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
"Hacker Tools, Techniques, and Incident Handling (Security 504)"
at http://www.giac.org/registration/gcih

OPTIXPRO 1.31 and NETDEVIL1.5 TROJAN BACKDOOR EXPOLITS

GCIH Practical Assignment

By Sherman Hung
February 26, 2004

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

TABLE OF CONTENTS

PART 1 – ABSTRACT…… 4

PART 2 - THE TROJAN HORSES…….....…… 5

Backdoor Trojan…… 5

The Programs Used in the Exploit……...…… 5

Threats of the Trojan Horses…… 9

Operating Systems…….. 10

Protocols/Services/Applications…… 11

PART 3 – RECONNAISSANCE/SCANNING…… 12

PART 4 - EXPLOITING THE SYSTEM…… 14

Network Settings…….. 14

The Exploit Scenario…… 16

Net Devil Exploit……..…… 17

Exploit Step by Step…… 17

Signature Verification …… 21

Gaining Access…….. 23

OptixPro Exploit…… 24

Exploit Step by Step…… 24

Signature Verification …… 31

Gaining Access…… 33

Summary of the Exploits…….. 40

PART 5 – KEEPING ACCESS AND COVERING TRACKS…… 42

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

PART 6- THE INCIDENT HANDLING PROCESS …….. 44

Preparation …….. 44

Identification ……. 49

Containment ……. 51

Eradication …….. 52

Recovery …….. 53

Lessons Learned……. 53

PART 7 - CONCLUSION……. 55

PART 8 - REFERENCE……. 56

© SANS Institute 2004, Author retains full rights

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

PART 1 – ABSTRACT

This paper was submitted to fulfill the partial requirement of the GIAC Certified Incident Handler Certification (GCIH).

I attended the SANS Institute's "Hacker Techniques, Exploits and Incident Handling" class in Los Angeles on September 2003. I was impressed with how the backdoor Trojan can be used to exploit networks. During my research, I found a website (see Exhibit 1) that had a public poll for a list of nine different Trojans. The top three on the scoreboard were Sub7, Net Devil 1.5, and OptixPro 1.31. Since Sub7 has been covered in other papers, I decided to explore Net Devil and OptixPro as my research topic.

The objective of this paper was to exploit a simulated network using Net Devil 1.5 and OptixPro 1.31, and then apply incident handling procedures to recover the infected computer. Windows Server 2003 was installed on the network server. An additional test was conducted to verify whether both Trojans survived on the new operating system.

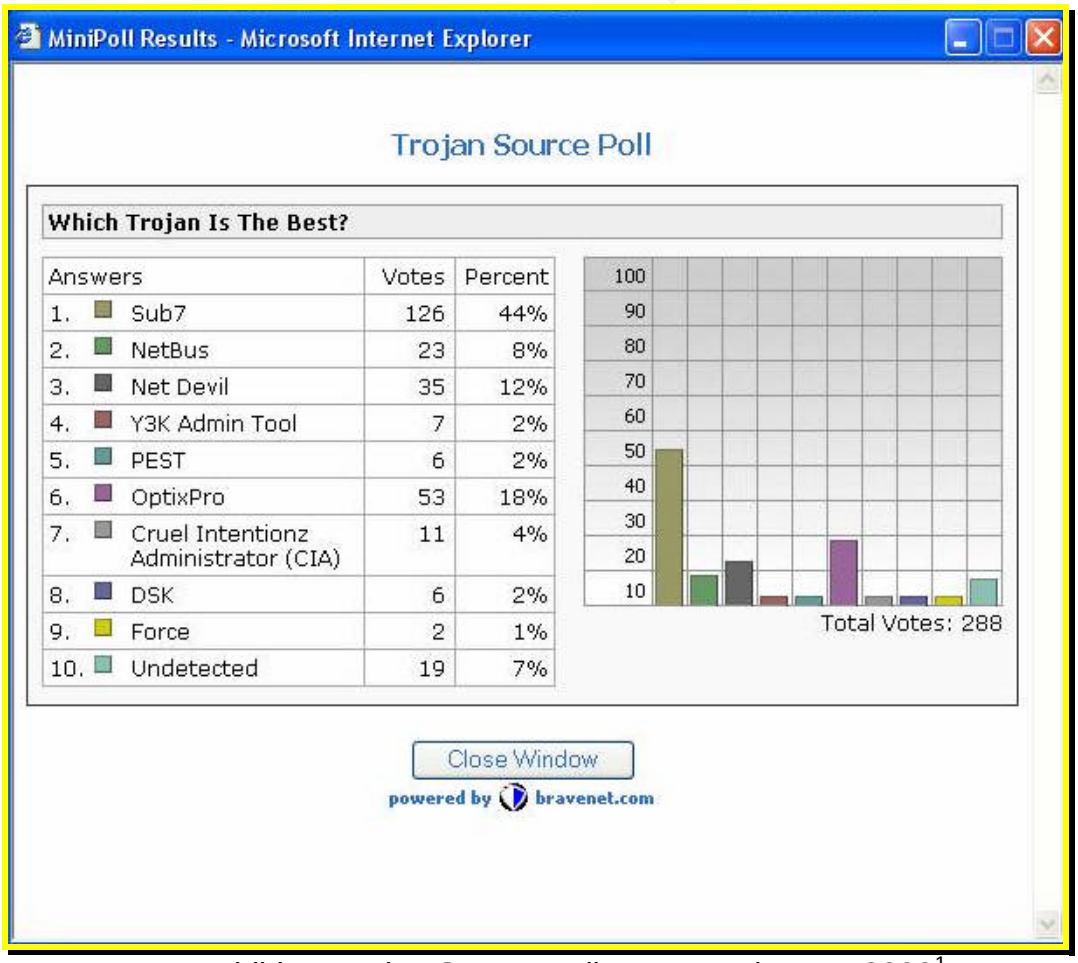


Exhibit 1. Trojan Source Poll on December 11, 2003[1]

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

PART 2 – THE TROJANS HORSES

Backdoor Trojan

According to TrendMicro, "a backdoor Trojan is a program that opens secret access to systems, and is often used to bypass system security. A Backdoor program does not infect other host files, but nearly all backdoor programs make registry modifications." [2]

The Programs Used in the Exploit

Five programs were used in the exploit: Net Devil 1.5, OptixPro 1.31, WinRAR, Tiny Personal Firewall 5.0, and eLiteWrap. The detailed descriptions of these programs are listed below:

<u>Net Devil 1.5</u>

Net Devil, a backdoor Trojan, was written by Nilez. It was first found in June 2002. No CVE was noted. Several versions of this Trojan were released. In version 1.5, a better GUI and icons were added to make it more user-friendly. According to Symantec, when the Net Devil runs on a victim machine, it performs the following tasks to take control:

1. The Trojan locates the \Windows\System32 folder and copies itself to the folder. The default program name is kernel32bit.dll, but it is changeable by hackers.

2. "It adds a value that refers to the Trojan program to one of the following registry keys:

   HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run
   HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices." [3]

3. "When a hacker creates the server file, Net Devil can be configured to perform the following hacking tasks to a victim machine:

   - Display a fake error message to conceal its true purposes.
   - Choose the ports that are used by the backdoor to communicate with the hacker. By default, it uses port 901 for direct control, port 902 for communicating logged keystrokes, and port 903 for file transfer.
   - Use different notification methods such as sending an email and cgi notification in order to give information to the hacker about the compromised computer.
   - Attempt to kill running firewall and anti-virus services. This is a very interesting feature and was tested in this exploit." [4]

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

OptixPro 1.31

OptixPro, another backdoor Trojan, was first written in Borland Delphi. No CVE was reported as of date. It uses a server program to infect the target system, a client program to access the infected system, and a server editor program to configure the server program at the hacker's machine. Once the server program infects the target system, the hacker, at a remote site, runs the client to exploit the victim machine.

OptixPro has been reputed to continuously provide upgrades to fight against antivirus patches. OptixPro has the following versions: version 10, 10c, 11, 12, 13, 14, and 15.

The OptixPro has powerful features that can be used to upload, download files, log keystrokes, kill anti-virus and firewall software, etc. Specifically, the OptixPro 1.31 has the following functions, according to Symantec:

1. Files
   OptixPro 1.31 copies itself to the System32 folder. The program name is changeable at hacker's choice.

2. Registry changes
   "OptixPro 1.31 creates a string value under the registry keys:

   HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
   HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServices

   so that OptixPro 1.31 is executed each time Windows is started." [5]

3. Ports
   OptixPro 1.31 opens a listening port on 3410. (This is the default port, but the attacker can set to any other port.)

The Wrapper: eLiteWrap

eLiteWrap is an EXE wrapper, "used to pack programs into an archive executable program that can extract and execute the packed programs in a hidden mode."[6]

The advantages eLiteWrap has over other common self-extractor programs wrappers are:

1. "eLiteWrap has the ability to start any number of programs contained in the pack file or extant on the user's system."[7]

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

2. "Programs (packed and external) can be started visibly or hidden from the user."[8]

3. "Programs that do not require user input can be started completely hidden from the user."[9]

4. "Programs can be started synchronously or asynchronously. Running a program synchronously allows programs to run in a defined sequence. In other words, a program will wait for another program to finish before being executed. "[10]

5. Packed files are produced with a "professional-look" icon.

WinRAR

WinRAR is used to compress the wrapped programs including the Trojans and eLiteWrap. WinRAR has its own encryption that can bypass virus scans in Yahoo Mail and Microsoft Hotmail.

Tiny Personal Firewall (TPF) 5.00

Tiny Personal Firewall contains firewall and intrusion detection functions that work on the Windows Server 2003 platform.

In order to test the "kill firewall" features in the Net Devil and OptixPro, TPF was installed on the victim server to verify that it functions as it claims.

For the testing of "kill firewall", the original settings of the TPF were used and I did not go further to add more filter rules. The settings are listed below:

1. Network Security Rules (firewall filter): the original settings open the inbound and outbound ports, both TCP and UDP. (See Exhibit 1.2)

2. Intrusion Monitoring Rules: enable all the blocking rules including the one for backdoors. (See Exhibit 1.3)

3. Registry Access Rules: trust all the changes to these registries. (See Exhibit 1.4)

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

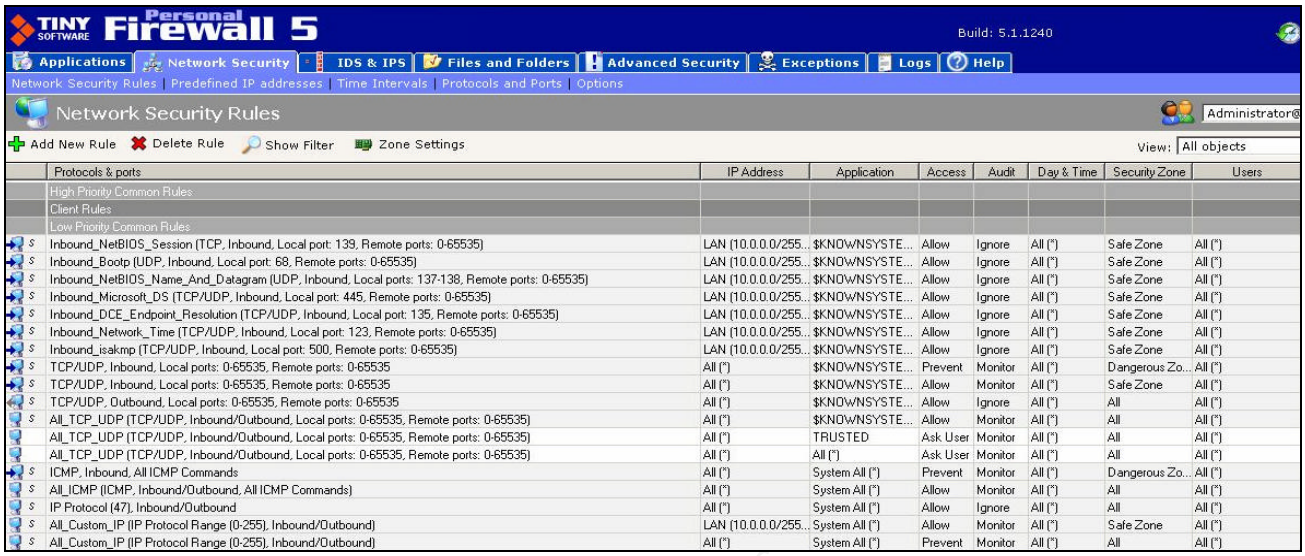


Exhibit 1.2 Network Security Rules of TPF 5

Exhibit 1.3 Intrusion Monitoring Rules of TPF 5

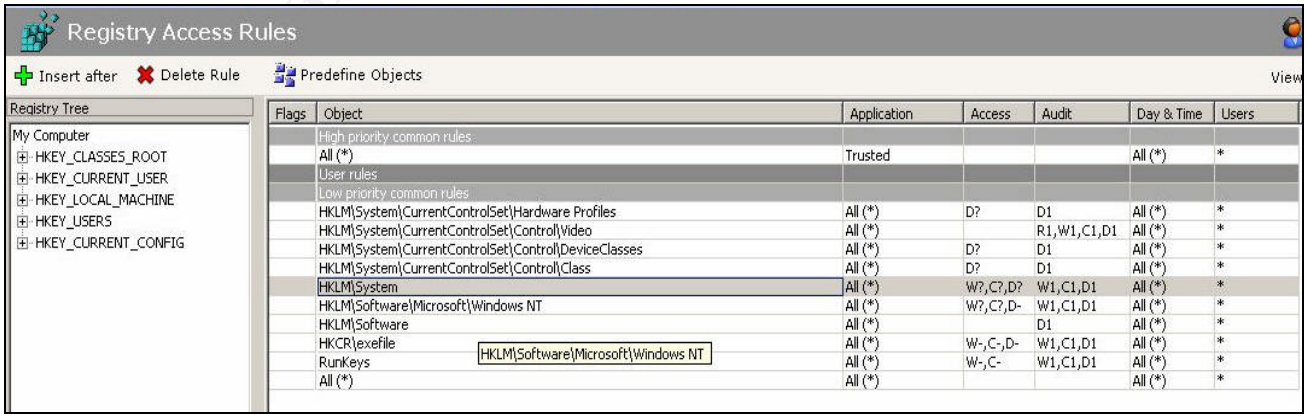


Exhibit 1.4 Registry Access Rules of TPF 5

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Threats of the Trojan Horses

The threats of backdoor Trojans are similar to each other. First, they are wrapped with a legitimate-looking program and sent to a victim machine. When the "legitimate" program is executed, the Trojan is also executed, usually in a hidden mode. The Trojan then attaches itself to system folder and creates a registry entry to be executed at Windows startup. A good Trojan is determined by how stealthily it is executed at the victim machine without drawing forth attention.

Another factor to determine a good Trojan is by the functions it has. In this exploit, OptixPro has more functions than Net Devil. Both Trojans can be used to download, upload, execute programs on the victim machine, kill process, and log keystrokes. In addition, OptixPro provides port scanning, port redirect, stealing passwords and other functions that hackers may want.

Below are the details of how these two Trojans can harm an infected machine:

<u>Net Devil 1.5</u>

When the Net Devil runs, it allows the hacker to remotely take control over the victim computer. Net Devil allows a hacker to:

- "Obtain full control of the file system
- Upload files to and download files from the host computer
- Run files of the hacker's choice
- Kill running processes
- Display messages
- View the contents of the screen
- Log keystrokes
- Perform annoying actions: manipulating the mouse, opening and closing the CD-ROM drive, turning the monitor on and off, etc. "[11]

<u>OptixPro 1.31</u>

OptixPro 1.31 has more functions than Net Devil. The detailed functions are listed below:

"Power options:
- Log off the current user
- Reboot the system
- Shut down and suspend the system
- Crash the system

File system:
- Upload and download files

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

- Execute files
- Create folders
- Delete files and folders
- Rename files and folders

Processes:
- List running processes
- Stop running process

Registry:
- Create new values and keys
- Edit values
- Delete values and keys

FTP server:
- Launch an FTP server on a specified port

IP scanner:
- Launch a port scan from the compromised system for the open ports

Port redirection:
- Redirect connections to the compromised system on a specific port to another computer and port

System information:
- Acquire system information, such as the owner, OS version, CPU type, and speed
- Steal cached passwords
- Steal AIM passwords
- Steal RAS passwords

Other teasing and taunting inconveniences:
- Open and close the CD-ROM drive
- Show and hide the clock
- Turn the monitor on and off
- Start and stop the screensaver
- Enable and disable the mouse and keyboard
- Produce beeping sounds from the computer's speaker."[12]

Operating Systems

Both Net Devil 1.5 and OptixPro 1.31 can run on the following Windows versions:

- Windows 95
- Windows 98

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

- Windows NT
- Windows 2000
- Windows XP
- Windows Me

Please note that Windows Server 2003 was not on the above list. In this exploit, Server 2003 was installed on the victim machine to determine whether these two Trojans could survive in the new operating system.

