as simply "a hacker tool."

SubSeven's feature set has increased over time. Among other features, it is possible to:

- Set a server's access password
- Change the filename used by the server (the name of the executable)
- Change the registry keys used (the default are in Run and RunServices in HKLocalMachine\Software\Microsoft\Windows\CurrentVersion)
- Direct the server to use win.ini and system.ini (with "shell = <file name>") to restart after a reboot
- Direct the server to contact an IRC channel or ICQ address each time it starts up

The latest SubSeven distribution includes the following components:

- The SubSeven Server
- The SubSeven Client

- EditServer (for pre-configuring a SubSeven distribution, hereinafter referred to as a 'variant')
- Various readme files

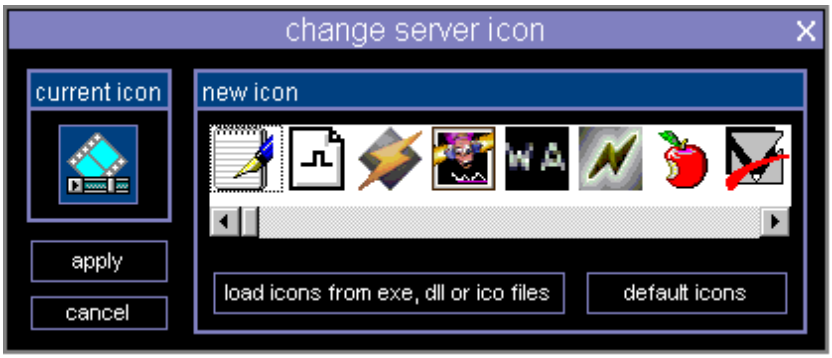
The SubSeven server (the part that runs on the compromised host), beginning with version 2.0 released early this year, also includes an IRC (Internet Relay Chat) "bot." This IRC bot is usually pre-configured (by the attacker) to connect to a specific IRC server and channel using a specific nickname and (optional) channel key. After connecting, the bot can monitor the channel, looking for specific strings and interpreting them as commands to perform certain functions. Most of these functions are described in the SubSeven documentation (e.g., http://subseven.slak.org/bothelptext.txt). However, at least two undocumented commands have been added within the last six months. These are the "ping" command (i.e., "ping <host>") and the "mping" command (i.e., "mping <host> <ping size> <number of pings>"). It is this mping command that provides rudimentary distributed attack capabilities. An mping attack (i.e., a ping flood) of thousands of very large ping packets sent from a few thousand SubSeven servers can easily cause service disruptions for the average business or home user (e.g., see http://www.insecure.org/sploits/ping-o-death.html).

A member of the SubSeven developers group, contacted via e-mail on 06/13/2000, stated the following regarding the unpublished mping functionality:

> Well the mping was first added to irc bots (drones) just after new year in SubSeven Gold edition so is not new by any means. The idea for inclusion came originally from me and was included in the spec i wrote for subseven bots but was not included until later versions and was only included as mping as to add more would be too irresponsible and give too much power to people that would most probably misuse. The mping was largely not publicized for those reasons I mention above. SubSeven is an ongoing development and will be for the forseeable future. We see it as a learning and development process and constantly break new ground. We do not include all that we could due to the fact we need to keep a critical eye on server size etc and possible damage or misuse. While we are not responsible for what people do with it we still like to make sure thay cannot do too much damage by including too many possibly destructive features like format hard drive etc.
> Regards HeLLfiReZ for and on behalf of SubSeven and SubSeven Crew Members.

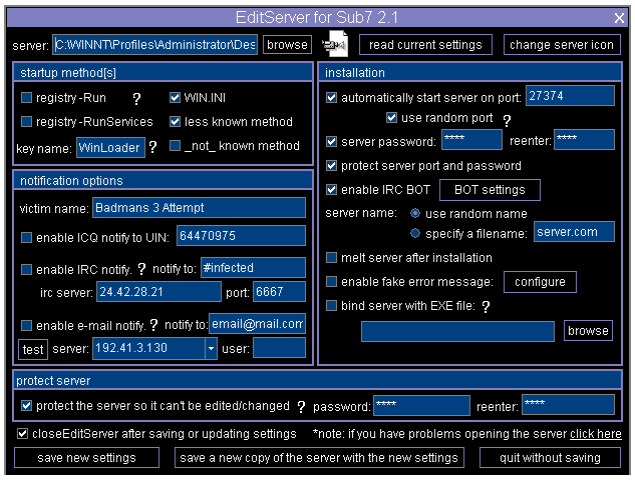
Clearly, if the mping functionality were extended to spoof originating IP addresses, then the ping traffic from many compromised hosts could be directed through "smurf amplifiers" in order to dramatically increase its effectiveness against the victim (i.e., the host, router, web server, etc. corresponding to the spoofed IP address). Smurf amplifiers are easily found at locations such as http://www.powertech.no/smurf/ and http://netscan.org/. Note, however, that properly placed traffic egress filters would eliminate this particular threat (as would the clean up of networks that allow ping traffic to broadcast addresses).

