Global Information Assurance Certification Paper

SANS Practical Assignment for Advanced Incident Handling and Hacker Exploits - SANS Network Security 2000
Submitted by Patrick Prue

Exploit details:

Name:	Deep Throat V3.1
Aliases:	Win32.DeepThroat, DTV2 , Backdoor-J.Srv, Backdoor-J.cli
Variants:	F0rePlay , Reduced F0replay
Advisories:	X-Force Backdoor III Advisory , 2290
CERT :	CA-1999-02 (Backdoor Related)
Operating System:	Systems running Microsoft Operating Systems Prior to Windows 2000
Protocols/Services:	41, 999, 2140 (UDP), 3150 (UDP), 6670, 6771, 60000
Brief Description:	Remote Administration Trojan similar to Back Orifice and Netbus

Introduction :

A programmer going by the nickname of ^Cold^ released a Windows95 / Windows98 Trojan horse program named "Deep Throat" in October 1999.The Deep Throat Trojan consists of a client program called "Deep Throat Remote Control" which is run on a remote computer to gain access to any computer connected to a TCP/IP network or the internet. An executable server program is required to be installed on the victim's computer to permit the remote site access to the victim's computer in a manner similar to Netbus, Back Orifice and other internet "Remote administration" Trojan horses. This program exploits security vulnerabilities in the Windows95 and Windows98 platforms. It failed to operate on NT machines in its early releases but version 2 and above make NT susceptible to infection in the most basic forms although most other than the basic functions fail to operate.

Description of variants

Other than versions of DeepThroat there are prevalent variants are F0rePlay and Reduced F0rePlay.

Reduced F0rePlay server was found mostly in the "wild" as a bound application in WinNuke Extreme

Both of these variants are basically stripped down DeepThroat 1.0 Servers which contain very basic DeepThroat Functionality:

- **FTP Server**
- Change FTP server port
- Delete file
- Make Directory
- Reboot
- Run file
- Run file invisible
- Close server

The F0replay variants only listen on port 6670 which is not changeable, and is not effected by Master password settings as DeepThroat is. F0replay installs itself as systray.exe in the Windows Directory and Autoloads via the registry keys - HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion \Run\ *Key:* Systemtray

Additional Information on F0replay can be found at

http://www.dark-e.com/archive/trojans/foreplay/index.html

SOURCE CODE –

DeepThroat is written in Delphi Version 4

The source code for the 3.1 client and server are available at www.megasecurity.org/~masterrat/Sources/

How It Works ?

The Hack

Objective: Getting the potential victim to install the server onto his/her system.

Method 1

Send the server file (for explanation purposes we'll call the file server.exe) to you via E-Mail. This was how it was originally done. The hacker would claim the file to be a game of some sort. When you then double click on the file, the result is nothing. You don't see anything. **(Very Suspicious)**

Note: (How many times have you double clicked on a file someone has sent you and it apparently did nothing)

At this point what has happened is the server has now been installed on your system. All the "hacker" has to do is use the Deepthroat Client to connect to your system and everything you have on your system is now accessible to this "hacker."

With increasing awareness of the use of Trojans, "hackers" became smarter, hence method 2.

Method 2

Objective: Getting you to install the server on your system.

Let's see, how many of you receive games from friends?

Games like hit gates in the face with a pie. Perhaps the game shoot Saddam? There are lots of funny little files like that.

Now I'll show you how someone intent on getting access to your computer can use that against you.

There are utility programs (Binders) available that can combine the ("server" (a.k.a. Trojan)) file with a legitimate "executable file." (An executable file is any file ending in .exe). It will then output another (.exe) file of some kind. Think of this process as mixing poison in a drink.

For Example:

Tomato Juice + Poison = something

Now the result is not really Tomato Juice anymore but you can call it whatever you want. Same procedure goes for combining the Trojan with another file.

For Example:

The "Hacker" in question would do this: (for demonstration purposes we'll use a chess game)

Name: chess.exe (name of file that starts the chess game)

Trojan: Trojan.exe (Deep Throat Server)

The joiner utility will combine the two files together and output

1 executable file called: **<insert name here>.exe**
This file can then be renamed back to chess.exe. It's not exactly the same Chess Game. It's like the Tomato Juice, it's just slightly different.

The difference in these files will be noticed in their size.
The original file: chess.exe size: 50,000 bytes
The new file (with Trojan): chess.exe size: 65,000 bytes
(Note: These numbers and figures are just for explanation purposes only)
The process of joining the two files, takes about 10 seconds to get done. Now the "hacker" has a new chess file to send out with the Trojan in it.

The unsuspecting user receives my new chess program and double clicks the executable , the chess program starts like normal. No more suspicion because the file did something. The only difference is while the chess program starts the Trojan also gets installed on your system.
Now you receive an email with the attachment except in the format of chess.exe.
The unsuspecting will execute the file and see a chess game.
Meanwhile in the background the "Trojan" gets silently installed on your computer.