Protocols/Services/Applications

The two Trojans used Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) ports to communicate between the Attack PC and the Victim Server. The port numbers can be specified at a hacker's discretion.

"TCP is a session-oriented communication protocol that requires a three-way handshake to establish a connection. Sequence numbers are used for TCP packet delivery to ensure a reliable transmission. TCP is the main protocol currently used in the Internet. The UNIX type operation systems use TCP as the communication protocol.

UDP does not have the three-way handshake and packet sequencing is not required. UDP is used for applications that value speed over reliable delivery such as voice or video transmissions."[13]

Both TCP and UDP have a total of 65,536 ports. A port is an entry point to access a system. Ports can be considered as a door or window to your system.

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

PART 3 – RECONNAISSANCE/SCANNING

The two Trojans can be sent through regular emails. The reconnaissance and scanning are performed to find out the victim's email address and operating system platform.

The reconnaissance step looks for victim's email addresses. Many companies have their own domain name, and the employee email addresses use patterns of first and last names, first initial and last names, or simply the first name. If a hacker knows the domain name, it is easy to try several common names like John Smith, John Andersen, John Thomas, etc. It would be surprising if a company did not have employees under these names. One other approach will be looking for a "Contact Us" link on a web page. The link usually brings up an email address to public relations representative of the company.

Another method of identifying email addresses is surfing on the company's executive page. On these types of pages, the names of the executives are usually listed. This should provide the hackers a fruitful list of names ranging from the Chairman to Executive Vice President.

After the email addresses are determined, the next step is to identify more company network information. Since both Trojans work only in Windows environments, other operating systems such as Linux and UNIX would not be viable exploit candidates.

If I am the hacker, I would definitely further research in the following areas:

1. Topology of the company's network. Cheops-ng would be a good tool for this type of purpose. Obtaining a network map of the Victim company would be necessary so that one can narrow down to target servers. Cheops-ng can be downloaded from http://cheops-ng.sourceforge.net/.

2. Obtain IP address of the victim's systems. The following Internet databases can be used to get IP addresses:

   - "American Registry For Internet Number (ARIN): www.arin.net.
   - Reseaux IP Europeans Network Coordination (RIPE NCC): www.ripe.net.
   - Asia Pacific Network Information Centre (APNIC): www.apnic.net.
   - Different Whois sites: www.allwhois.com and www.uwhois.com."[14]

   In addition to the above sites, Nmap ("Network Mapper") can be also used to find out the IP addresses if the web site name is known. Just type in the web site name and Nmap scan will return the IP address and open ports.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

4. Scan open ports. Open ports are crucial to make the Trojan backdoors to work. Both Nmap and Nessus are good tools for this type of purpose.

   "Nmap is a free open source utility for network exploration or security auditing. It is used to rapidly scan large networks. Nmap uses raw IP packets in novel ways to determine what hosts are available on the network, what services (application name and version) they are offering, what operating system (and OS version) they are running, what type of packet filters/firewalls are in use, and dozens of other characteristics. Nmap runs on most types of computers and both console and graphical versions are available. Nmap is free software, available with full source code."[15] Nmap is working on both Windows and UNIX platforms. Nmap can be downloaded from http://www.insecure.org/nmap/.

   Nessus is a free and open-source vulnerability scanner. It is used to remotely audit a network and determine open ports and other security vulnerabilities. It is working on both Windows and Unix Platforms. Nessus is very fast, reliable and allows user plug-in modules to add additional functions. At my workplace, we used Nessus to perform port scanning and vulnerability study on our IBM AIX networks. Nessus can be downloaded from http://www.nessus.org.

5 Does the company have firewall, intrusion detection and antivirus installed? This will determine the potential security controls the victim has implemented to fight with you.

   It is my experience that banking and financial institutions usually have tighter security control implementations because state and federal regulators have strict and specific requirements in this regards. Social engineering work can be used to obtain this type of information. For example, one could call up the firewall vendors and ask specific questions about the victim company. . .

6. General information security controls of the company. For example, does the company follow the industrial standards to change their password every 60 days? Are the administrator account passwords shared?

Up to this point, a hacker should have a very good idea who and where the victim is. The exploit will start here.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

PART 4 – EXPLOITING THE SYSTEM

Network Settings

A simulated network was set up for the exploit. The network components were quite simple: a hacker machine (Attack PC), a victim machine (Victim Server), and both were linked with an Internet broadband router (See Exhibit 2). The Attack PC and the Victim Server are considered as two machines in separate networks. The detailed configurations of the components are listed below:

Attack Computer
AMD Athlon XP 2600+
Speed 1.91 GHz
512 MB of RAM
DVD ROM
Pioneer DVD Burner A105
Microsoft XP Professional Version 2002 with Service Pack 1 patched.
Microsoft Office 2003
Norton Anti-Virus 2003 but was disabled.

Victim Server
Intel Pentium III processor
Speed 848 MHz
512 MB of RAM
DVD ROM
CD RW Drive
Microsoft Server 2003 Enterprise Edition with the following security patches applied (See Exhibit 1.5):

Status	Date	Description	Source
Successful	Saturday, November 15, 2003	**Cumulative Security Update for Internet Explorer for Windows Server 2003 (KB824145)**	Automatic update
Successful	Monday, October 20, 2003	**Security Update for Microsoft Windows (KB824141)**	Automatic update
Successful	Monday, October 20, 2003	**Security Update for Microsoft Windows (KB823182)**	Automatic update
Successful	Monday, October 20, 2003	**Security Update for Microsoft Windows Server 2003 (KB825119)**	Automatic update
Successful	Monday, October 20, 2003	**Security Update for Microsoft Windows Server 2003 (KB828035)**	Automatic update
Successful	Sunday, October 12, 2003	**DirectX 9.0b End-User Runtime** Read more...	Web site
Successful	Sunday, October 12, 2003	**Q282010: Recommended Update for Microsoft Jet 4.0 Service Pack 7 (SP7) – Windows Server 2003**	Web site
Failed	Saturday, October 04, 2003	**Flaw In Windows Media Player May Allow Media Library Access (819639)**	Web site
Successful	Saturday, October 04, 2003	**Security Update for Windows Server 2003 (819696)**	Web site
Successful	Saturday, October 04, 2003	**Security Update for Windows Server 2003 (KB824146)**	Web site
Successful	Saturday, October 04, 2003	**Security Update for Microsoft Windows (KB824105)**	Web site
Successful	Saturday, October 04, 2003	**Security Update for Windows Media Player (KB828026)**	Web site
Successful	Saturday, October 04, 2003	**823559: Security Update for Microsoft Windows**	Web site
Successful	Saturday, October 04, 2003	**October 2003, Cumulative Patch for Internet Explorer for Windows Server 2003 (KB828750)**	Web site

Exhibit 1.5 Security Patches applied to Windows 2003.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Internet Broadband Router
AirLink Internet Broadband Router with a WAN and four LAN ports. The Router is using IEEE 802.3 10 BaseT standards. The router has four auto-negotiation 10/100 Mbps RJ-45 switching ports. It supports TCP/IP, HTTP, and DHCP Server/Client network protocols.

There are two computers connected to the router:
The router gateway IP is 192.168.xxx.1
The Attack Computer's IP is 192.168.xxx.4
The Victim Server's IP is 192.168.xxx.5

The detailed support information of the router can be found at www.airlinkplus.com.

Cable Modem
A cable modem was used to facilitate the Internet connection. The cable modem was subscribed through a local Internet service provider in Southern California.

Iogear KVM
An Iogear two-port KVM was used to share monitor, keyboard and mouse between the two machines.

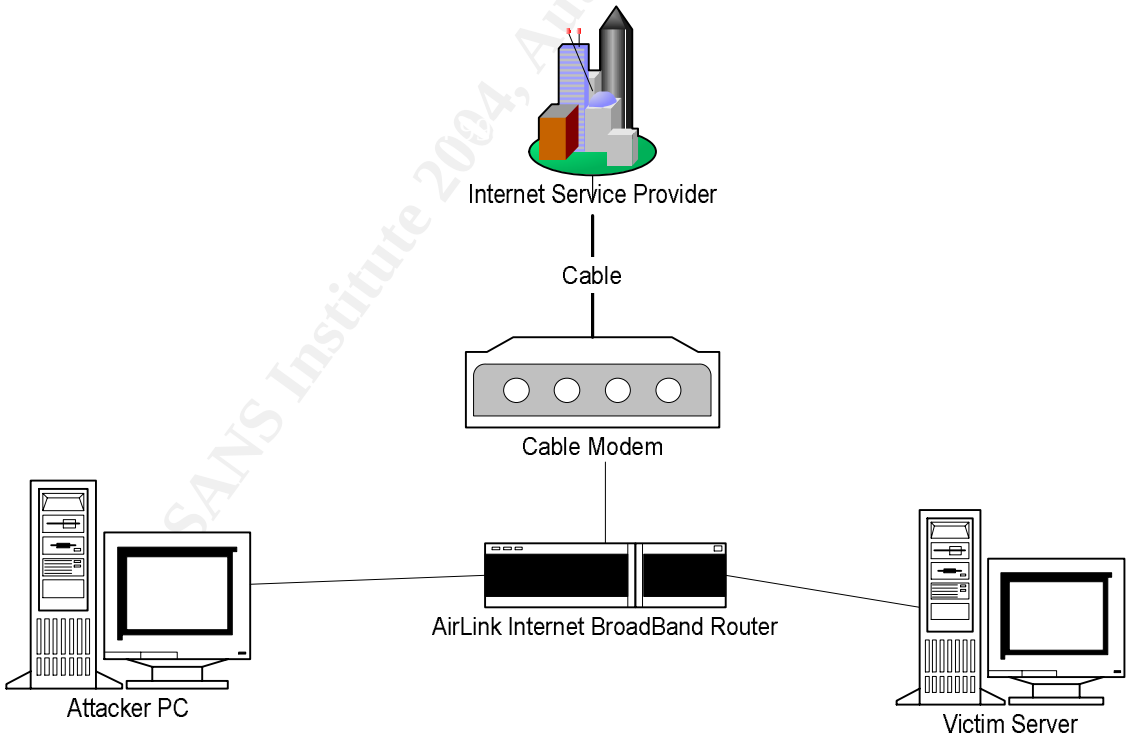


Exhibit 2. Network Settings

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

The Exploit Scenario

The goal of the exploit was to infect the Victim Server using Net Devil 1.5 and OptixPro 1.31 and then use these two Trojan backdoors to explore the resources on the Victim Server.

The following is the exploit scenario. The network included an "Attack PC" and a "Victim Server" (both names will be used for later references). The Trojans were wrapped with a program that was a visible runner. The hacker attached the wrapped Trojans in an email that was sent from the Attack PC to the Victim Server.

After the Victim Server was infected, the hacking activities were started. Acting as a hacker, I performed the following tasks:

1. Navigated the file systems, Process Manager, and Windows System folders.

2. Logged victim keystrokes including accounts and passwords.

3. Downloaded Windows SAM database.

4. Changed registry key values.

5. Played "ghost haunting" tasks such as opening the CD ROM Drive and shutting down the victim computer, etc.

Windows Server 2003 was just recently released. It is a good opportunity to verify whether both Trojans can survive on the new release.

Again, this is a simulated exercise. A few real life factors were not included in this exercise:

1. The network was simplified to have only the Attack PC and the Victim Server.

2. The Victim Server did not install enterprise antivirus software.

3. The Server 2003 was installed with the standard configurations and suggested patches. (See Exhibit 1.5, page 14.) No additional security mechanisms were implemented.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Net Devil Exploit
Exploit Step by Step

At each step, the location of the task being performed was indicated at the beginning of the paragraph.

1. Attack Machine:
   Turned off the Norton Antivirus 2003 on the Attack Machine.

2. Attack Machine:
   Downloaded the Net Devil 1.5 to the Attack Machine from www.geocities.com/trojansource_2003/. Unzipped it.

3. Attack Machine:
   Ran Edit-Server.exe to configure the server.exe program that would be later sent to the Victim Server. The configurations for the Server.exe are discussed below:

   a. General Section (see Exhibit 3)
      Chose the default server file name: "kernel32bit.dll". This file will be automatically saved to Windows\System32 when the Trojan is executed at the Victim Server.

      Specified the Main port to 65528, Keylog port to 65529, and Transfer port to 65530.

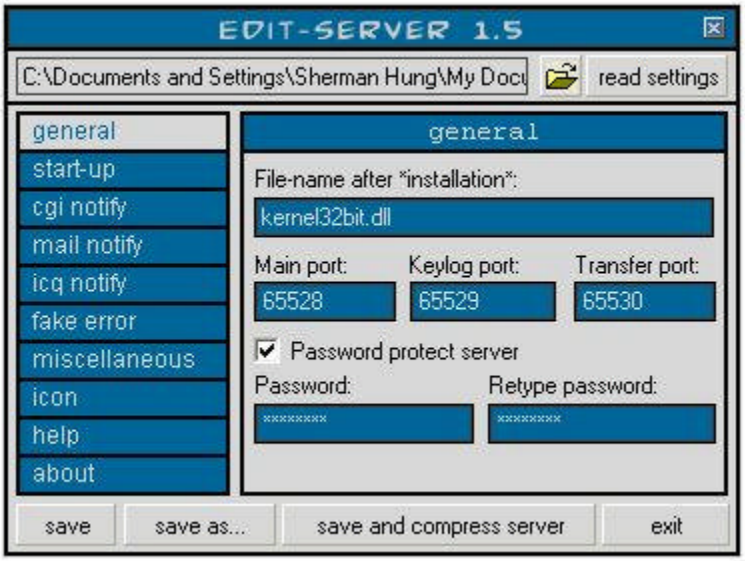


Exhibit 3. General Section of Net Devil Server.exe Configurations

   b. Start-up Section (see Exhibit 4)
      Selected "Registry – Run" to put an entry with the name "kernel32".

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

The entry appeared in the Windows registry
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run
when the server was later infected.

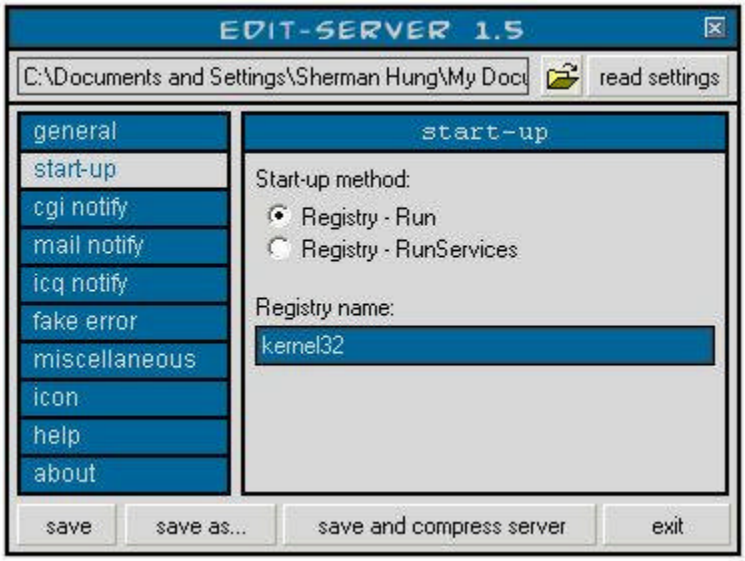


Exhibit 4. Start-up Section of the server.exe Configurations

c. Fake Error Section (see Exhibit 5)
Specified an error icon and followed the default message text. An error message will show up when the server.exe is executed at the Victim Server.

