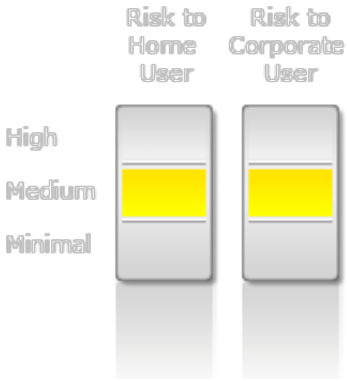

McAfee
SECURE
TESTED 26-AUG



W32/Nachi.worm

This page shows details and results of our analysis on the malware W32/Nachi.worm

- Download Current DAT: **6449**

Threat Detail

Malware Type: Virus

Malware Sub-type: Internet Worm

Discovery Date: 2003-08-18

Next Steps:

- Search Again
- View All Threats
- Sign Up for McAfee Labs Security Advisories

Overview

This is a virus detection. Viruses are programs that self-replicate recursively, meaning that infected systems spread the virus to other systems, which then propagate the virus further. While many viruses contain a destructive payload, it's quite common for viruses to do nothing more than spread from one system to another.

Minimum DAT	Minimum Engine	Description Added
4286 (2003-08-18)	5.1.00	2003-08-18
Updated DAT	**File Length**	**Description Modified**
4299 (2003-10-22)	10,240 bytes (UPXed)	2004-02-23

Malware Proliferation

Characteristics

-- Update 3 January 2004 --
The risk assessment was lowered to Low-Profiled due to the self-removal routine of the worm. Infected systems that haven't been rebooted since the start of 2004, or computers with incorrect system clocks may still emit Nachi worm traffic.

-- Update 21 October 2003 --
4299+ DATs improve the reporting of the renamed tftpd.exe file. Instead of W32/Nachi.worm it will be reported as W32/Nachi!tftpd to distinguish this renamed system file from the worm itself.
--

This detection is for another virus that exploits the MS03-026 vulnerability. In addition to exploiting this RPC DCOM vulnerability, the virus also attempts to exploit an NTDLL.DLL vulnerability (MS03-007) via WebDav.

It is not related to the W32/Lovsan.worm.d variant described here .

Intentions of the worm
This worm spreads by exploiting a hole in Microsoft Windows. It instructs a remote target system to download and execute the worm from the infected host. Once running, the worm terminates and deletes the W32/Lovsan.worm.a process and applies the Microsoft patch to prevent other threats from infecting the system through the same hole. When the system clock reaches Jan 1, 2004, the worm will delete itself upon execution.

Installation

To ensure only one instance of the worm on the victim machine, a mutex of the following name is created:

```
RpcPatch_Mutex
```

The virus installs itself within a WINS directory in the Windows System directory:

```
C:\WINNT\SYSTEM32\WINS\DLLHOST.EXE (10,240 bytes)
```

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

The virus attempts to copy the TCP/IP trivial file transfer daemon (TFTPD.EXE) binary from the dllcache on the victim machine to this directory also, renaming it:

```
C:\WINNT\SYSTEM32\WINS\SVCHOST.EXE
```

Note: If TFTPD.EXE is not present on the target machine, this copy will fail. TFTPD.EXE only exists by default on specific OSes.

The following services are installed:

1. **RpcPatch** Set to run the installed copy of the worm (DLLHOST.EXE)

   Display name: "WINS Client"

2. **RpcTftpd** Set to run the copy of the TFTPD application (SVCHOST.EXE)

   Display name: "Network Connections Sharing"

Downloading of Patches

The worm carries links to various patches for the MS03-026 vulnerability:

- 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

The worm attempts to download and install one of these patches on the victim machine.

Removal of W32/Lovsan.worm.a
The worm also looks for and removes W32/Lovsan.worm.a from an infected system. It achieves this by targeting MSBLAST.EXE. (The process is terminated if running on the victim machine.) NB: The Registry hook employed by MSBLAST.EXE is not removed by the worm.

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

Symptoms

- large volumes of ICMP traffic in network
- existence of the files and Windows services detailed above

Method of Infection

This worm spreads by exploiting a vulnerability in Microsoft Windows. Target machines are selected by scanning Class-B sized subnets based on the local subnet, and IP addresses constructed from a list of hard-coded addresses (first two octets) carried in the worm.

To check whether the target machine is on the network, the worm sends an ICMP ping to potential victim machines, and upon a reply, sends the exploit data. A remote shell is created on the target system which connects to the infected machine on a TCP port in the range 666-765. Victim machines are instructed to download the worm via TFTP.

Irrespective of anti-virus detection, unless the system has been (MS03-026) patched, it is susceptible to the buffer overflow attack from an infected host machine. An infected machine will send packets across the local subnet to the RPC service running on port 135. When these packets are received by any unpatched system, it will create a buffer overflow and crash the RPC service on that system. All this can occur without the worm actually being on the machine.

By applying the MS03-026 patch to the machine, it will prevent the RPC service from failing, in-turn solving these symptoms. It is very important that the machine is rebooted after the patch has been installed.

Web servers (IIS 5) that are vulnerable to an MS03-007 attack (port 80), via WebDav, are also vulnerable to the virus propagating though this exploit.

Removal

Microsoft Patches
It is imperative that infected systems are patched prior to disinfecting a system. As for the W32/Lovsan.worm, some systems may be in a crash loop where each time the system is restarted, SVCHOST.EXE crashes and the user has 60 seconds before the system restarts. This action can continue to happen even after the virus is removed if the patch is not applied. It may be necessary to install/configure a firewall prior to downloading/installing this patch. Microsoft has outlined the necessary steps to address Windows issues when removing this virus. These actions should be taken prior to removing the virus (see below).