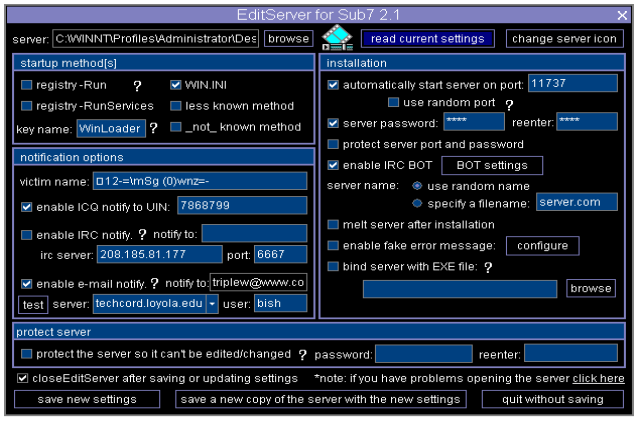
The most recent SubSeven variant was publicized on 06/08/2000 by NETSEC (http://www.netsec.net), who dubbed it the 'Serbian Badman Trojan', and shared a copy with iDEFENSE for analysis. iDEFENSE examined that variant (which happened to be named wuyiwekxb.exe and displayed the grey movie camera icon commonly associated with .avi files) and found it to be an executable file that had been packed using UPX (http://wildsau.idv.uni-linz.ac.at/mfx/upx.html). Upon execution, wuyiwekxb.exe unpacked itself, placed the SubSeven 2.1 server (which is also packed) into C:\Windows, and modified two system files. This specific installation of SubSeven was used in the tests described below. iDEFENSE also examined a copy of MySissy.mpg.exe, which used a movie icon. These icons can be easily changed through the SubSeven client interface.



2. The Stages of SubSeven Distribution

There are several ways for a host to become compromised by SubSeven, but the most prevalent method is a user overtly executing the application. For example, the user may be tricked into executing a file that looks like a .mpg rather than a .exe file, or may carelessly execute an e-mail attachment or a file received through IRC. Another method is an attacker placing SubSeven on a host compromised through alternate means (e.g., open file shares). The point is that SubSeven servers do not mysteriously appear on hosts. The following is one example of how hosts involved in the recent events may have been compromised and how an attacker can then use the compromised hosts to carry out a flood attack.

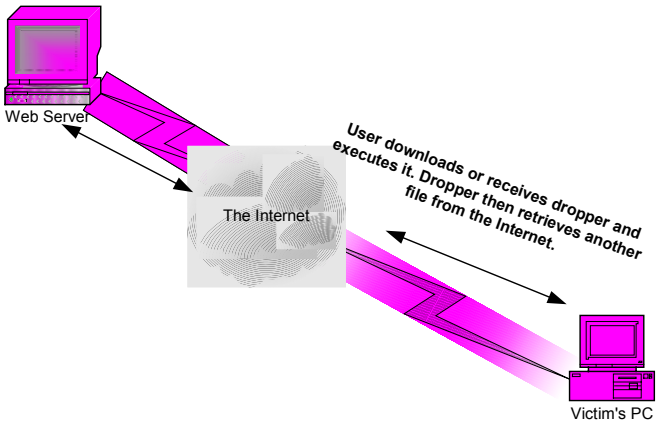




Stage 1: Pre-configuring a SubSeven Server
An attacker surfs to the SubSeven web site or one of its mirrors and downloads the latest version of SubSeven. The attacker uses SubSeven EditServer to access the server executable and change its default configuration. The attacker then saves this pre-configured variant of the server. Now the attacker builds or borrows a separate program and packs SubSeven into that new program (e.g., MySissy.mpg.exe). Then the attacker prepares a download site and an IRC server–either his own or otherwise legitimate locations that he uses for his own purposes. Now all the attacker has to do is find a few interesting ways to get people to download and execute his program.

As shown in the EditServer screens, there are several ways for an attacker to ensure that the SubSeven server will restart after a reboot. This includes entries in win.ini and/or system.ini, as well as entries in Run and/or RunServices under HKEYLM/Software/Microsoft/Windows/CurrentVersion. There are also a variety of notification options.