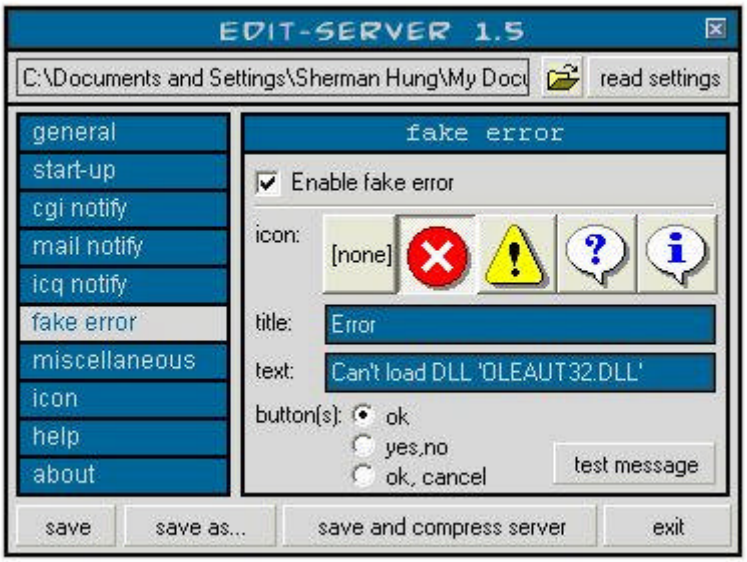


Exhibit 5. Fake-error Section of the server.exe Configuration

d. Miscellaneous Section (see Exhibit 6)

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Clicked on “Kill AV/Firewalls”, “Only open port when online”, and “Log pressed keys (offline keylogger)” options.

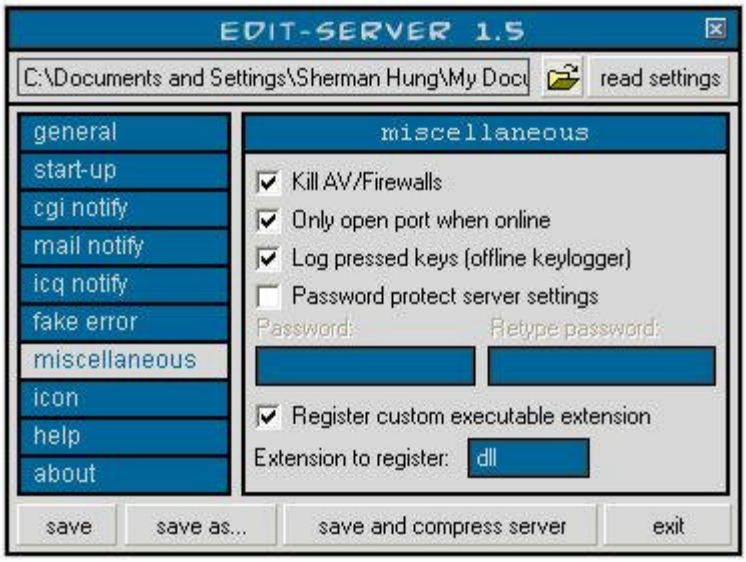


Exhibit 6. Miscellaneous Section of the server.exe Configurations

e. Icon Section (see Exhibit 7)
Selected an icon for the kernel32bit.dll.

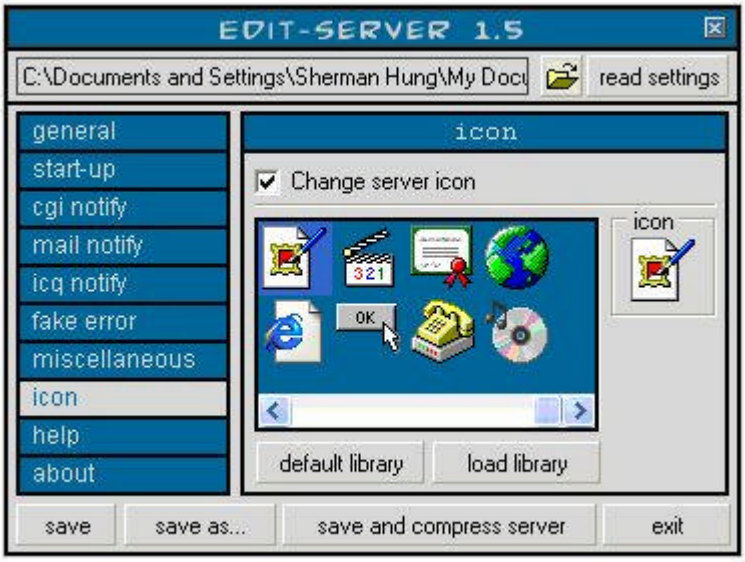


Exhibit 7. icon Section of the server.exe Configurations

f. Saved the server.exe.

4. Attack Machine:

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Downloaded the wrapper program eLiteWrap from www.packetstormsecurity.com. Unzipped it. Copied the server.exe to the eLiteWrap folder.

5. Attack Machine:
Clicked on the Start button and got the DOS prompt. Used eLiteWrap to wrap aiepk IE Popup Killer and Net Devil 1.5 into an executable file called "Setup IE Popup Killer.exe". Set the aiepk as visible runner and Net Devil 1.5 as hidden runner. (See Exhibit 8 below)

Used aiepk – IE Popup Killer to run as front-end when exploiting to the Victim Machine. The aiepk Popup Killer, used to kill popups, is a small program with only 40 Kilobytes.

```
C:\WINDOWS\System32\cmd.exe

C:\Documents and Settings\Sherman Hung\My Documents\Trojan Backdoor\Wrapper\elitewrap>dir
 Volume in drive C has no label.
 Volume Serial Number is 08EA-D48D

 Directory of C:\Documents and Settings\Sherman Hung\My Documents\Trojan Backdoor\Wrapper\elitewrap

12/20/2003  09:45 AM    <DIR>          .
12/20/2003  09:45 AM    <DIR>          ..
04/06/1999  03:55 AM            16,416 elitewrap.exe
12/16/2003  08:56 PM            40,960 IE Popup Killer.exe
12/19/2003  07:17 PM           407,813 Install IE Popup Killer.rar
08/23/2001  04:00 AM            66,048 NOTEPAD.EXE
05/03/1999  11:39 PM            10,460 readme.txt
12/20/2003  09:46 AM           659,970 Server.exe
04/05/1999  11:35 PM               140 test1.ews
               7 File(s)      1,201,807 bytes
               2 Dir(s)  33,800,548,352 bytes free

C:\Documents and Settings\Sherman Hung\My Documents\Trojan Backdoor\Wrapper\elitewrap>elitewrap

eLiTeWrap 1.03 - (C) Tom "eLiTe" McIntyre
tom@dundeecake.demon.co.uk
http://www.dundeecake.demon.co.uk/elitewrap

Stub size: 7712 bytes

Enter name of output file: Setup IE Popup Killer.exe
Operations: 1 - Pack only
            2 - Pack and execute, visible, asynchronously
            3 - Pack and execute,  hidden, asynchronously
            4 - Pack and execute, visible,  synchronously
            5 - Pack and execute,  hidden,  synchronously
            6 - Execute only,     visible, asynchronously
            7 - Execute only,      hidden, asynchronously
            8 - Execute only,     visible,  synchronously
            9 - Execute only,      hidden,  synchronously

Enter package file #1: IE Popup Killer.exe
Enter operation: 4
Enter command line:
Enter package file #2: Server.exe
Enter operation: 5
Enter command line:
Enter package file #3:
All done :)

C:\Documents and Settings\Sherman Hung\My Documents\Trojan Backdoor\Wrapper\elitewrap>_
```

Exhibit 8. Wrapping the Net Devil 1.5.

6. Attack Machine:
Used WinRAR to zip setup.exe into a smaller zipped file. The WinRAR has its own encryption that can bypass virus scans in Yahoo Mail and Microsoft Hotmail.

7. Attack Machine:

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Sent the wrapped file in an attachment through Yahoo Mail to the Victim Server.

8. Victim Server:
Opened the Hotmail account and downloaded the zipped WinRAR file. Unzipped and ran it.

The Net Devil server.exe was then executed and the error message defined at Step 3.c showed up (see Exhibit 9). This indicated that the Net Devil had been applied to the operating system.

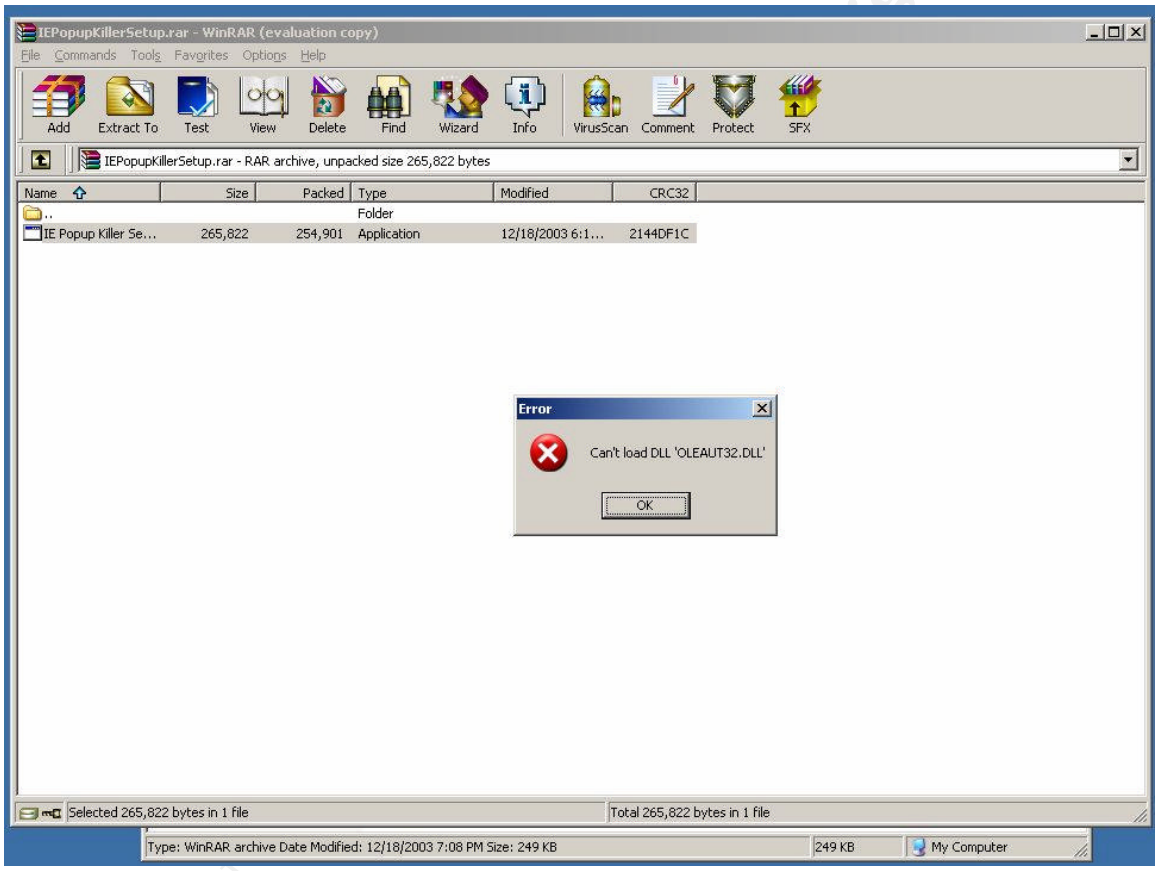


Exhibit 9. The Error Message appeared after executing the wrapped file

Signature Verification

Step 9 below verified signatures to make sure that Net Devil had hooked up the Victim Server (see Page 5).

9. Victim Server:
Four areas were reviewed to verify the signature of attack:

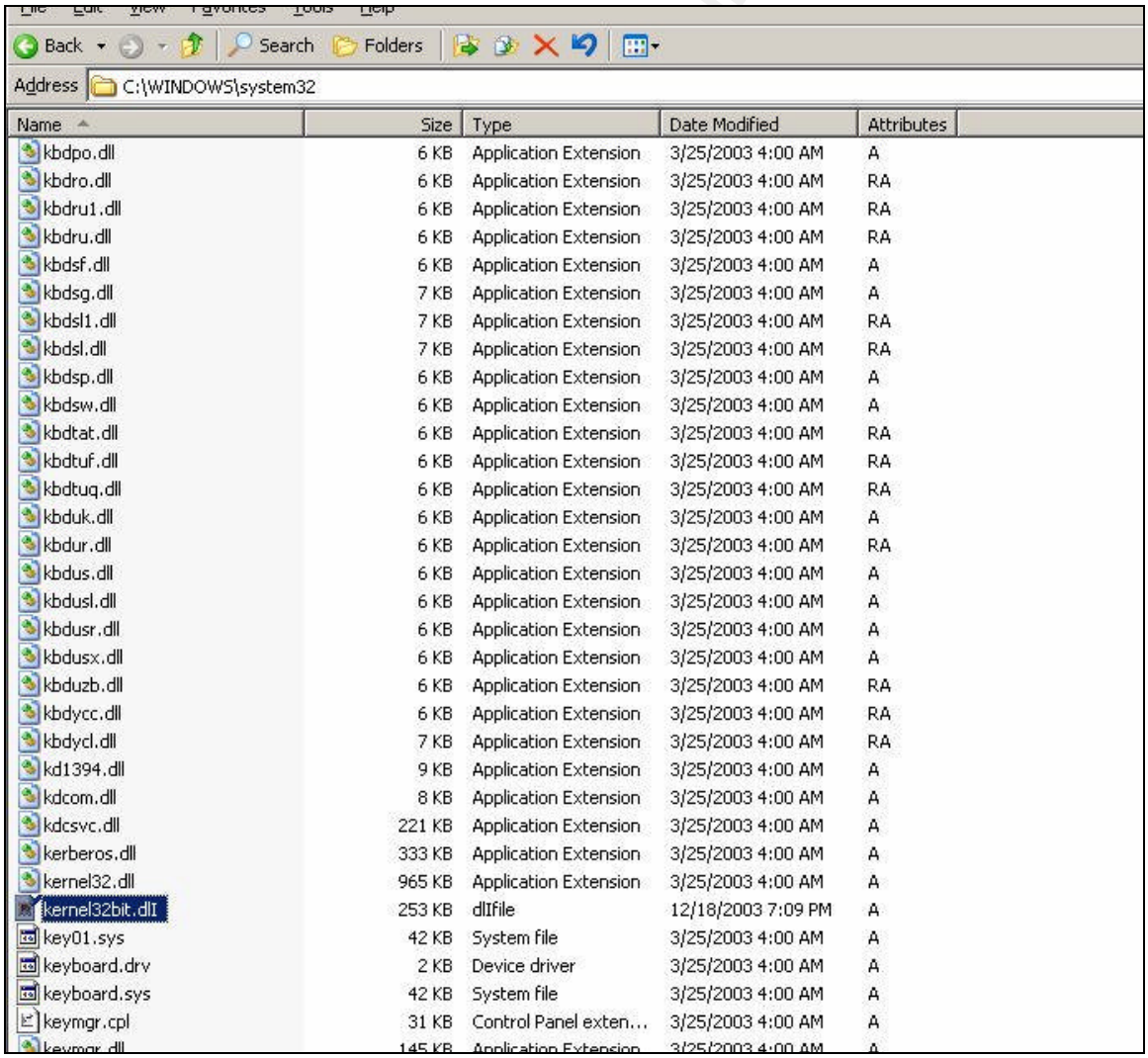
© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

a. I looked into Server 2003's Event Viewer. Application, Security, and System logs were reviewed but I was unable to find an entry that would tell me that OptixPro had infected the server.

b. Verified kernel32bit.dll and found it in \Windows\System32 (Step 3.a). See Exhibit 10.

c. Verified kernel32 registry entry and found it in the "HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run" (see Exhibit 11).

d. The kernel32 was also noted in the Processes Task Manager.



