

McAfee® Best Practices advisory for W32/Nachi.worm

By Greg Day/Lee Fisher
Solution Architects

What does the threat do?

W32/Nachi.worm was first discovered on the 18th August 2003.

Other security organisations have given this threat alternate names including Welchia and MSBlast.D, it is not however a variant of the W32/Lovsan 'family' of worms.

The Nachi worm propagates through exploiting two security vulnerabilities. Both vulnerabilities target Microsoft® Windows NT4, 2000 and XP. Microsoft® announced the first security vulnerability (WebDAV) on the 17th March 2003, the second (DCOM/RPC) on 16th July 2003.

The first vulnerability is within WebDAV, and allows a remote computer to execute any chosen code or application locally on the vulnerable computer.

You can view the Microsoft® WebDAV announcement at the following URL:

<http://www.microsoft.com/technet/treeview?url=/technet/security/bulletin/MS03-007.asp>

The second vulnerability, within the DCOM/RPC service, allows a remote computer to execute any chosen code or application locally on the vulnerable computer.

You can view the Microsoft® DCOM/RPC announcement at the following URL:

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

NOTE: The vulnerabilities listed above are chronologically listed. The worm actually utilises the DCOM/RPC vulnerability first, then after 200,000 'attacks', utilises the WebDAV vulnerability.

The objective of the Nachi worm is to terminate W32/Lovsan.worm.a if active on the host (which was first discovered on the 11th of August 2003) and delete the MSBLASTER.EXE executable.

It then attempts to apply the Microsoft® patch to prevent other threats from infecting the system through the same security hole.

When the system clock reaches Jan 1, 2004, the worm will delete itself upon execution.

Nachi infection methodology

It is important to understand the 'attack cycles' which the worm utilises.

The worm scans the local subnet for host machines using ICMP pings on port 135. This can create high volumes of network traffic, as the worm attempts to ping from x.x.0.0 to x.x.255.255 (where x.x are taken from the local network).

It will attempt to connect to 200,000 IP addresses in this manner before switching into the second attack cycle.

The only difference between the attack cycles is the 'exploit' used by the worm. In the first cycle the worm will attack remote hosts utilising the DCOM/RPC vulnerability. In the second cycle the worm will attack remote hosts utilising the WebDAV vulnerability.

Once the worm has received a reply from a remote host, it will perform a test to check the security level of the remote host, and if vulnerable, the worm sends the appropriate exploit to gain control of the remote host.

The victim's machine is instructed open a remote shell to download and then execute the worm using TFTP through TCP port 707.

Upon execution the worm installs itself (DLLHOST.EXE) into the Windows System32 WINS folder and registers itself as the service RPCPatch with the display name "WINS Client".

You should be aware that DLLHOST.EXE can exist on non-infected systems, as a genuine file. It is normally about 5-6Kb in size, which is much smaller than the version added by the Nachi worm, which is 10Kb in size.

Please Note: There is a perfectly legitimate system file with filename DLLHOST.EXE. Typically, the legitimate file is only approximately 5-6 kB.

It then checks the local DLLCache on the host machine and copies and TFTP.DEX to the above WINS folder, renaming it to SVCHOST.EXE which again registers itself as the service RPCTFTP with the display name "Network Connections Sharing". We believe the purpose of renaming the file is purely in an effort to thwart future W32/Lovesan variants which use the application to 'download' the worm.

You should note that TFTP.DEX does not exist on all operating systems by default. Obviously where not present on the local machine in the DLLCache the copy and rename will fail.

The worm checks the OS and service pack on the host and attempts to use a HTTP GET request to download and apply the MS03-026 security patch from the sites listed below.

- <http://download.microsoft.com/download/6/9/5/6957d785-fb7a-4ac9-b1e6-cb99b62f9f2a/Windows2000-KB823980-x86-KOR.exe>
- <http://download.microsoft.com/download/5/8/f/58fa7161-8db3-4af4-b576-0a56b0a9d8e6/Windows2000-KB823980-x86-CHT.exe>
- <http://download.microsoft.com/download/2/8/1/281c0df6-772b-42b0-9125-6858b759e977/Windows2000-KB823980-x86-CHS.exe>
- <http://download.microsoft.com/download/0/1/f/01fdd40f-efc5-433d-8ad2-b4b9d42049d5/Windows2000-KB823980-x86-ENU.exe>
- <http://download.microsoft.com/download/e/3/1/e31b9d29-f650-4078-8a76-3e81eb4554f6/WindowsXP-KB823980-x86-KOR.exe>
- <http://download.microsoft.com/download/2/3/6/236eaaa3-380b-4507-9ac2-6cec324b3ce8/WindowsXP-KB823980-x86-CHT.exe>

- <http://download.microsoft.com/download/a/a/5/aa56d061-3a38-44af-8d48-85e42de9d2c0/WindowsXP-KB823980-x86-CHS.exe>
- <http://download.microsoft.com/download/9/8/b/98bcfad8-afbc-458f-aaee-b7a52a983f01/WindowsXP-KB823980-x86-ENU.exe>

W32/Nachi.worm checks for the presence of W32/Lovsan.worm.a and where present terminates the process and deletes MSBLASTER.EXE. The registry changes made by W32/Lovsan.worm.a are NOT removed by the W32/Nachi worm. It should also be noted that the worm fails in patching the vulnerable system.