Stage 2: The Initial Delivery: Trojan.Downloader
In this scenario, a user first downloads (or receives in e-mail, etc.) what is advertised as a video file viewer, a site access enabler, or something equally enticing to the user. This file is actually a Trojan-known by various names such as Trojan.Downloader, Trojan.Win32.Loder.WPW, Dropper, and Maglo-whose function is to retrieve another file from the Internet. The user executes the dropper, which connects to an Internet server and downloads, in this case, QuickFlick.mpg.exe or MySissy.jpg.exe. Note that one site accessed in the recent events (http://www.lomag.net/~ryan1918) was taken down almost immediately and is no longer a threat (although the executable can probably be found in other locations).



Stage 3: Installing the SubSeven Trojan
QuickFlick.mpg.exe and MySissy.mpg.exe are packed executables that contain the SubSeven Trojan (which is itself a packed executable). Using a utility (such as UPX) to pack an executable not only reduces its size, but also hides some of the character strings and other clues within the executable file from the average user

who has a hex editor. However, it typically will not hide it from current anti-virus products (although there is always some small time lag between new malicious software being "in the wild" and signatures being developed by anti-virus companies and usually a larger time lag until users update their desktop software). Once QuickFlick.mpg.exe or MySissy.mpg.exe is executed, the SubSeven server executable is extracted, given a random character string as a file name (a behavior which may have led to early reports of "polymorphism"), placed in the c:\windows directory, and executed. In our tests, the SubSeven server extracted from MySissy.jpg.exe modified the win.ini file, but the SubSeven server extracted from wuyiwekxb.exe did not (it appeared that code within wuyiwekxb.exe itself made the changes to win.ini and system.ini).

Note that Windows 95/98 defaults to hiding extensions for known files types (e.g., .exe, .doc, .txt). Since both QuickFlick and MySissy have embedded icon types that are normally associated with movie files and since most users will only see QuickFlick.mpg and MySissy.mpg as the file name, there is a much lower chance that the deception will be noticed. However, all up-to-date anti-virus software (subject to the time lags discussed above) should detect SubSeven the moment it is unpacked from QuickFlick or MySissy and, with some sort of real-time auto-protect feature, should prevent it from ever executing.

Stage 4: SubSeven Awakens

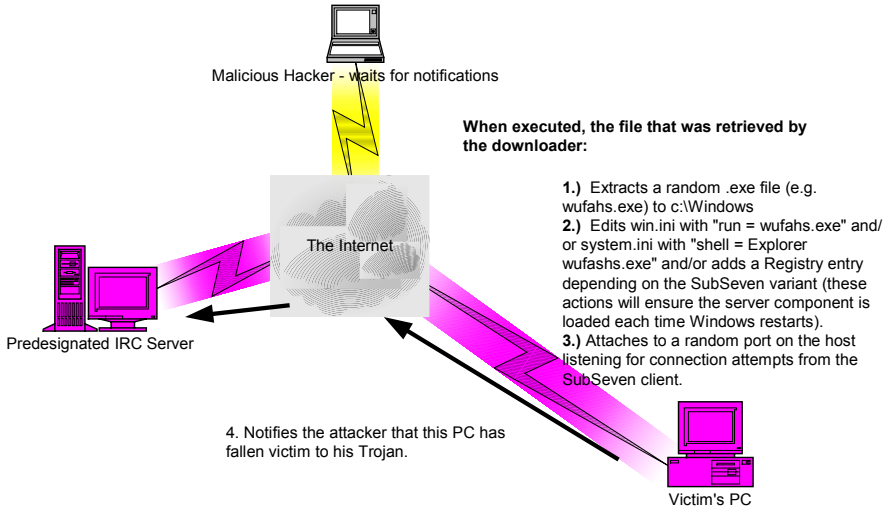
When the SubSeven server starts, it will follow the parameters in its pre-established configuration. One of the servers we examined binds itself to a random high-numbered port, sets its IRC command prefix to '-', and connects to an IRC server at 'bsvf.dhs.org' (which was IP address 64.65.17.188) on the channel '#badman' with the nickname 'BdMan' and the channel key 'bsvfowns'. If the nickname 'BdMan' is already in use, SubSeven will append some random characters to the name and try again (e.g., with 'BdManfghs').