Name	Size	Type	Date Modified	Attributes
kbdpo.dll	6 KB	Application Extension	3/25/2003 4:00 AM	A
kbdro.dll	6 KB	Application Extension	3/25/2003 4:00 AM	RA
kbdru1.dll	6 KB	Application Extension	3/25/2003 4:00 AM	RA
kbdru.dll	6 KB	Application Extension	3/25/2003 4:00 AM	RA
kbdsf.dll	6 KB	Application Extension	3/25/2003 4:00 AM	A
kbdsg.dll	7 KB	Application Extension	3/25/2003 4:00 AM	A
kbdsl1.dll	7 KB	Application Extension	3/25/2003 4:00 AM	RA
kbdsl.dll	7 KB	Application Extension	3/25/2003 4:00 AM	RA
kbdsp.dll	6 KB	Application Extension	3/25/2003 4:00 AM	A
kbdsw.dll	6 KB	Application Extension	3/25/2003 4:00 AM	A
kbdtat.dll	6 KB	Application Extension	3/25/2003 4:00 AM	RA
kbdtuf.dll	6 KB	Application Extension	3/25/2003 4:00 AM	RA
kbdtuq.dll	6 KB	Application Extension	3/25/2003 4:00 AM	RA
kbduk.dll	6 KB	Application Extension	3/25/2003 4:00 AM	A
kbdur.dll	6 KB	Application Extension	3/25/2003 4:00 AM	RA
kbdus.dll	6 KB	Application Extension	3/25/2003 4:00 AM	A
kbdusl.dll	6 KB	Application Extension	3/25/2003 4:00 AM	A
kbdusr.dll	6 KB	Application Extension	3/25/2003 4:00 AM	A
kbdusx.dll	6 KB	Application Extension	3/25/2003 4:00 AM	A
kbduzb.dll	6 KB	Application Extension	3/25/2003 4:00 AM	RA
kbdycc.dll	6 KB	Application Extension	3/25/2003 4:00 AM	RA
kbdycl.dll	7 KB	Application Extension	3/25/2003 4:00 AM	RA
kd1394.dll	9 KB	Application Extension	3/25/2003 4:00 AM	A
kdcom.dll	8 KB	Application Extension	3/25/2003 4:00 AM	A
kdcsvc.dll	221 KB	Application Extension	3/25/2003 4:00 AM	A
kerberos.dll	333 KB	Application Extension	3/25/2003 4:00 AM	A
kernel32.dll	965 KB	Application Extension	3/25/2003 4:00 AM	A
kernel32bit.dll	253 KB	dllfile	12/18/2003 7:09 PM	A
key01.sys	42 KB	System file	3/25/2003 4:00 AM	A
keyboard.drv	2 KB	Device driver	3/25/2003 4:00 AM	A
keyboard.sys	42 KB	System file	3/25/2003 4:00 AM	A
keymgr.cpl	31 KB	Control Panel exten...	3/25/2003 4:00 AM	A
keymgr.dll	145 KB	Application Extension	3/25/2003 4:00 AM	A

Exhibit 10. kernel32bit.dll was found in Windows\System32 folder.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

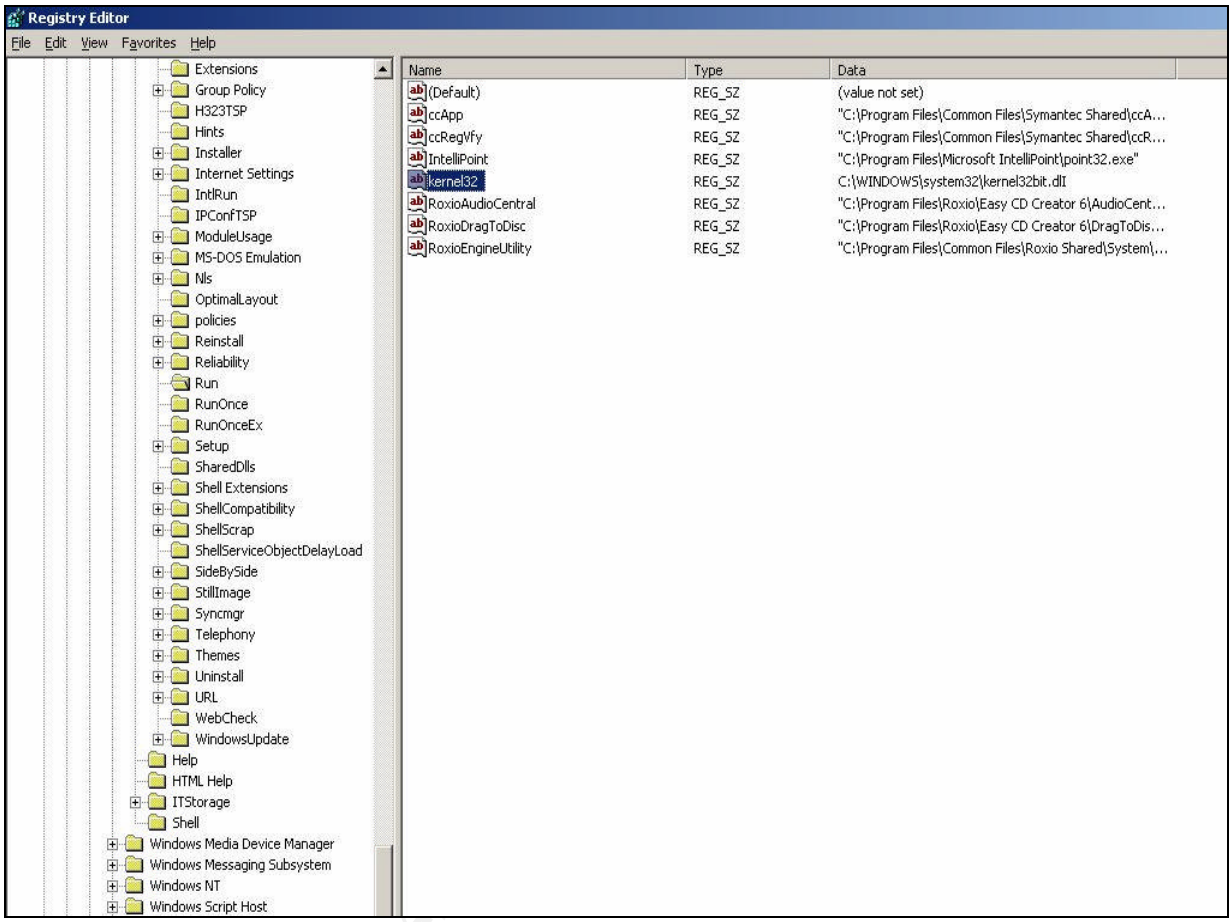


Exhibit 11. kernel32 was found in the Windows registry

Up to this point, I was sure that Net Devil had been successfully applied to the Victim Server. The next step was to get connection and start the exploit.

Gaining Access

10. Attack Machine:
    Executed Net Devil.exe and keyed in IP and port numbers defined earlier (See Exhibit 3). Clicked on the Connect button.

11. Attack Machine
    This could have been an exciting moment; however, the connection could not be established.

12. An Early Ending
    I repeated the above steps a few times to make sure I did not miss anything critical but I was still unable to establish a connection.

    One observation from the Victim Server was that the server could not be shutdown normally. After I removed the kernel32 from the Process Manger, deleted the registry entry and kernel32bit.dll from

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

\Windows\System32, the server returned to normal and was able to be shutdown immediately.

I have to say that the exploit was not successful. It appears to me that Net Devil has not upgraded itself to work in the Server 2003 environment.

OptixPro Exploit
Exploit Step by Step

1. Attack Machine:
   Turned off the Norton Internet Security software on Attack Machine.

2. Attack Machine:
   Downloaded OptixPro 1.31 to the Attack Machine from www.geocities.com/trojansource_2003/. Unzipped it to a folder.

3. Attack Machine:
   Ran Builder.exe to configure the server.exe program. The server.exe was later sent to the Victim Server. The configurations for the server.exe are listed below:

   a. Main Settings
      The first sub-item under Main is General Information. In this section, I followed the default settings.

      The screen also included a Fake Error setup. The default error message was used: "Fatal exception whilst interfacing with OpenGL drive. (See Exhibit 12)

      On the second sub-item, I selected an icon that I thought was stealthy. A very simple step. (See Exhibit 13).

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

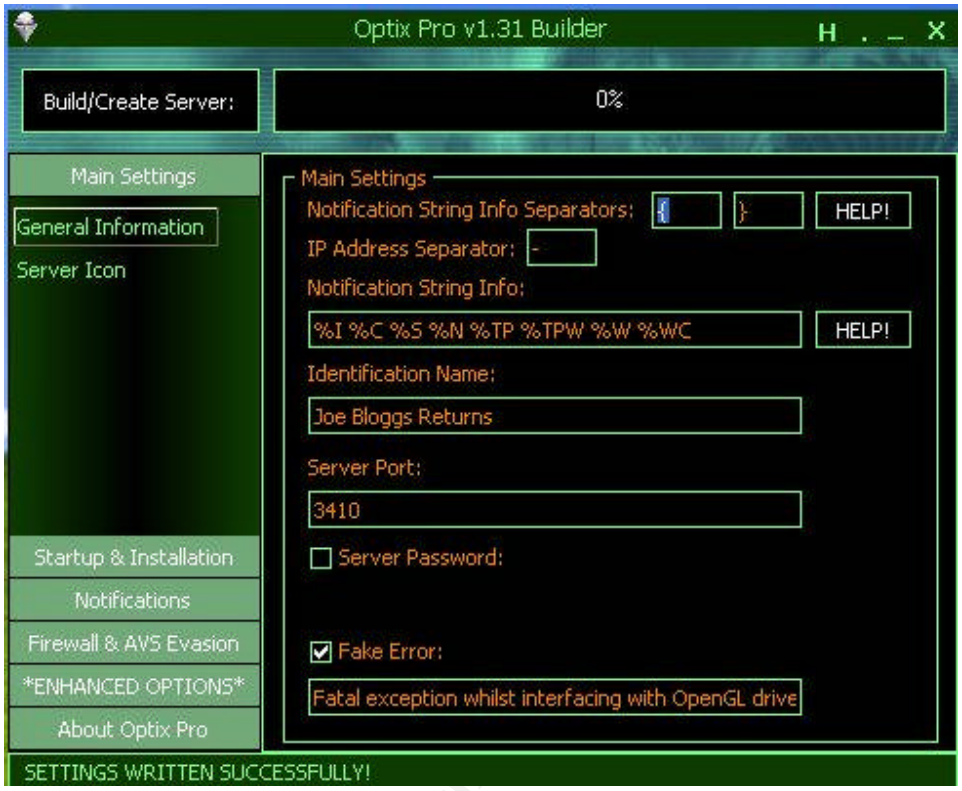


Exhibit 12. General Information Section of the Server.exe Configurations

Exhibit 13. Server Icon Screen of the Server.exe Configurations

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

b. Startup and Installation

Two items under Startup and Installation: Startup and File Setup. On the Startup, I used the default startup settings: “Registry – Run” and the default registry name “GLSetIT32” to specify the name and location of a registry entry. (See Exhibit 14)

On the second item File setup, I also used the default Server File Name: “msiexec16.exe” and default Start Directory: “System Directory”. (See Exhibit 15)

By far, the setup seems very “hacker friendly”. They have default values on each setup field and that made the configuration really quick and easy.

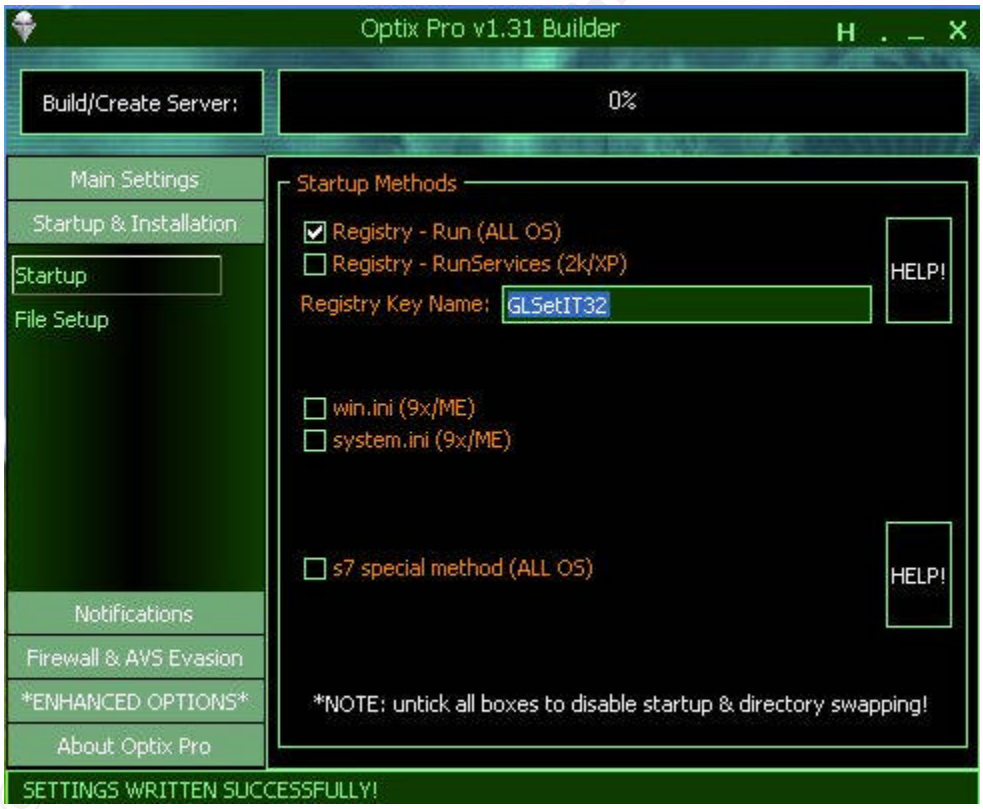


Exhibit 14. Startup Screen of the Server.exe Configuration

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

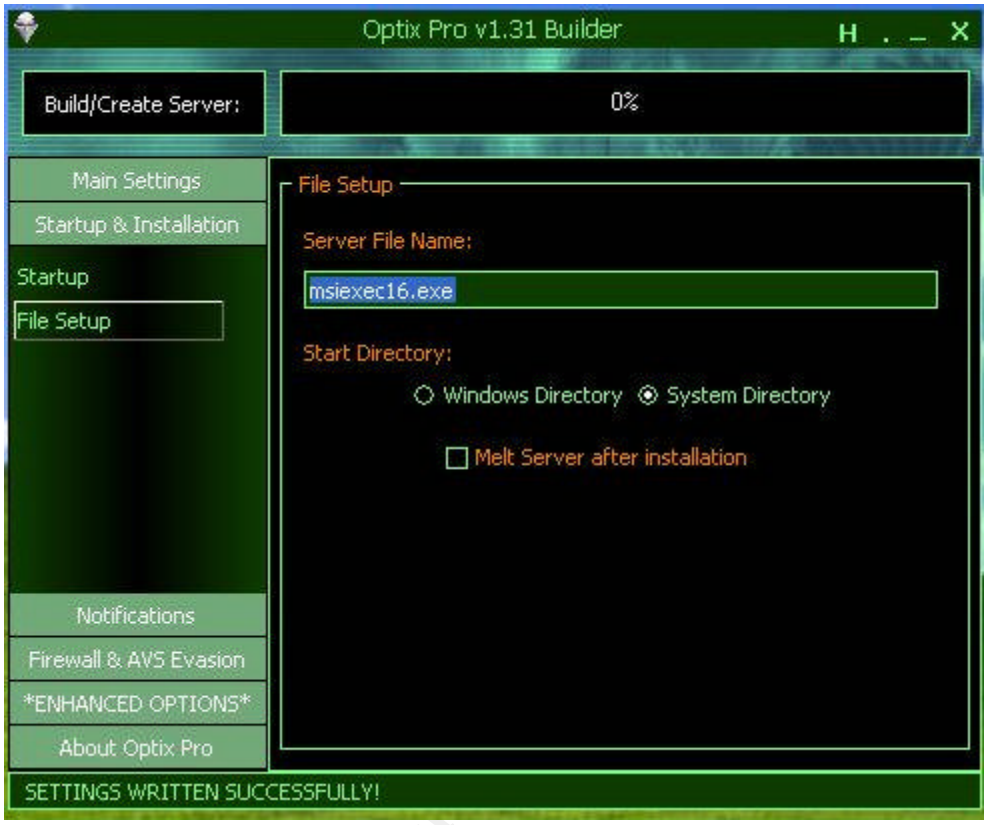


Exhibit 15. File Setup Screen of the Server.exe Configuration

c. Firewall & AVS Evasion (See Exhibit 16)
On the setup screen, I clicked on the following options:
"Enable killing of in-build firewalls"
"Enable killing of in-build Anti-viruses"
"Enable killing of in-build packages that are both Firewall's & AVS"

I was curious to see if OptixPro could kill firewalls and anti-viruses. I had included this in a testing that used Tiny Personal Firewall 5.0 as the firewall.

I did not go further for other functions and saved the setups to server.exe file by clicking "Build/Create Server" button.