DAT Files
Detection is included in the 4286 DAT files . The 4.1.60 scan engine is capable of detection, however the 4.2.40+ scan engine is required for repair. Additionally, services removed by the cleaning process may still appear in the Services Control Panel / Snap In, until a reboot has occurred. This is not an indication that a reboot is required to delete the necessary files or registry keys, simply that Windows will still show the service as being present until after the reboot has happened. Run an **On-demand** scan after applying the Microsoft patch and updating to the required DAT files.

Stand alone remover
Stinger has been updated to include detection/removal of this threat.

Sniffer Customers: A new filter has been developed that will look for any traffic exploiting the RPC Exploit, plus traffic on port 4444 (Lovsan) and traffic on 707 (Nachi) (Sniffer Distributed 4.3 and Sniffer Portable 4.7.5).

Manual Removal Instructions

To remove this virus "by hand", follow these steps:

1. Apply the MS03-039 patch (includes MS03-026 patch)
2. Terminate the following services :
    1. WINS Client
    2. Network Connections Sharing
3. Delete the **DLLHOST.EXE** and **SVCHOST.EXE** files from the WINS directory with your WINDOWS SYSTEM32 directory. For example, c:\winnt\system32\wins\svchost.exe.

    Note: a legitimate system file exists with the filename DLLHOST.EXE, which must not be deleted.

4. Edit the registry to:
    - Delete the "RpcPatch" key from
        - HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services
    - Delete the "RpcTftpd" key from
        - HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services

Additional Windows ME/XP removal considerations

Desktop Firewall Users
The default McAfee Desktop Firewall policies will prevent Nachi from spreading, by blocking the ICMP request used by the virus to find other vulnerable systems and blocking the TFTP traffic generated by infected systems. Unless you have created specific rules to allow these types of traffic, systems are protected without any action required. If you do need to make a policy change, it can be done quickly and easily from a central location with ePolicy Orchestrator.

Threatscan Users
There are two ways of using ThreatScan with regards to the Nachi worm. The first is to detect the Vulnerability that the worm uses to exploit the machine. Finding the vulnerable machines and patching them will help prevent this worm from interfering with your business. To find machines that are vulnerable to being exploited by this worm, ensure that your ThreatScan installation is up to date and then follow the steps below under the heading:

To scan for the MS03-026 (Q823980) vulnerability.

The other way is to detect machines that are already infected by this worm. To do this you will ensure that your ThreatScan installation is up to date, and then follow the steps below under the heading: To scan for the Nachi virus infection. This method will allow you to look for machines that are running the one of the services that this worm creates.

To update your ThreatScan installations with the latest signatures perform the following tasks:

-From within ePO open the Policies tab.
-Select McAfee ThreatScan and then select Scan Options
-In the pane below click the Launch AutoUpdater button.
-Using the default settings proceed through the dialogs that appear. Upon successful completion of the update a message will appear stating that; update 2003-08-12 has completed successfully.

- From within ePO create a new AutoUpdate on Agent(s) task.
-Go into the settings for this task and ensure that the host field is set to *ftp.nai.com* , the path is set to */pub/security/tsc20/updates/winnt/* and that the user and password fields are both set to *ftp* .Note that tsc20 in the above path is used for ThreatScan 2.0 and 2.1.The correct path for ThreatScan 2.5 is tsc25.

-Launch this task against all agent machines.
-When the task(s) complete information will be available in the Task Status Details report.

To create and execute a new task to check for Nachi do the following:

To scan for the MS03-026 (Q823980) vulnerability:

-Create a new ThreatScan task.
-Edit the settings of this task.
-Edit the Task option, Host IP Range to include all desired machines to scan.
-Select the Remote Vulnerability Detection category and Windows Client Vulnerabilitiestemplate. -or-
-Select the Remote Vulnerability Detection category and Sans/FBI List template. -or-
-Select the Other category and Scan all Vulnerabilities template.
-Launch the scan.

To scan for the Nachi virus infection:

-Create a new Resource Discovery task.
-Edit the settings of this task.
-Edit the Task option, Host IP Range to include all desired machines to scan.
- Select only the Windows Service Scan option.
-Launch the scan.

For additional information regarding the vulnerability:

-Look for module number 29055 in generated ThreatScan report.

For additional information regarding possible infection:

- Export the generated Resource Discovery report and search for the following sentences:

WINS Client
Network Connections Sharing

Variants

- Careers
- Contact Us
- Website Feedback
- Legal Notices
- Legal & Contract Terms
- Site Map
-

United States - English

- América Latina - Español
- Australia - English
- Brasil - Português
- Canada - English
- Canada - Français
- China - 中国 (Simplified Chinese)
- Czech - Čeština
- Danmark - Dansk
- Deutschland - Deutsch
- España- Español
- France - Français
- Hong Kong - English
- India - English
- Italia - Italiano
- Japan - 日本 (Japanese)
- Korea - 한국 (Korean)
- México - Español
- Nederland - Nederlands
- Norge - Norsk
- Polska - Polski
- Portugal - Portuguese
- Russia - Русский (Russian)
- Sverige - Svensk
- Singapore - English
- Taiwan - 台灣 (Traditional Chinese)
- Turkey - Türkiye
- United States - English
- United Kingdom - English