When pre-configuring the SubSeven server, there are several ways that the attacker can configure automatic notification using the built in features of SubSeven 2.1.3 Bonus (the latest distribution). These include:

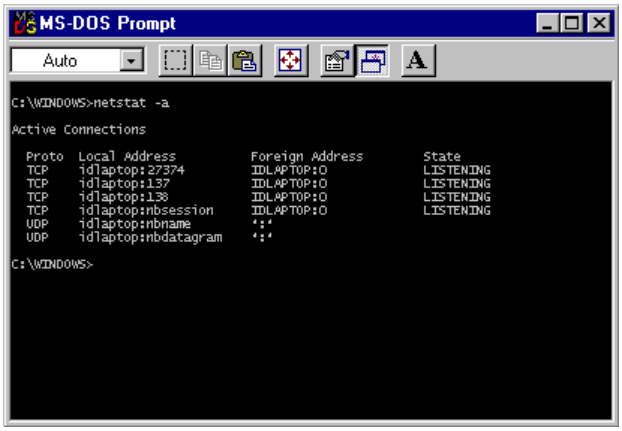
- launching an IRC bot that connects to an IRC server on a specific port
- sending an ICQ message
- sending an email

In each of these cases, the essential information that is transmitted includes the compromised host's IP address, the random or predefined port on which the SubSeven server is listening for connections, and the password needed to connect to the compromised host.

In this example, the notification technique is the use of an IRC bot to connect to port 2222 of an IRC server on bsvf.dhs.org.



Typing "`netstat -a`" at a Windows command prompt will reveal all active connections inbound and outbound from the host (assuming the netstat command hasn't been maliciously modified). Notice the suspicious open port on 27374 (in this example) listening for incoming connections. This is the SubSeven server component waiting for a SubSeven client connection from the Internet. In general, you should scrutinize all LISTENING or ESTABLISHED connections on ports above 1024.



Stage 5: The "Bots" Report for Duty

In this case, our bot's nick is BdMan. The bot joins a designated IRC channel known to the attacker and beings to actively listen for certain keywords. Once the attacker logs into the IRC server and finds one or more bots, he can then start to interact with them.

The IRC log below shows the bot has joined the #badman channel and is waiting for the proper activation commands. The hacker (who has cleverly nicknamed himself 'hacker' in this example) is already waiting in the channel and issues some commands after the bot has connected. To cause the bot to respond to additional commands, he first must offer the password that was set by the attacker before the Trojan was distributed (which was '0dy' [zero-d-y] in the code we examined). After receiving the "-login <password>" command, the bot is then ready to respond to other commands it sees in the IRC channel. The attacker then uses the "-info" command to cause the bot (and all other bots that accepted the login string) to display the SubSeven server connection information for the compromised host (i.e., IP address, port, password, etc.). Now the attacker has enough information to try to connect to the compromised host directly using the SubSeven client. In our case, the server password was "yugo".

```
*** on channels: #badman
*** on irc via server localhost.idefense.com (our irc daemon)
*** hacker (~hacker@10.1.1.37) has joined channel #badman
*** BdMan (~bot@10.1.1.50) has joined channel #badman
> -login 0dy
*BdMan* password accepted
> -info
<BdMan> Sub7Server v.M.U.I.E. 2.1 installed on port: 27372, ip:
10.1.1.50 - +victim: Badmans 3 Attempt - password: yugo
> -mping 12.3.4.5 56 10
<BdMan> pinging: 12.3.4.5
<BdMan> pinging finished.
```

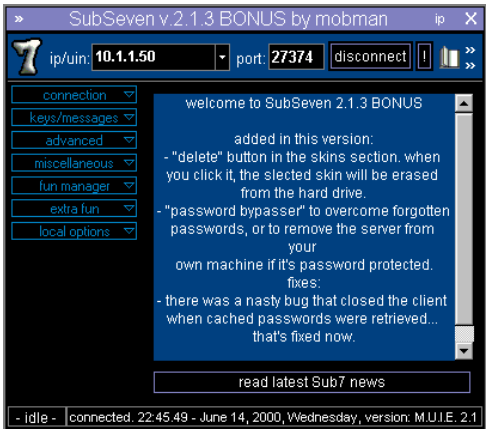
Of course, all of this roundabout activity through IRC would not be necessary in the case where an attacker knowingly placed a pre-configured SubSeven server on a host compromised through other methods and only wanted to control that one host. However, a well-configured firewall will likely stop the unsolicited incoming connection.

In our example, the attacker now uses the undocumented "-mping" command to cause the compromised host to send 10 packets of 56 bytes each to the IP address 12.3.4.5. **Now consider that there are possibly thousands of bots logged into this channel when this command is given and that the command could also have been '-mping 12.3.4.5 65500 1000000', in effect causing a large, distributed burst of traffic to be sent to the target IP address.** This feature of SubSeven effectively empowers an attacker to perform distributed ping flood attacks, and has been widely overlooked. This is not to say that the attack will always be successful, but simply that it can happen.