4. Attack Machine:
Downloaded the eLiteWrap from www.packetstormsecurity.com.
Unzipped it. Copied the server.exe to the eLiteWrap folder.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

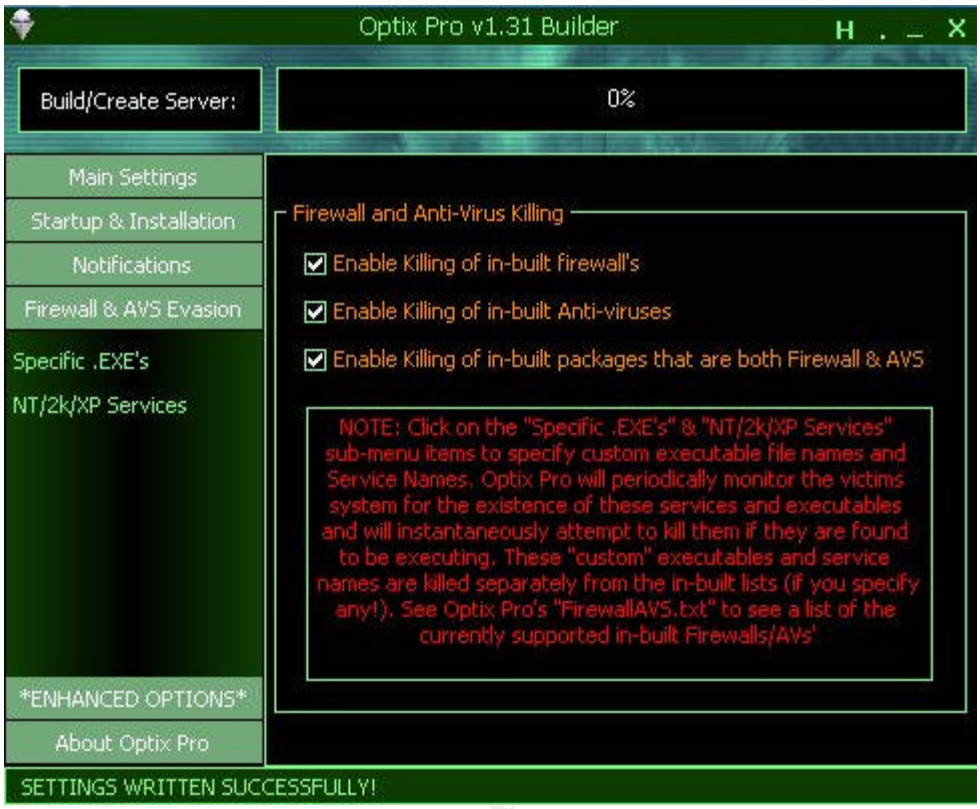


Exhibit 16. Firewall& AVS Evasion Screen of the Server.exe Configuration

5. Attack Machine:
Ran CMD to bring up the DOS command prompt. Used eLiteWrap to wrap aiepk and OptixPro 1.31into an executable program called “Install IE Popup Killer.exe”. Set the aiepk as the visible runner and OptixPro as the hidden runner. (See Exhibit 17 below) The aiepk Popup Killer, used to kill popups, is a small program with only 40K size.

Sent the “Install IE Popup Killer.exe” using Yahoo Mail. Unfortunately, Yahoo Mail detected the Trojan and did not allow the send. (See Exhibit 18). I was impressed that Yahoo Mail was able to detect the Trojan. I then tried to use UPX to compress the file but it did not also pass the virus scan in Yahoo Mail.

6. Attack Machine:
Used WinRAR to zip the setup.exe into a small zipped file and was able to bypass Yahoo Mail’s virus scan. (See Exhibit 19.)

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

```
C:\WINDOWS\System32\cmd.exe

C:\Documents and Settings\Sherman Hung\My Documents\Trojan Backdoor\Wrapper\elitewrap>dir
 Volume in drive C has no label.
 Volume Serial Number is 08EA-D48D

 Directory of C:\Documents and Settings\Sherman Hung\My Documents\Trojan Backdoor\Wrapper\elitewrap

12/19/2003  07:06 PM    <DIR>          .
12/19/2003  07:06 PM    <DIR>          ..
04/06/1999  03:55 AM            16,416 elitewrap.exe
12/16/2003  08:56 PM            40,960 IE Popup Killer.exe
08/23/2001  04:00 AM            66,048 NOTEPAD.EXE
05/03/1999  11:39 PM            10,460 readme.txt
12/19/2003  06:56 PM           925,395 Server.exe
12/18/2003  09:17 PM           659,970 Server2003.exe
12/18/2003  09:20 PM           708,696 Setup IE Popup Killer.exe
12/18/2003  09:20 PM           280,199 Setup IE Popup Killer.rar
               8 File(s)      2,708,144 bytes
               2 Dir(s)  33,857,302,528 bytes free

C:\Documents and Settings\Sherman Hung\My Documents\Trojan Backdoor\Wrapper\elitewrap>elitewrap

eLiTeWrap 1.03 - (C) Tom "eLiTe" McIntyre
tom@dundeecake.demon.co.uk
http://www.dundeecake.demon.co.uk/elitewrap

Stub size: 7712 bytes

Enter name of output file: Install IE Popup Killer.exe
Operations: 1 - Pack only
            2 - Pack and execute, visible, asynchronously
            3 - Pack and execute,  hidden, asynchronously
            4 - Pack and execute, visible,  synchronously
            5 - Pack and execute,  hidden,  synchronously
            6 - Execute only,     visible, asynchronously
            7 - Execute only,      hidden, asynchronously
            8 - Execute only,     visible,  synchronously
            9 - Execute only,      hidden,  synchronously

Enter package file #1: IE Popup Killer.exe
Enter operation: 4
Enter command line:
Enter package file #2: Server.exe
Enter operation: 5
Enter command line:
Enter package file #3:
All done :)

C:\Documents and Settings\Sherman Hung\My Documents\Trojan Backdoor\Wrapper\elitewrap>dir
 Volume in drive C has no label.
 Volume Serial Number is 08EA-D48D

 Directory of C:\Documents and Settings\Sherman Hung\My Documents\Trojan Backdoor\Wrapper\elitewrap

12/19/2003  07:09 PM    <DIR>          .
12/19/2003  07:09 PM    <DIR>          ..
04/06/1999  03:55 AM            16,416 elitewrap.exe
12/16/2003  08:56 PM            40,960 IE Popup Killer.exe
12/19/2003  07:10 PM           974,117 Install IE Popup Killer.exe
08/23/2001  04:00 AM            66,048 NOTEPAD.EXE
05/03/1999  11:39 PM            10,460 readme.txt
12/19/2003  06:56 PM           925,395 Server.exe
12/18/2003  09:17 PM           659,970 Server2003.exe
12/18/2003  09:20 PM           708,696 Setup IE Popup Killer.exe
12/18/2003  09:20 PM           280,199 Setup IE Popup Killer.rar
               9 File(s)      3,682,261 bytes
               2 Dir(s)  33,856,327,680 bytes free

C:\Documents and Settings\Sherman Hung\My Documents\Trojan Backdoor\Wrapper\elitewrap>_
```

Exhibit 17. Wrapping the OptixPro using eLiteWrap.

7. Attack Machine:
   Attached the wrapped file in an email and sent it through Yahoo Mail to the Victim Server.

8. Victim Server:
   Logged on to a Hotmail account and downloaded the compressed WinRAR file. Unzipped and ran the server.exe program. The error

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

message defined at Step 3.a showed up. This indicated that OptixPro had been attached to the operating system.

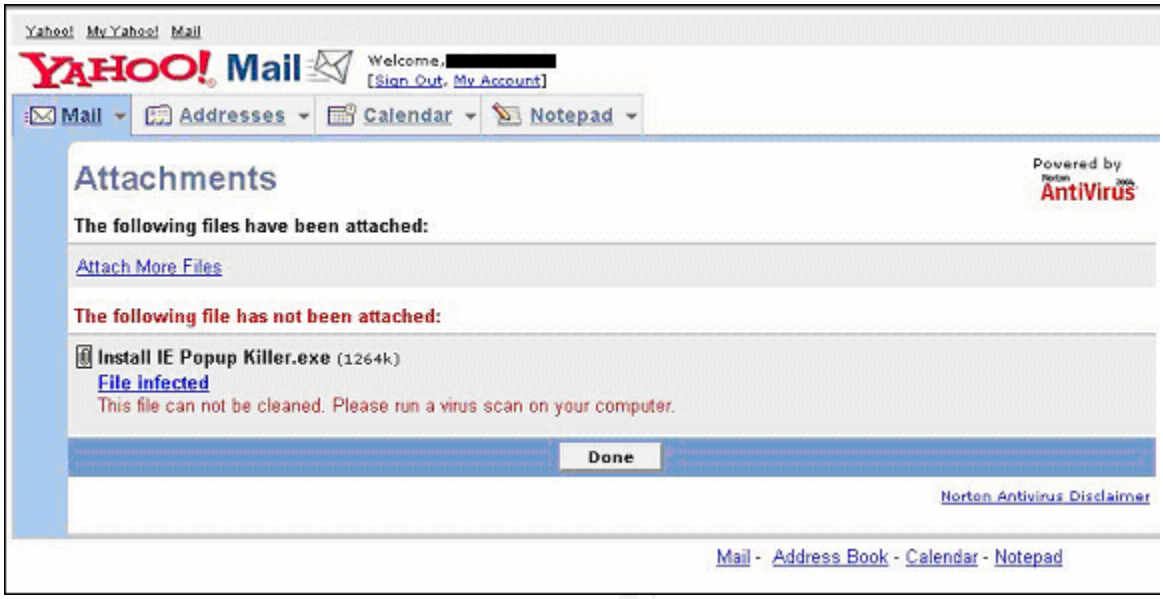


Exhibit 18. The compressed UPX file did not pass the Yahoo Mail Virus Check

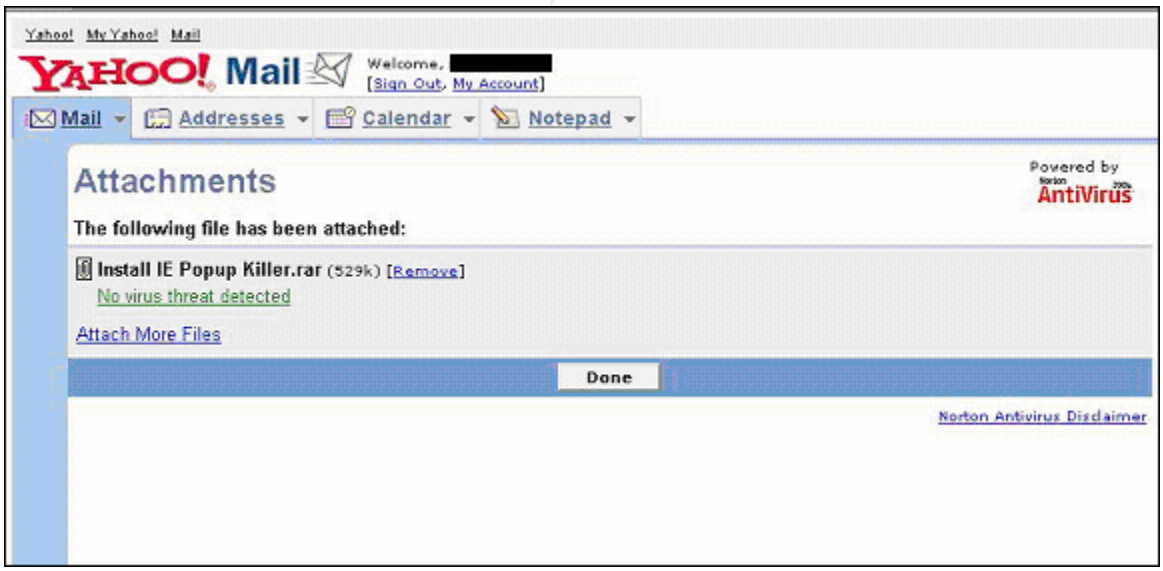


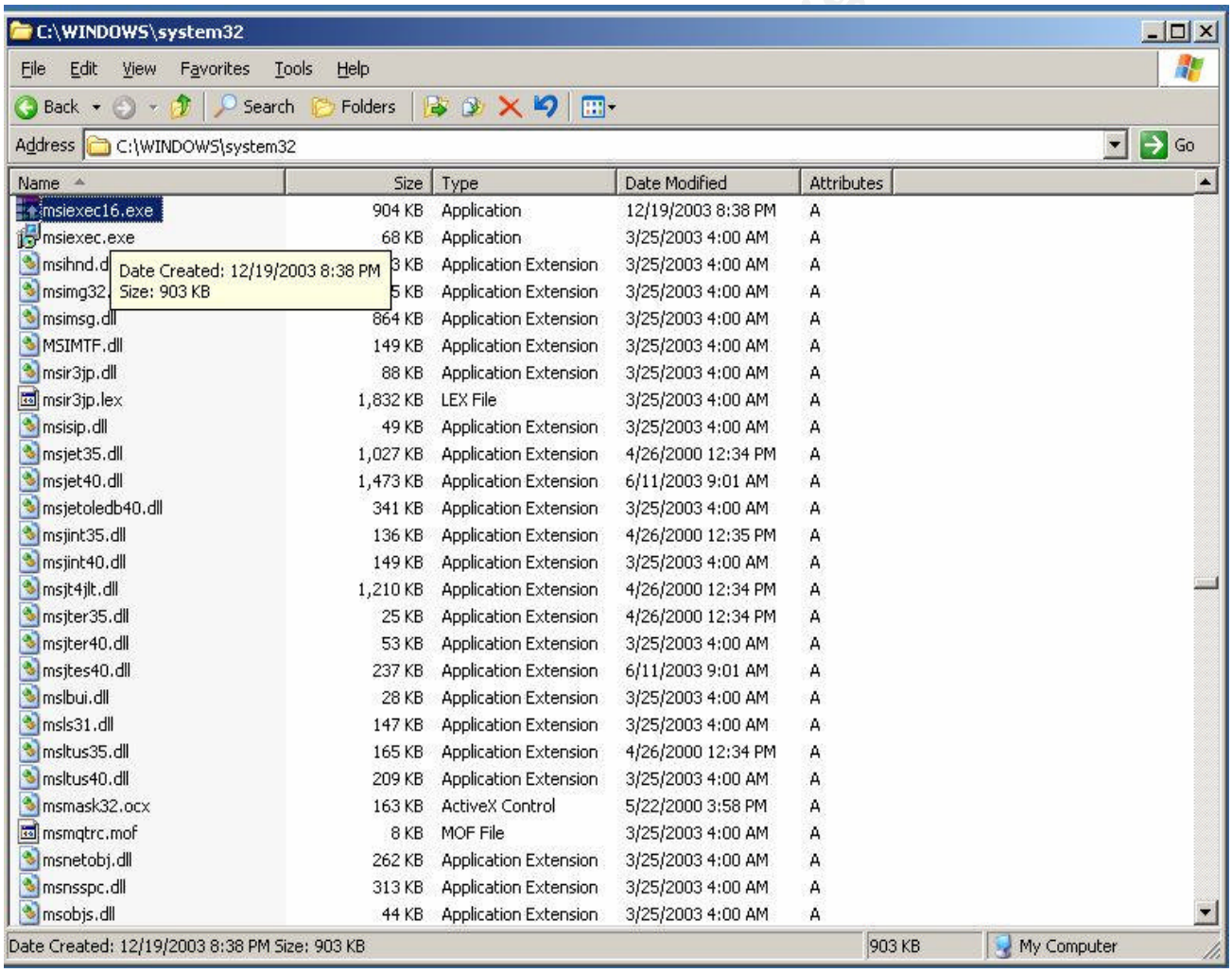
Exhibit 19. The WinRAR compressed file passed Yahoo Mail Virus Check

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Signature Verification

Step 9 verified if OptixPro had infected the server by looking to the signatures specified by Symantec (see Page 6).

9. Victim Server:
   Four tasks were performed for the signature checks:
   a. Verified msiexec16.exe and found it is in \Windows\System32 folder. (Step 3.b). The file was highlighted in the Exhibit 20 below.