Common Distribution Techniques

News Groups:
By posting articles in newsgroups with file attachments like (mypic.exe) in adult newsgroups are almost guaranteed to have someone fall victim.

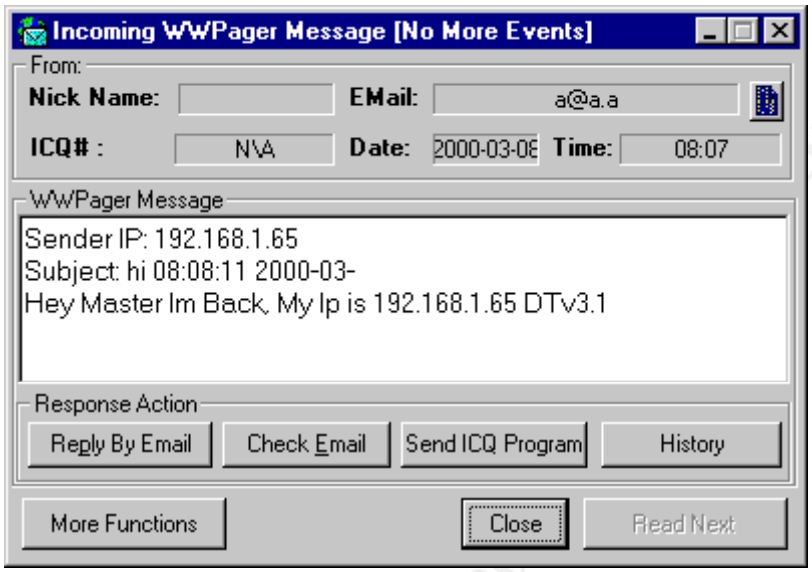
Grapevine:
Unfortunately there is no way to control this effect. You receive the file from a friend who received it from a friend etc.
etc.

Email:
The most widely used delivery method. It can be sent as an attachment in an email addressed to you.

Unsafe Web sites:
Web sites that are not "above the table" so to speak. Files downloaded from such places should always be accepted with high suspicion.

IRC:
On IRC servers sometimes when you join a channel you will automatically get sent a file like "mypic.exe" or sexy.exe" or sexy.jpg.vbs something to that effect. Usually you'll find "script kiddies" or previously infected persons are at fault for this.

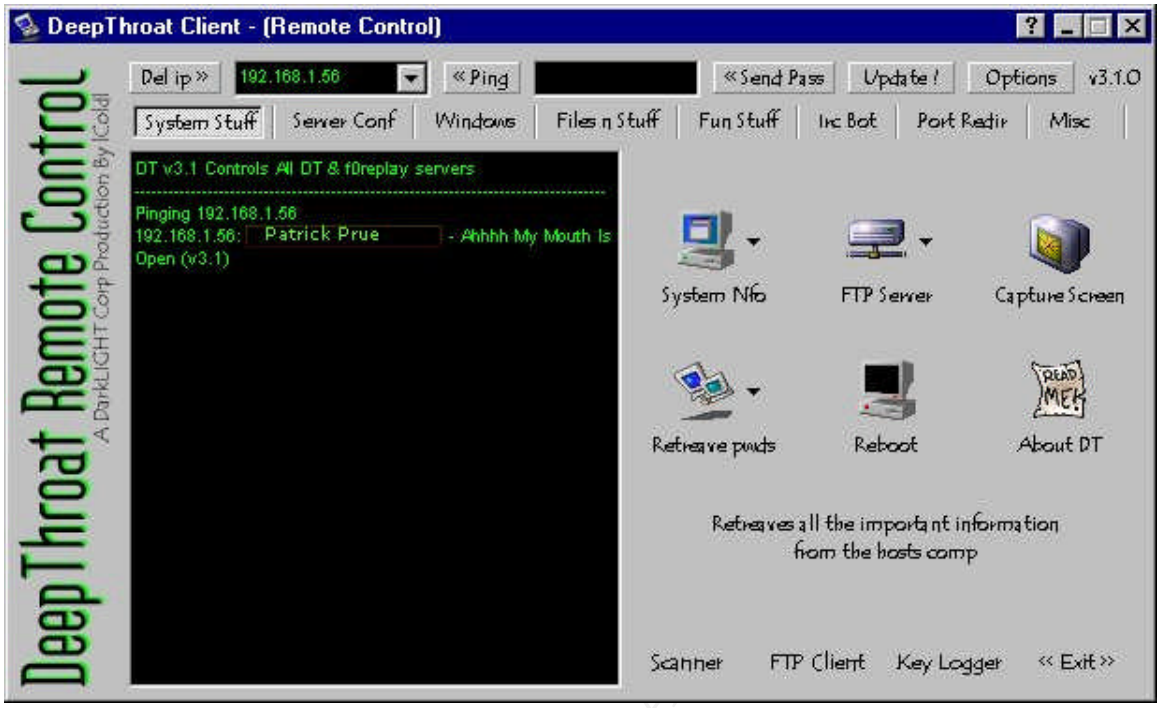
Once the Server is successfully installed the server can "phonehome" utilizing ICQ to alert the "hacker" that it was successfully installed and ready to proceed.