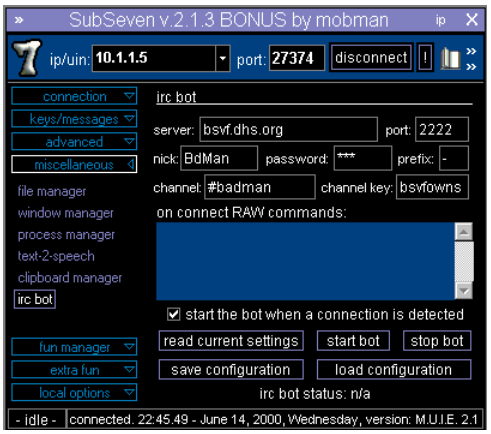
In our tests, a single Pentium 233MHz laptop generated a sustained traffic rate of 1.8 Mbits per second across a local LAN after receiving the command '-mping 12.3.4.5 65500 100000'. Note that the maximum ping packet size allowed by SubSeven is 65,500 bytes, although it is almost certainly possible to patch the code to allow larger packets.

Stage 6: A SubSeven Client Connection is Achieved

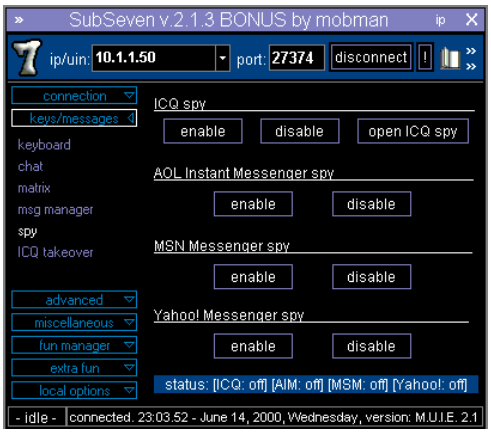
At this point, the IRC bot, ICQ message, and/or email have given the attacker all the info he needs to try a SubSeven client connection to the victim. The attacker brings up the client window, enters the compromised host's information, and attempts to connect. There are several reasons why the connection may not be successful including the host being down, the user having detected SubSeven and removed it, and a firewall not allowing the unsolicited incoming connection. If a connection is made and the (optional) password is entered correctly, the attacker has full control of the compromised host.



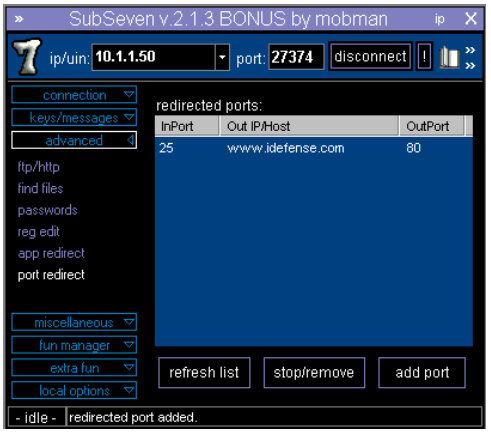
Now that the attacker is connected, he can reconfigure the IRC bot's behavior using the graphical interface.



The attacker truly has full control of the compromised host and the victim's privacy.



The attacker can even use the compromised host as a relay point for malicious traffic.



3. Mitigation

Be reasonably paranoid
Users should avoid opening files from unknown or untrustworthy sites. Equal skepticism should be applied to unsolicited e-mail attachments. Home and small office users with "always on" xDSL or cable modems should invest in personal firewall software that can block unsolicited inbound connections (ingress filtering) before they reach machines on the internal network. Any unauthorized connection attempts should be logged, reviewed, and reported appropriately.

Use current anti-virus software
Unsolicited e-mail attachments and files downloaded from questionable web sites should not be opened or run unless they have been scanned by current anti-virus software. The SubSeven Trojan is easily detected by up to date anti-virus scanning tools, which are available from a number of sources. Users should purchase anti-virus software featuring a regular update service. Automatic protection features that examine files as they are being accessed should be enabled in order to catch malicious software that has been compressed or encoded.

Enable egress filtering & logging
Egress filtering has also become a necessary evil. Outbound connections should be limited to the minimum necessary ports and services needed, and spoofed IP addresses should be blocked. All other connection attempts should be blocked and also logged for review and analysis.

This document is a product of iDEFENSE

Version 1.0, June 16, 2000

For additional information, please send e-mail to:

EccentricLabs@idefense.com

Or telephone us at:

(703) 914-9400