Name	Size	Type	Date Modified	Attributes
msiexec16.exe	904 KB	Application	12/19/2003 8:38 PM	A
msiexec.exe	68 KB	Application	3/25/2003 4:00 AM	A
msihnd.d	3 KB	Application Extension	3/25/2003 4:00 AM	A
msimg32.	5 KB	Application Extension	3/25/2003 4:00 AM	A
msimsg.dll	864 KB	Application Extension	3/25/2003 4:00 AM	A
MSIMTF.dll	149 KB	Application Extension	3/25/2003 4:00 AM	A
msir3jp.dll	88 KB	Application Extension	3/25/2003 4:00 AM	A
msir3jp.lex	1,832 KB	LEX File	3/25/2003 4:00 AM	A
msisip.dll	49 KB	Application Extension	3/25/2003 4:00 AM	A
msjet35.dll	1,027 KB	Application Extension	4/26/2000 12:34 PM	A
msjet40.dll	1,473 KB	Application Extension	6/11/2003 9:01 AM	A
msjetoledb40.dll	341 KB	Application Extension	3/25/2003 4:00 AM	A
msjint35.dll	136 KB	Application Extension	4/26/2000 12:35 PM	A
msjint40.dll	149 KB	Application Extension	3/25/2003 4:00 AM	A
msjt4jlt.dll	1,210 KB	Application Extension	4/26/2000 12:34 PM	A
msjter35.dll	25 KB	Application Extension	4/26/2000 12:34 PM	A
msjter40.dll	53 KB	Application Extension	3/25/2003 4:00 AM	A
msjtes40.dll	237 KB	Application Extension	6/11/2003 9:01 AM	A
mslbui.dll	28 KB	Application Extension	3/25/2003 4:00 AM	A
msls31.dll	147 KB	Application Extension	3/25/2003 4:00 AM	A
msltus35.dll	165 KB	Application Extension	4/26/2000 12:34 PM	A
msltus40.dll	209 KB	Application Extension	3/25/2003 4:00 AM	A
msmask32.ocx	163 KB	ActiveX Control	5/22/2000 3:58 PM	A
msmqtrc.mof	8 KB	MOF File	3/25/2003 4:00 AM	A
msnetobj.dll	262 KB	Application Extension	3/25/2003 4:00 AM	A
msnsspc.dll	313 KB	Application Extension	3/25/2003 4:00 AM	A
msobjs.dll	44 KB	Application Extension	3/25/2003 4:00 AM	A

Exhibit 20. msiexec16.exe was found in the Windows\System32 folder.

   b. Verified GLSetIT32 registry entry and found it in the "HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run". Please see Exhibit 21. The GLSetIT32 entry was highlighted.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

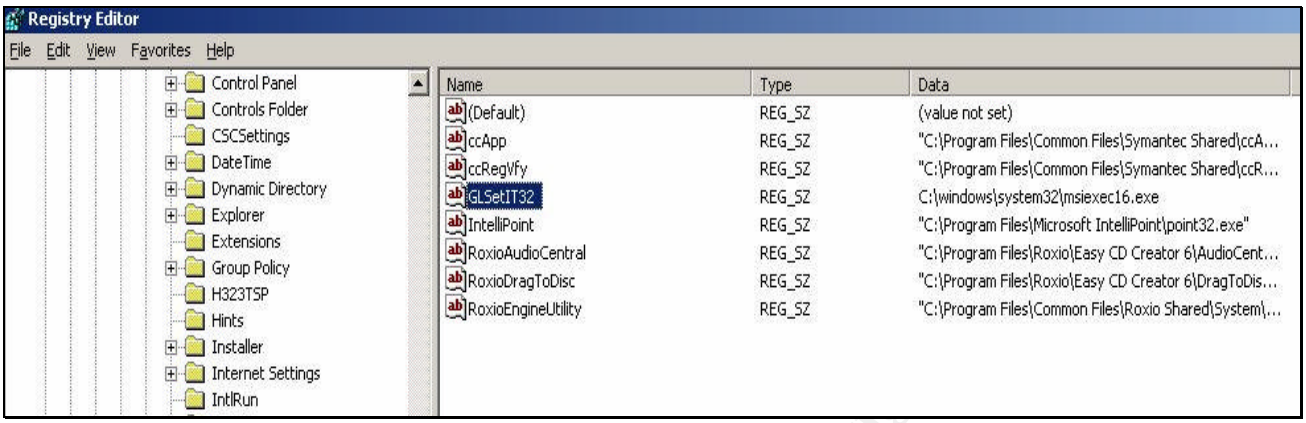


Exhibit 21. GLSetIT32 was found in the Windows registry.

c. kernel32 was also checked and found in the Processes Task Manager. (See Exhibit 22 below. The msiexec16.exe was highlighted.)

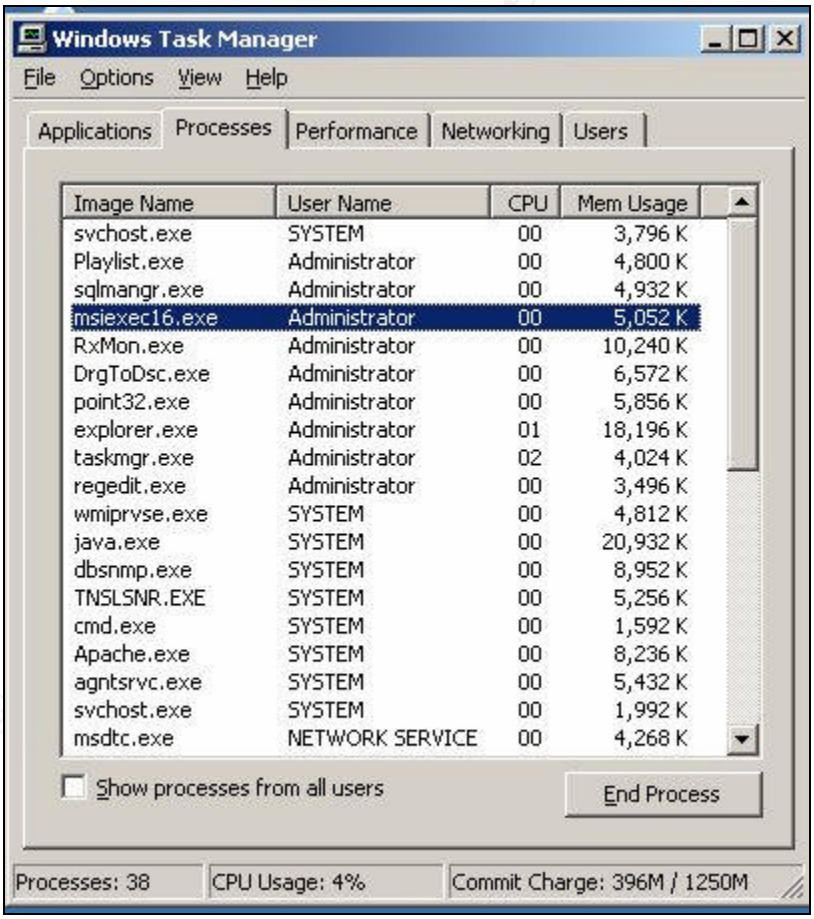


Exhibit 22. msiexec16.exe was found in the Task Manager.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

d. I looked into Server 2003's Event Viewer. Application, Security, and System logs were reviewed but I was unable to find an entry that would tell me that OptixPro had infected the server.

So far, the required components were all in place and running. OptixPro was ready to go. The next step was to gain the access to the Victim Server.

Gaining Access

10. Attack Machine:
Executed Client.exe and specified IP address of the Victim Server. The default port is 3410. Clicked on button to connect. This was an exciting moment. The connection was established!!! (See Exhibit 23)

Exhibit 23. It was successfully connected!

Steps 11 through 14 were performed on the Attack Machine:

11. Exploit 1 – Server Options
In the Server Options, Power Options have malicious functions. They can be used to reboot, shutdown, suspend, logoff the Victim Server. These functions would create a ghost haunting atmosphere to the victims.

The second item under Server Options used to verify the configurations made in Step 3 were implemented to the Victim Server. Clicked on the "Get!" button at the right. In less than a second, the configuration

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

information returned from the Victim Server and was correct. (See Exhibit 24.)

12. Exploit 2 – Managers

I consider this to be one of the more powerful functions in OptixPro. It has File Manager, Process Manager, Windows Manger, Registry Manager, FTP Manager, SOCKS Server, Remote Scanning, and Port Redirect functions. All the meat that a hacker needs is here. I tested File Manager, Process Manager, Registry Manager, and Remote Scanning below.

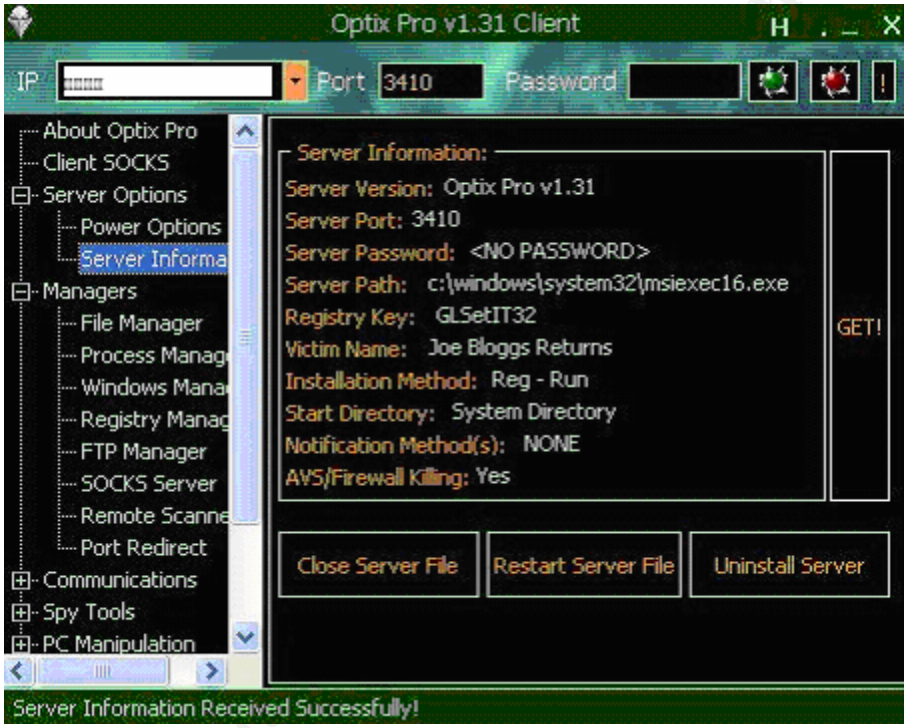


Exhibit 24. OptixPro Configurations returned to the Attack Machine.

File Manager explores a Victim Server's folders and files. Files can be executed in hidden mode, copied/pasted/cut, uploaded from client, downloaded to client. You can even use the Search function to look for a file. (See Exhibit 25)

I downloaded samlib.dll and samsrv.dll to the Attack Machine. Both files were successfully downloaded. See Exhibit 26. However, no confirmation notification message appeared when the download was complete.

Process Manager lists tasks that are currently processed. Hackers can use this function to kill any tasks that are currently running.

Registry Manager can be used to change registry values. I consider this to be a powerful function. (See Exhibit 27.)

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

I then tested the Remote Scanner. I specified Start IP, Stop IP, and Port number. I then clicked on “Start Scan” and “Get Current Results”. A message “Results List Updated Successfully” appeared. However, I was not sure what that meant. I could not find a log file or other port scanning results.

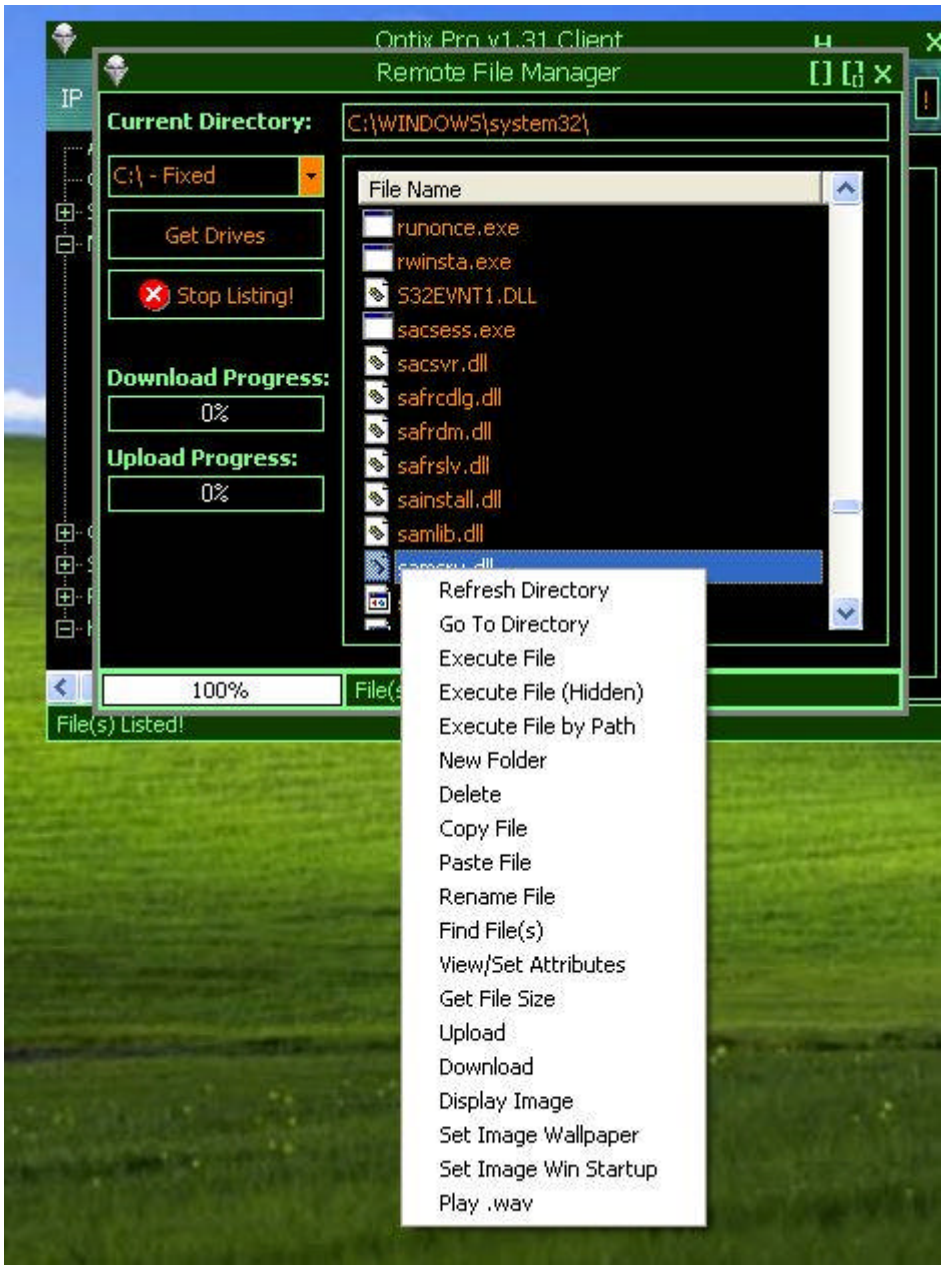


Exhibit 25. File Manager has powerful functions to manipulate files.

13. Exploit 3 – Spy Tools

Computer Information, under the Spy Tools, is used to list the computer information of the victim. It lists very detailed information including Organization, Owner, Computer Name, Windows Version, Windows Key,

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Windows Directory, System Directory, Processor, Processor Speed, Free Disk Space, ICQ Number, System Drives, and Client Connected. (See Exhibit 28.) Very powerful!

The second option is “Get Password”. It acquires Cashed, AIM, and RAS passwords.