- ScreenShot taken from http://www.sans.org/y2k/DT.htm

Once the Server is in place or you have found an applicable victim on the network. You Fire up your client piece.

Connecting to your victim the Deep Throat Client first Pings the server with a 2 byte UDP packet to port 2140 to elicit a version response as below.



Once connected to the victim you have at your disposal a wealth of tools.

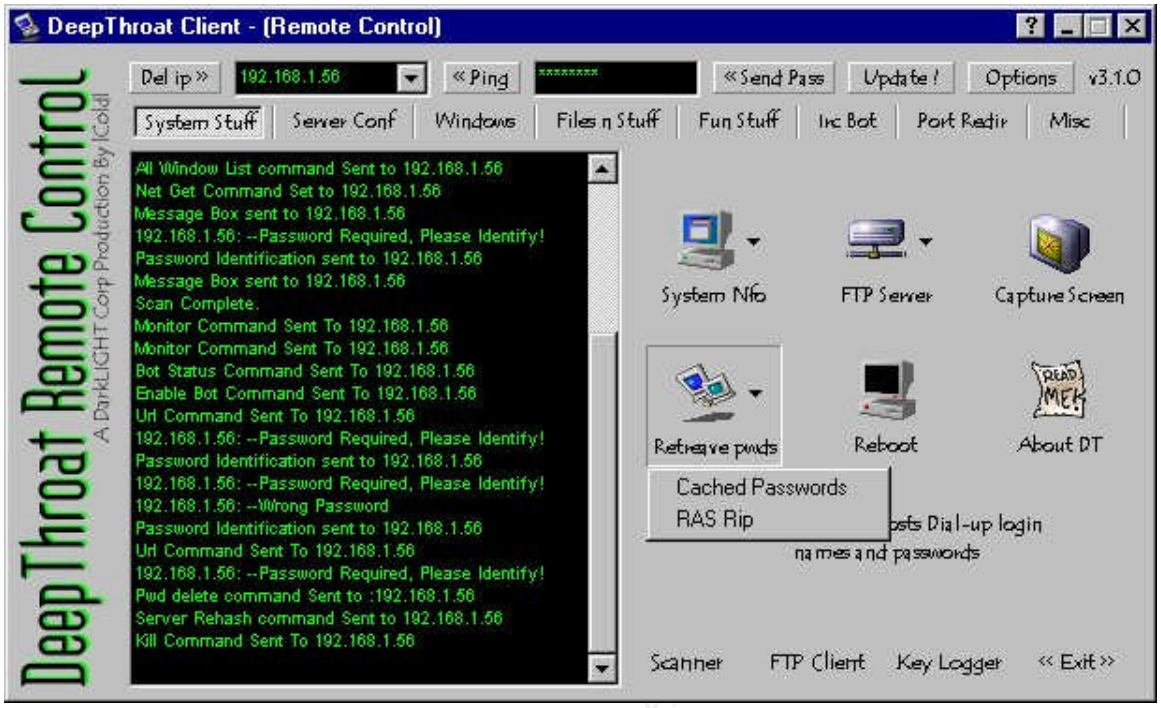
System NFO Button allows Access to – System Information (Registered User, Serial Number etc.), Drive Information, Server Status and Email Information

FTP Server – Allows to Enable / Disable the Server and to also change the listening Port (Which is 41 by default)