When the system clock reaches Jan 1, 2004, the worm will delete itself upon execution.

McAfee® AVERT™ has a full description of the worm on the Virus Information Library, you can review this information here :http://vil.nai.com/vil/content/v_100559.htm

What proactive steps can be taken against the threat ?

1. The most likely method for the worm to enter your organisation is via the Internet, from your IP address being scanned by an infected computer. This 'scan' would have been conducted using TCP port 135, so blocking this port at your Internet gateway is an option.
2. Certainly Microsoft® based computers should have had the security updates (available from Microsoft® in the links listed above) applied to secure them from the vulnerability. Of course it may not have been practical to have implemented the security update on every machine, but certainly Microsoft based computers at your gateway/perimeter should have been updated since they would likely be the easiest to connect to on your network.
3. McAfee Enterecept™ Host based behavioural protection technology is also capable of preventing this attack by providing protection against buffer overflow attacks. This level of protection functions regardless as to the level of security updates, or virus definition updates, installed on the 'target' computer.
4. McAfee IntruShield® Network based Intrusion Prevention technology can both detect and prevent the worms attack from even reaching vulnerable hosts. The anomaly detection engine technology within McAfee IntruShield will alert customers of suspicious network activity it has and prevent it from crossing the network.
5. McAfee Desktop Firewall™ would block access to TCP port 135 if no legitimate applications were defined to make use of the port, and would have prevented the worm from opening TCP port 707. This would prevent infected systems from further propagating the worm. Even if the worm had been executed by an unsuspecting user (received for example, in email) the worm would not have been able to connect to any remote computer system, in effect isolating the infected computer on the network.
6. Sniffer® Technologies filters can be used to alert managers to the presence of the malicious worm exploiting the Microsoft RPC buffer overflow vulnerability. Sniffer Technologies filters for Sniffer Portable and Sniffer Distributed, can identify the W32/Nachi.worm used to exploit the Microsoft DCOM/RPC vulnerability and to monitor traffic on TCP port 135. To download the latest Sniffer Technologies filters, [click here](#).

What can I do if I have been infected with the threat ?

The first steps with any infection are to gain some level of information as to the scale of the infection and then limit it from progressing further.

- Immediately update your mail/gateway scanners to at the 4286 DATs.
- If possible, you should block TCP port 135 and TCP port 707 at your perimeter firewalls if you have no business usage for them.
- Ensure that all Microsoft® Windows NT4, 2000 and XP computer systems are patched against the MS03-007 (WebDAV) and MS03-026 (DCOM/RPC) vulnerabilities.
- Microsoft® has released a utility to ensure that the MS03-026 patch has been correctly applied. You can also scan across your network from a single location. It is available [here](#).

Once infected machines are discovered they should be quarantined to limit the infection.

- ThreatScan™ can help detect infected host by running a resource scan across the network for open TCP port 707 connections will indicate potentially infected clients.
- Where Desktop Firewall is in place an attempt to send data through any of the compromised ports listed above would result in an alert event being created. Where this is being managed by ePolicy Orchestrator (ePO), this will give you real time data on any instances of PC's infected by the worm.
- A free to use Stinger utility has been made available to clean potentially infected clients. AVERT™ Stinger can be located [here](#). McAfee ePolicy Orchestrator™ (ePO) can manage and deploy the Stinger utility if you need to quickly deploy the utility across your network.
- InfiniStream™ Security Forensics mining capabilities can accurately pin point the infected machines, and the source of infection, reducing mean time to resolution and the chances of reoccurrence.
- Sniffer® capture filters have also been created to aid and assist you tracking down infected hosts. Captures are available for Sniffer portable and Sniffer distributed and are located [here](#).

You should clean infected PC's first, then expand to apply the update all other PC's. Use McAfee ePO to generate infection reports to help confirm the removal of the worm. Also, ePO users can use the 'wake-up call' feature to help you ensure all PC's get and apply the update immediately. The ePO coverage reports give you visibility, to ensure compliancy.

If you have ThreatScan, we would suggest running a ThreatScan resource scan to give you visibility into all the devices on the network, so you can ensure they are ePO- managed. Rogue PC's are a common source of infection and re-infection.

Expert Services – We can help you

Network Associates Expert Services offers several services to help organization clean up all varieties of outbreaks, including W32/Nachi.worm. If your customer seems to be struggling, engaging services is a way to provide them a complete and expedient solution to their virus problem. Our emergency outbreak services provide swift detection and cleanup of viruses. Specific to W32/Nachi.worm, our services can detect the worm with Sniffer technology and detect and contain with vulnerability assessment, firewalls, and coordination with their security team.

The impact of this virus also highlights the need for Threat Assessment services. This service provides a review of their anti-virus products, policies and processes, a vulnerability scan of mission critical servers and a scan of random nodes to determine the organization's exposure to threats, a review of their change management procedures and policies, and incident response planning.

For more information contact your local services representative.