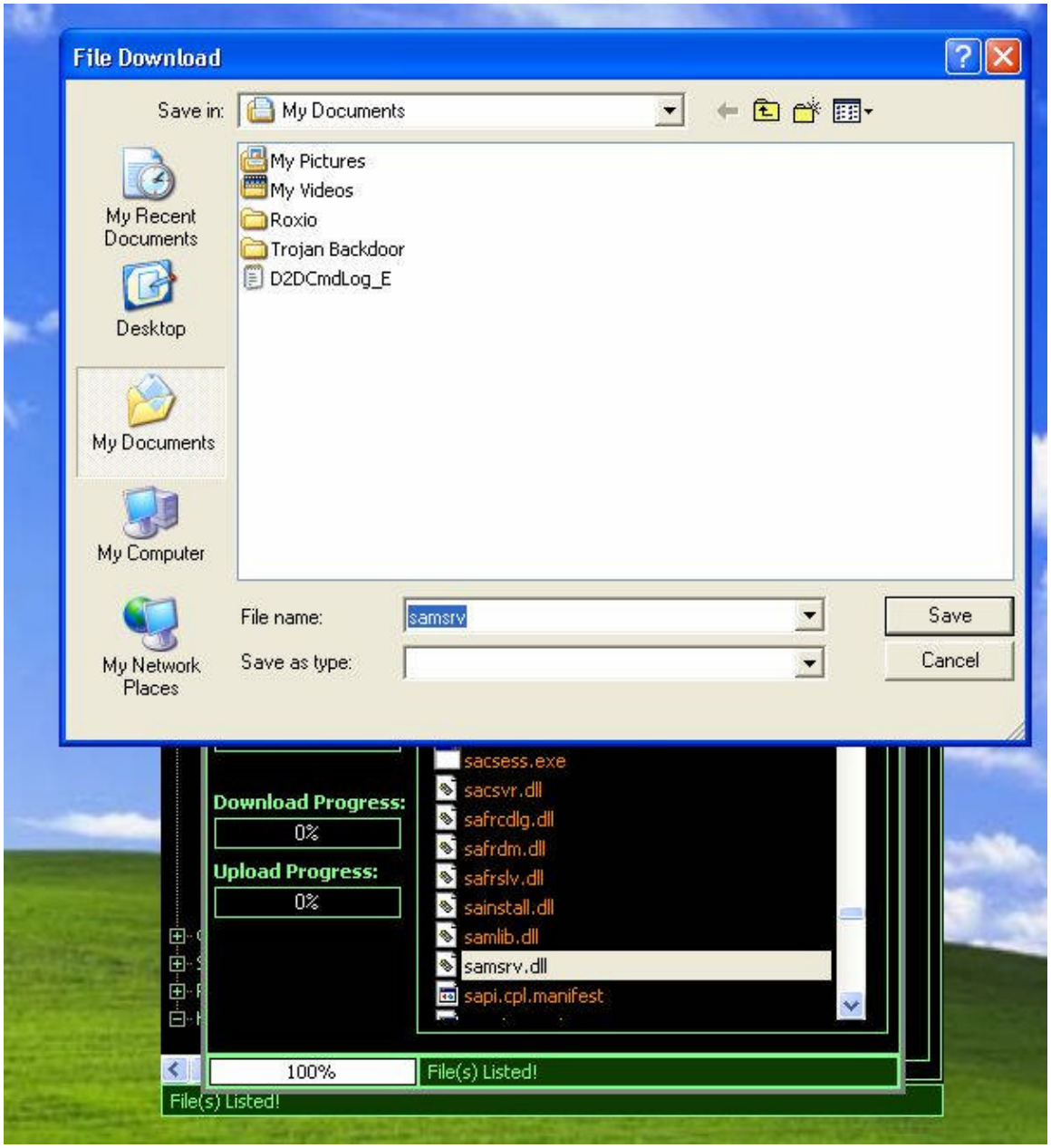


Exhibit 26. samsrv was downloaded.

The third option is key logging, which logs victims’ keystrokes. I tested the function and found it worked very well. I logged into Microsoft Hotmail on

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

the Victim Server. The account and password were captured and logged on the Victim Machine.

I did not play around the PC Manipulation section and went ahead to Humor/Fun Stuff section.

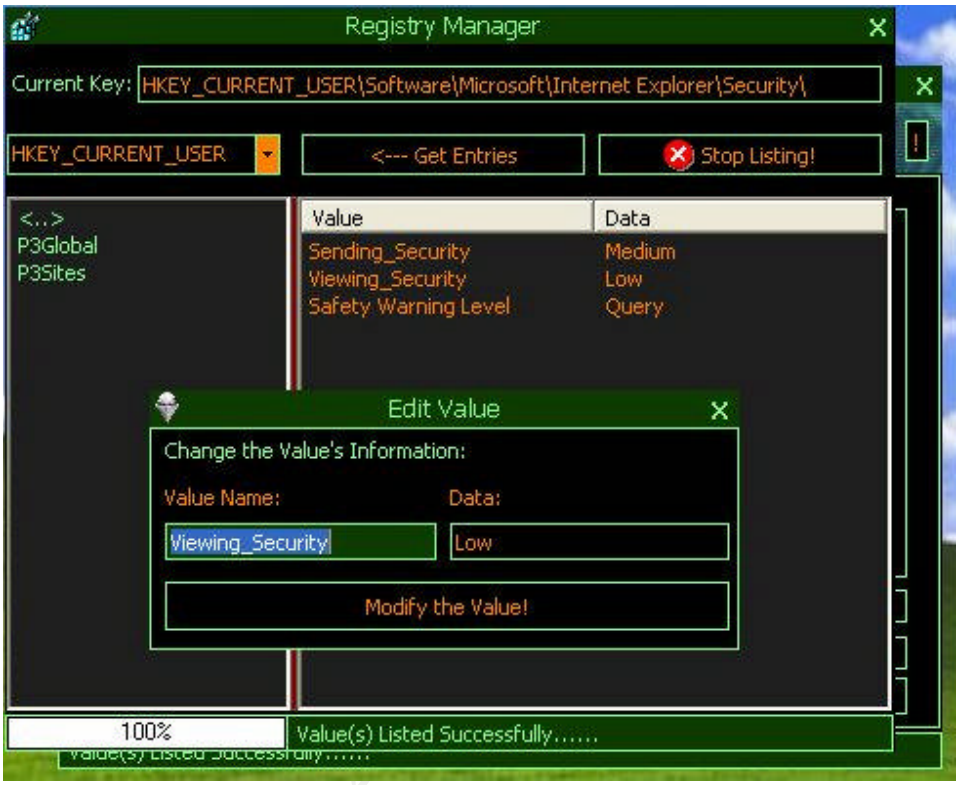


Exhibit 27. Registry Manager changes a registry value.

© SANS Institute

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Exhibit 28. Spy Tools lists the detailed information of the Victim Server.

14. Exploit 4 – Humor/Fun Stuff

This part includes a list of buttons that are “ghost haunting” functions. A hacker can do crazy and bizarre tasks such as: hiding the clock, turning the monitor off, initiating screen saver, hiding the start button, opening CD drives, disabling mouse and keyboard functions, and setting IE startup page.

I tested these functions by opening and closing a CD drive. This would undoubtedly make a victim panic or furious (especially when it is midnight and things become spooky). . .(See Exhibit 29.)

While I was wrapping up the hacking, I executed the client.exe again, a message panel appeared and it was quite interesting. The author of OptixPro was offering a service for $300 to continuously provide updates to kill new/upgraded anti-viruses and firewalls. (See Exhibit 30.) I was amazed that the author was willing to take on challenges to fight with the “fixes” to OptixPro.

Unlike Net Devil, which lost its power in Server 2003, I believe OptixPro will continue to survive and evolve with the new releases of operating system software.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

15. Exploit 5 – Kill Firewall

The last but not the least, I tested if OptixPro could kill firewall. I installed Tiny Personal Firewall 5.0 (TPF) on the Victim Server to test if OptixPro could still survive. The test procedures were documented below:

a. Removed OptixPro from the Victim Server by deleting msiexec16 from registry, Process Manager, and the System32 folder.
b. Installed TPF to the Victim Server. I did not further configure the firewall and kept the original settings. Executed the "Install IE Popup Killer.exe" to start the OptixPro on the Victim Server.
c. Went to Attack Machine, initiated the client.exe and clicked on the connect button.

The result was interesting. TPF detected the server.exe and asked if it should be allowed or denied. When I denied it, OptixPro did not infect the server at all.

When I allowed it, OptixPro sprawled. The OptixPro suspended the TPF's Activity Monitor that logged the incoming and outgoing port activities. In other words, the TPF was somewhat disabled.

OptixPro does as it claims: "kill firewall" only if the user allows the server.exe when it knocks on the door.

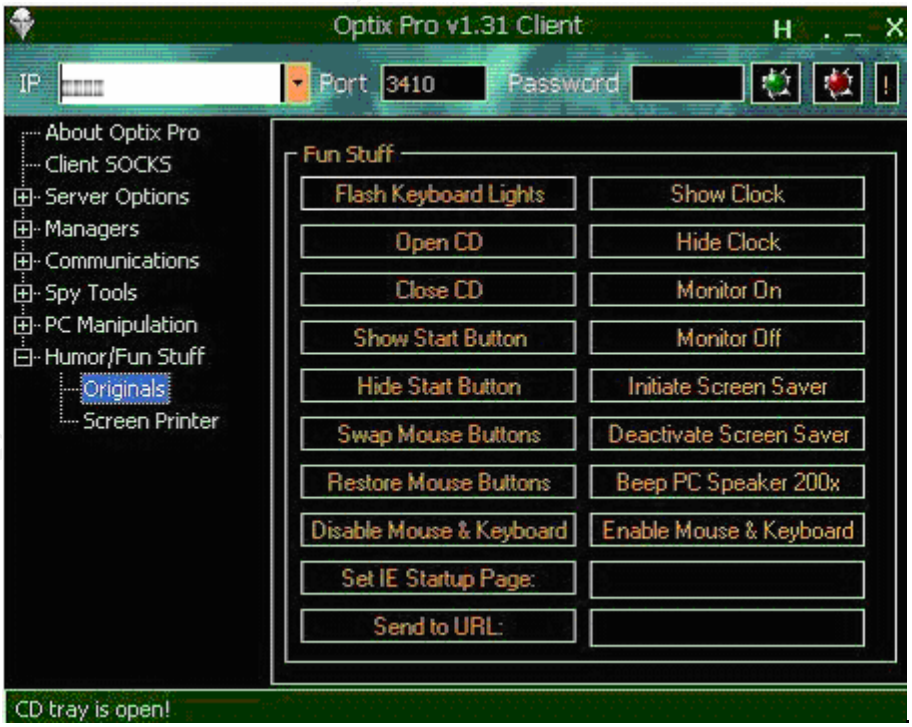


Exhibit 29. CD Drive was opened on the Victim Server.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Exhibit 30. Author's Offer Upgrade Services.

Summary of the Exploits

In summary, based on the above exercises, OptixPro worked out better than Net Devil in the Windows Server 2003 environment.

It appears that the author of the OptixPro had kept the program abreast of the new Server 2003 operating system. However, Net Devil 1.5 had failed in this regard. This tells me that OptixPro has a better opportunity of being used by the black hat society.

Both programs had many similarities. They attached themselves to the System32 folder, created an entry in the registry, were executed during the Windows startup, and they can be found in the Process Manager.

In OptixPro, the upload and download features in both programs are useful. The port scanner is considered a good feature. The capabilities of manipulating registry and Process Manager and logging keystrokes are impressive.

Both programs were delivered with a compressed utility called UPX. I tested it and was not impressed. Public email services (Yahoo Mail and Microsoft Hotmail) were able to detect the Trojan in the UPX compressed files.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Trojan programs compressed with WinRAR files were able to bypass the virus scan. This could be a recommendation to the anti-virus software developers.

The port scanner in OptixPro did not work as I expected. This could be due to my lack of understanding in using this feature.

The TPF 5.0 detected the server.exe. When the “server.exe” was permitted in the TPF, OptixPro sprawled. It suspended the intrusion detection in TPF and I could connect to the server again from the Attack Machine. The “kill firewall” worked only when the user allows it at the front door.

This was a good exercise but it still has a few limitations that may not accurately reflect a real business world:

1. The simulated network environment was not as sophisticated as a real network environment. Only the Tiny Personal Firewall was tested in the Victim Server.

2. Enterprise anti-virus software was not used on the Victim Server in the scenario. I am anxious to know if OptixPro would have been able to take control of the server had an enterprise anti-virus been installed.

3. The IE Popup Killer program was noted as a poor choice to run as the front canvas. It appeared in less than a second and consequently did not provide a good cover-up.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

PART 5 – KEEPING ACCESS AND COVERING TRACKS

Both Trojans survived reboots. They continued to exist until they were removed. They did not show up on the screen nor did they slow down the processing speed. The file and registry names on the Victim Server can be changed by a hacker to very system-like names. This makes both Trojans difficult to identify.

Since the Net Devil exploit did not work, I can only speak for the OptixPro based on what I learned from the exploit. What follows below is on the assumption that I am the hacker who would perform the following tasks to keep access and cover my tracks.

To me, the most powerful features in OptixPro are the capability to modify and download files, log screen keystrokes, and change Windows system settings. To continuously keep access, I would first perform a keystroke logging to obtain a user account name and password. In addition, I downloaded the SAM file and use L0phtcrack (LC4) to crack and obtain administrator accounts and passwords. Once you have the administrator account and its password, the server is considered to be “conquered”. I would then login to the server as a regular user at the “official” front door.

I would also try to turn off the three server logs: Application, Security, and System. Even though these logs did not track down the exploits as mentioned in the earlier discussion, it is possible that you could leave other trails from other activities (i.e. file downloading and modification).

If my goal were to obtain critical and confidential data from the Victim Server, I would not hesitate to search and download these files first. The download capability as discussed in the earlier sections is very fast. I would not change or delete the files or system settings unless it is necessary. Making file changes on the Victim Server may leave audit trails somewhere and consequently could be logged or identified manually later.

To cover my tracks, I would use Netcat to control a remote computer as the attack machine. Netcat is a simple but powerful hacking tool that works on both UNIX and Windows. Netcat is considered a utility tool and it may pass an antivirus scan. (Note: I ran a test and it passed a virus scan.)

Netcat has two modes: client and listener. The client mode would be used on the Attack PC and listener on the Victim Server.

Use Netcat to get a shell going on a remote machine by using the -l or "listen" option and the -e or "execute" option. You run Netcat to listen on a particular port for a connection.

When a connection is made, Netcat executes the program of your choice

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

and connects the stdin and stdout of the program to the network connection.

In our OptixPro exploit, I could run the OptixPro client program by typing 'nc -l -p 23 -t -e client.exe' and it will get Netcat listening on port 23 (telnet). When it gets connected by a client, it will spawn a shell (OptixPro's client.exe). The -t option tells Netcat to handle any telnet negotiation the client might expect. This will allow you to telnet to the machine you have Netcat listening on and get a OptixPro shell when you connect.

"Netcat can also be used to relay data from machine to machine and make it harder to trace the original point of an attack. Netcat can bounce an attack across several machines. In Exhibit 31, a hacker can first control Relay-A machine and Relay-B machine. The hacker can set up Netcat on each of the machines to relay data across these machines and make the trace work difficult."[16]

Netcat can be downloaded from http://www.atstake.com/research/tools/network_utilities/.

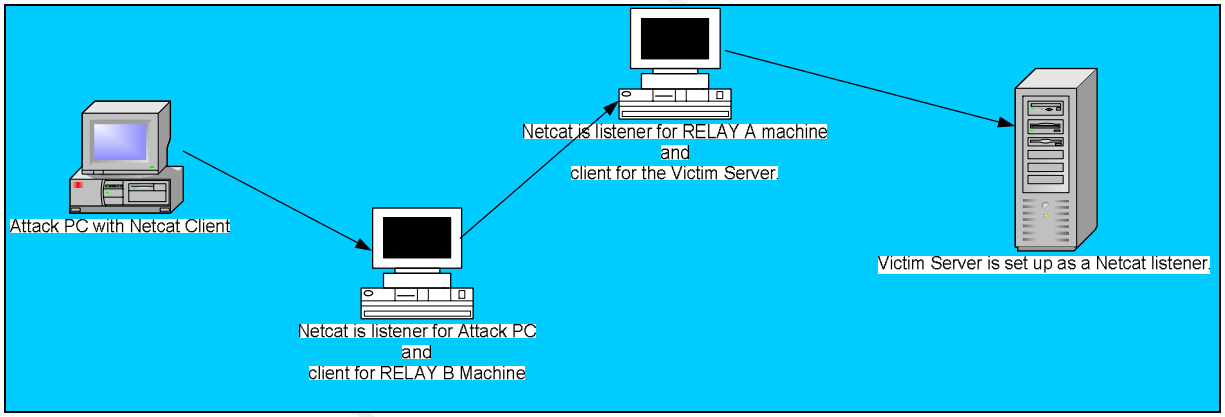


Exhibit 31. Netcat Relays[17]

Overall, the OptixPro is very stealthy. Once you are in, you can continue to have access as long as you are prudent and do not make careless mistakes (i.e. open the CD ROM, turn off monitor, hide clock at midnight, etc.)

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

PART 6 – THE INCIDENT HANDLING PROCESS

Preparation

The preparation steps of an incident handling process should be taken as a preventive measure to preclude an incident from occurring. In the auditing profession, these are called preventive controls. Adequate and effective preventive controls can always reduce losses resulting from incidents. Policies and procedures that establish guidelines to prepare and handle an incident can be an effective preventive control.

Policies usually come with detailed procedures. Policies are established at a high level to provide general guidelines that can be understood by the employees. Policies define the high-level business requirements. For example, "In order to protect the company's business data and application systems, antivirus should be installed on each workstation." Policies are usually dictated by a real business need that may result from a painful lesson learned, auditing/consulting recommendations, risk assessments, and other business requirements. In the Preparation Phase for the Trojan exploits, the policies should be prepared by the company's Information Technology (IT) Department, or more specifically, by the Information Security Team in the IT Department.