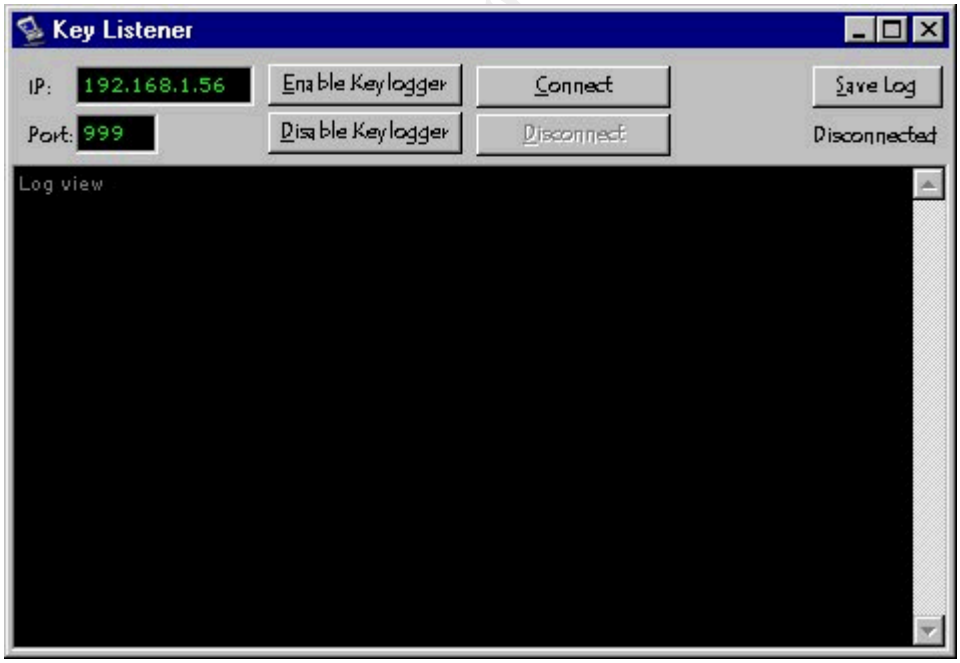
Capture Screen – Does a Screen Capture of the Server Host Machine

Reboot – Resets the Host Computer

Retrieve Pwds – Allows Retrieval of Cached Passwords from the Registry and also RAS Saved Passwords

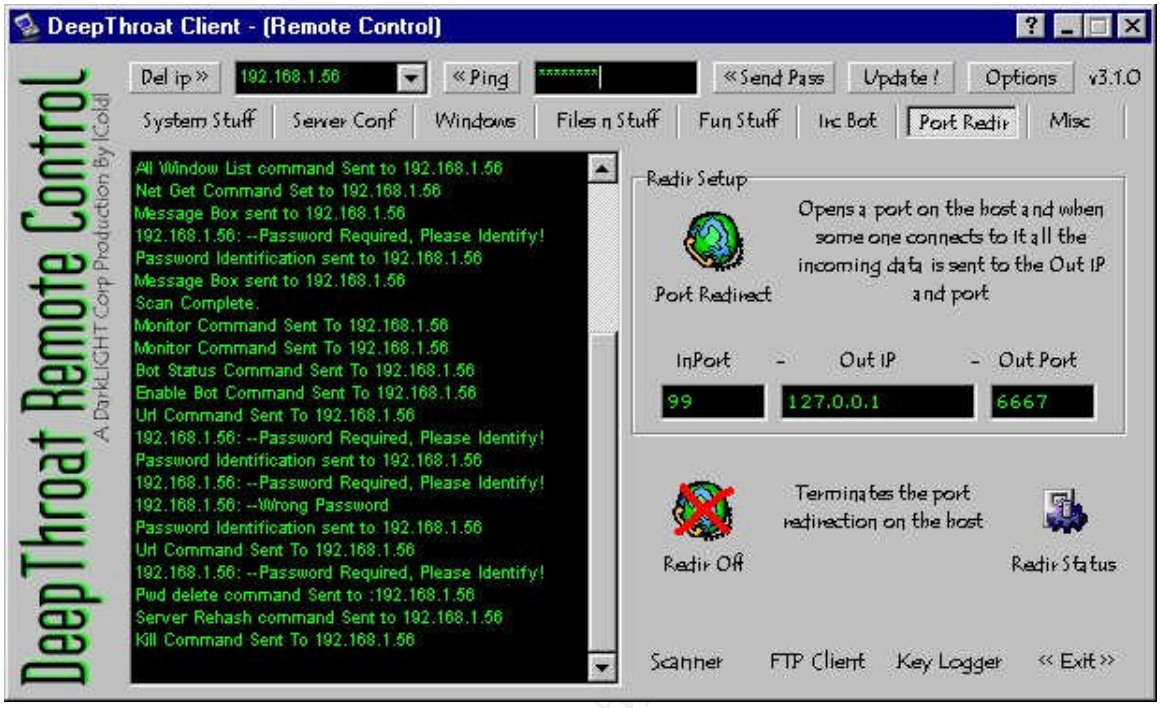


Key Logger Function Listens to by default Port TCP 999.When enabled it records all keystrokes on the victim machine.



Port Redirection Functionality allows for the "hacker " to use the victim machine as Bounce to IRC out of, a very popular thing to do from a compromised host. Usually implemented by Bnc.tar on Unix operating

systems.



Deep Throat also contains an IRC Bot Functionality that will connect to determined Irc Server to a channel (i.e. #hacked) using a nickname set on the server side. If the connection is unsuccessful (Nick in use) it will add some random characters to the end of the nick in order to connect to the channel.