When we move down to procedures, we are talking about detailed steps that can be used to handle an incident. Procedures are usually detailed instructions or list of questions that serve as guidelines, e.g. checklists, escalation procedures with a call tree, and other systematic instructions. To make sure these steps work, they need to be tested before being officially adopted. In our case, the detailed step-by-step instructions to prevent, detect, and remove Trojan backdoors are the procedures. (See #20 below, page 47)

Policies and procedures need to be officially approved, published, and communicated. The publishing and communicating process is important. Unless they are published and communicated to employees, policies and procedures are ineffective and useless. From my experience, there have been many cases where employees were not aware of well-documented policies and procedures saved on an individual hard drive.

Since my exploits were performed on a simulated network and some limitations exist, I am going to deploy the incident handling process using what I learned from the exploits and apply them to a real world situation. I have been working as an IT Auditor for fifteen years at major financial institutions and government agencies. The following policies and procedures are based on an assumption that I am the Information Security Manager for a large company. I would like them to be included in the Information Security Policies and Procedures.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

To prevent malware (Trojan backdoors in this case) attacks, below is a set of policies that should be published to general employees. Other security items that are not related to malware attacks are not discussed here.

1. Antivirus software should be installed and activated on each workstation.

2. Any personal data media or disks should be scanned for viruses before being loaded into a company computer. A separate scanning machine should be available and isolated from company network. (Note: I have to admit that this and the next item are not easy to implement but it is indeed an effective way to avoid Trojan backdoor and other viruses.)

3. Employees are not allowed to download programs/software from Internet. If a download is necessary, the download should be loaded into an isolated machine for virus scan before being used.

4. Employees should use email only for official business purposes. Unknown emails should be deleted and not opened.

5. Employee user accounts should be configured to have the following security restrictions:

    a. Passwords should be eight alphanumeric characters length.

    b. The passwords should be automatically expired at least every 60 day.

    c. Old passwords cannot be reused for a certain period of time (12 months).

    d. Each account should be set to have limited login attempts. Three login attempts should be applied to regular employees.

6. The Human Resources Department should coordinate with IT to schedule security awareness training sessions once a year. The training should be mandatory for each employee. Indications of different malware attacks should be communicated to employees in the training. An immediate reporting mechanism should be established.

7. The user accounts for terminated or resigned employees should be immediately revoked. Human Resources should notify the Information Security team as soon as an employee is terminated from the company. The coordination between the Human Resources and IT Department is extremely important. I have seen many cases where this communication was not established which resulted in increased security risks.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Below are the policies for the IT Department. They are more technical oriented:

8. The IT Department should apply a new patch and perform a virus scan on a regular basis. Automatic alerting mechanisms should be implemented. The alerting mechanism can page the first line responsible person 24/7.

   Most antivirus and intrusion detection software have established signatures for both Trojans. Antivirus and intrusion detection software will nail them down instantly. However, the threat exists that Trojan upgrades might pass the antivirus and firewall scanning.

9. The IT Department should implement controls to block spam and other soliciting emails. Configure your email server to block or remove email with attachments that have file extensions of .vbs, .bat, .exe, .pif and .scr files.

10. Prepare a set of change control procedures for the following:

    a. Applying antivirus patches.

    b. Changing network configurations.

    c. Changing firewall and intrusion detection settings.

    d. Changing operating system configurations.

    Approval process should be defined. Testing should be conducted before changes/patches are applied to production.

11. The ITS Department should encrypt the Windows passwords using NTLM Version 2 algorithm that is harder to be cracked. The password administration for #5 above should be effectively enforced.

12. The IT Department should prepare a set of procedures for malware and Trojans detection and removal. Related sources (i.e. websites) should also be documented.

    Trojan and other malware have the following common traits:

    a. Unexplained modification or deletion of data.

    b. Unexplained new or unfamiliar file names.

    c. Unexplained modifications to file lengths and dates in system files.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

d. Off-hour (i.e. 2:00am) usage of user accounts.

13. The IT Department should watch malware outbreak news and take appropriate actions.

14. The IT Department should periodically perform port scan and review and investigate any abnormal open ports.

15. The IT Department should implement firewall and intrusion detection tools to protect company networks. The filter rules and signatures should be defined, tested, approved, and documented.

16. The IT Department should have consultant or audit departments review security control adequacy and effectiveness.

17. The IT Department should develop an escalation procedure in the event of business operation interruptions due to the damage from hacker attack. In the escalation procedures, roles and responsibilities should be defined.

18. Daily backup and should be made and stored at an off-site. The backup and recovery procedures should be tested to make sure recoverability. Restore baseline procedures should be defined to facilitate a full and clean recovery.

19. A business contingency plan should be prepared, tested, and approved. The plan should cover natural disasters and unexpected hacking attacks that could result in business operation interruptions. The activation procedures should be clearly specified for different contingent circumstances including serious data corruptions due to a hacker attack.

20. Develop a checklist or step-by-step instructions as guidelines to identify the causes.

<u>Identification Checklist</u>

Both OptixPro and Net Devil have common characteristics of Trojan backdoors:

The detailed identification procedures for Net Devil and OptixPro are slightly different below. In general, the two Trojans can be identified by looking into signatures in Process Manager, Windows registries, Windows System/System32 folder, win.ini, and system.ini.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Net Devil:

a. Net Devil's default program name is kernel32bit.dli. This can be found in the Process Manager and System32 folder. However, this name is changeable at the hacker's discretion.

b. The default ports are 900 to 903. They are also changeable.

c. Startup methods are defined in either
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run or
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices.

The registry entry name is kernel32. Again, the registry name is changeable. I would say this is the best area to identify the Trojan since the registry name will be in either one of the two locations. Also, the entries at both locations are limited and therefore facilitate identification of an unusual item.

d. The default fake error message is "Can't load DLL 'OLEAUT32.DLL'". The default file extension to register is dll. Again, this is changeable.

OptixPro:

a. OptixPro default program name is msiexec16.exe and can be found in the Process Manager and System32 folder. This name is changeable at the hacker's discretion.

b. The default port is 3410. Again, it is changeable.

c. Startup methods are defined in either one of the two locations if the operating system is Windows 2000 or XP.
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run or
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices.

The registry entry name is GLSETIT32. However, the registry name is changeable. I would say this is the best area to identify the Trojan since the registry name will be in either one of the two locations. Even if the names can be changed, the number of entries is limited in the Run or RunServices.

For Windows 95, 98, and me, look for "run = " in the win.ini and system ini. The entry could appear as "run = explore <Trojan program name>"

d. The default fake error message is "Fatal exception whilst interfacing with OpenGL drive" when it copies itself to an infected machine. Again, this is changeable.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Above items may not be specifically applied to each company but they can serve as a baseline to prepare a robust set of policies and procedures. These policies and procedures should be effectively followed and executed.

Identification

Identification is used to uncover the cause of an incident. The following steps should be performed during the Identification Phase:

1. Understand the conditions.

   A Trojan attack usually begins with a user's report or an automatic alert from antivirus and intrusion detection systems.

   First, a user reports that his/her computer has unusual conditions like those mentioned in #12 in the Preparation phase:

   a. Unexplained modification or deletion of data.

   b. Unexplained new or unfamiliar file names.

   c. Unexplained modifications to file lengths and dates in system files.

   d. Off-hour (i.e. 2:00am) usage of the user's accounts.

   A rescue team, usually under the Information Security Team, should respond and start the rescue actions. The reported conditions should be analyzed and documented. The rescue team should be deliberate and write notes in detail.

   The rescue should run virus scan and check intrusion detection logs on the infected machines. Most of the time, the name of a Trojan or malware should be detected through a virus scan. The logs of intrusion detection should be reviewed and verified if any unusual packets were sent through open ports. After following these steps, the name of malware or Trojan should be identified.

2. Identify the causes.

   After gathering the information of an attack, the rescue team should ask the "what", "when", "where", "how", "why" and "who" questions:

   a. How did the Trojan bypass the company's network?

   b. Where and when was the first infected machine?

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

c. Why didn't the antivirus and/or intrusion detection capture the Trojan in the first place?

d. How long has the attack been going on?

e. What business data files have been stolen? Are they confidential?

f. Why were these users selected to be attacked instead of others?

g. Where may the attack have originated? What other company network and workstations could be next.

h. Who, if possible, could the hacker be? And, what would be their motives?

i. Does the Trojan backdoors come from mass spam? If so, how many employees may have opened the attachment in their emails? If the malware is from an Internet download, how many users could have used the software?

When posing these questions to the victims, the rescue team should be tactful and try not to point fingers. This information should be documented in as much detail as possible.

3. Evaluate the business impact.

Based on the information gathered in item #2, the rescue team should swiftly involve user management and discuss possible business impacts. The following factors can be used to evaluate the impact:

a. Monetary loss.

b. Interruption of business operations.

c. Violation of privacy/confidentiality.

d. Negative business reputation.

e. Legal implications.

Chief Information Officer, attorneys, and other top management should be notified if the impact is considered critical. To me, this is a very crucial point in time. Involvement with the proper personnel and immediate escalation actions are extremely important if the attack is deemed critical to the business.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

4. Determine the best and worst possible scenarios and prepare appropriate action plans.

   The rescue action plan should be started as soon as the business impact is recognized. This will require immediate action on the part of management. Appropriate plans for the best and worst case scenarios should be discussed and proper action should be taken. Resources and staff responsibilities should be swiftly assigned.

Containment

The objective of the Containment phase is to reduce the scale of damage from the incident. If the incident is not effectively and accurately contained, it is possible that the damage may spread rapidly. The key here is to identify which machines have been infected. This is not an easy job because a large company may have thousands of workstations many of which may have been infected.

The Information Security Team should determine at this point which workstations should be taken off the network and which systems are still clean, or untouched by the incident.

The following actions should be taken:

1. In item #3 of the Identification Phase, the cause and scale should have been measured. The rescue team should have an idea of the containment scope. Again, the key concerns are how many computers have been infected and what business data has been altered or stolen.

2. The impact on the daily operation impact should be also evaluated. The following questions should be answered:

   a. If these computers were taken away from the users, how would the business operations be interrupted? What level of management should be notified and involved?

   b. Can we temporarily close all the unused ports? What would be the business impact?

   c. When and where were the last backup made for the business data? What would the restore baseline be as mentioned in item #18 of the Preparation Phase. Can we recover the business data files to the point of “unplug”?

   d. Do we have temporary solutions to avoid business operation interruption? Are there unused computers that can be configured

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

and assigned to those employees whose computers are infected? How do we make sure that these replaced computers are clean?

e. Do we need to install business applications on these machines? Is there a manual processing mode available? Would it be necessary to switch to manual processing mode until the management makes further decisions?

These questions can be included in a checklist and the planned actions should be coordinated between the rescue team and business users.

3. Take the infected computers off the company's network. Turn off and remove unneeded network services. "By default, many operating systems install auxiliary services that are not critical, such as an FTP server, telnet, and a Web server. These services are avenues of attack."[4]

4. Reassign a new email account to those users whose computers are infected.

5. Backup of the infected machines is the next step after the computers are taken off the computer network. The following questions should be answered:

   a. Would this backup be used for forensic purposes? What other documentation is needed for legal needs?

   b. How many backups are needed?

   c. How do we isolate the backup copies and the infected machines to avoid further infection?

Eradication

The Eradication phase is to remove these malware, to verify they have diminished, and to ensure no more will follow. At this point, the infected machines should have been isolated so that further attacks do not occur.

The following items should be included in the procedures:

1. As mentioned in item #2c of the Containment Phase, business data files should be backed up daily. In the worst case situation, if no backup is available, use the checklist developed in item #20 of the Preparation phase. Remove both OptixPro and Net devil from the infected machines as follows:

   a. Go to the two possible registry locations to look for unusual entries.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Delete the unusual entries. This is easier than looking for objects in System32 and Process Manger because typically, there are not many lines in the Run and RunServices registry keys.

b. Go to System32 folder and look for program names (dll and/or exe) mentioned in the Identification. If those names are not found, look for system files with recent creation dates. Investigate these files.

c. Apply antivirus patches and have a full virus scan. This may take hours to complete. Make sure it is completely clean. Print the virus scan report.

2. If daily backups are available and restorable, it is recommended that this computer be re-formatted.

3. At this point, a vulnerability scan should be performed to make sure there are no other threats extant in the company's network. Also, a complete virus scan on the company's servers is required.

   The vulnerability scan should at least cover a port scanning to identify any unused open ports. Investigate the scan results.

4. Based on the causes identified in the previous phases, identify further security hardening strategies and improvement opportunities in the eradication process.

Recovery

The Recovery phase is to restore the systems back to operational mode. At this point, the servers and workstations should be clean, the vulnerability scan should have proven the system free of known problems, and all applicable patches should be installed.

The following actions should be performed by the rescue team:

1. If the computer is reformatted as mentioned at #2 in the Eradication Phase, a restore baseline should be identified for business data. Have a virus scan on the baseline copy. Changes/transactions since the baseline date should be also scanned before being applied to the baseline.

2. Install antivirus on the recovered machine before other application software. Apply patches and upgrades of antivirus, intrusion detection, and firewall.

3. Fully test the systems on the recovered machines to make sure they are clean before they are brought back to operations. A virus scan result

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

report should be prepared and it must show that the Trojan backdoors are cleaned up.

4. Demonstrate the virus scan report to business users, explain how the work was done, and have the management of the user department sign-off.

5. Allocate resources to follow up with the users.

Lessons Learned

Prepare an incident report based on the notes jotted down throughout the entire incident handling process. The report should include causes of the incident, control improvement opportunities, and possible policy and procedure enhancements. A meeting should be held to include user management, business users, and the IT Department. A consensus should be reached and recommended corrective actions should be documented.

The following items are usually included in the report:

1. Can improvements be made to the existing policies and procedures?

2. Is additional monitoring work required?

3. Are additional automatic alert mechanisms needed?

4. What can be improved to shorten the rescue team's response time?

5. How much time is needed before we verify effectiveness of these corrective actions?

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

PART 7 - CONCLUSION

With the evolution of the Internet, computers are connected globally. This has given hackers more avenues to explore and exploit using different tools that are easy to obtain. The backdoor Trojan is one of many hacking techniques available. Both Net Devil and OptixPro were developed with a user friendly GUI. These programs encourage regular users to become hackers. Proper security counter-measures (such as anti-viruses, firewall, intrusion detection, and Virtual Private Network) have become a necessity to protect computers and networks.

Through this exercise, I experienced some of the tug-of-war between the hacker and the network computing community as each challenges the other. New technology is always accompanied by bugs that allow the opportunity for new exploits. In this non-perfect world, the game will continue resulting in new opportunities for developers, hackers, and security professionals alike.

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

PART 8 - REFERENCE

[1] www.geocities.com/trojansource_2003/. Please note that the poll was as of 12/11/2003. The ranking may be changed with more votes coming in.

[2] http://www.trendmicro.com/en/security/general/glossary/overview.htm

[3] http://securityresponse.symantec.com/avcenter/venc/data/backdoor.netdevil.html

[4] http://securityresponse.symantec.com/avcenter/venc/data/backdoor.netdevil.html

[5] http://securityresponse.symantec.com/avcenter/venc/data/backdoor.OptixPro 1.31.13.html

[6] Readme.txt of the eLiteWrap.zip.

[7] Readme.txt of the eLiteWrap.zip.

[8] Readme.txt of the eLiteWrap.zip.

[9] Readme.txt of the eLiteWrap.zip.

[10] Readme.txt of the eLiteWrap.zip.

[11] http://securityresponse.symantec.com/avcenter/venc/data/backdoor.netdevil.html

[12] http://www.symantec.com.br/avcenter/venc/data/backdoor.optixpro.13b.html

[13] Page 73, "Section 4.2 - Computer and Network Hacker Exploits, Part1", "Track 4 – Hacker Techniques, Exploits and Incident Handling", by Ed Skoudis and SANS Institute. 2003.

[14] Page 21, "Section 4.2 - Computer and Network Hacker Exploits, Part1", "Track 4 – Hacker Techniques, Exploits and Incident Handling", by Ed Skoudis and SANS Institute. 2003.

[15] Adopted from http://www.insecure.org/nmap/.

[16] Page 89, "Section 4.3 – Computer and Network Hacker Exploits, Part2", "Track 4 – Hacker Techniques, Exploits and Incident Handling", by Ed Skoudis, SANS Institute, 2003.

[17] Developed based on the diagram on Page 89, "4.3 – Computer and Network Hacker Exploits, Part2", "Track 4 – Hacker Techniques, Exploits and Incident Handling", by Ed Skoudis, SANS Institute, 2003.

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.