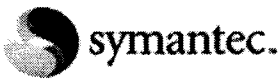

Symantec Security Response
http://securityresponse.symantec.com

W32.Nimda.A@mm

Discovered on: September 18, 2001
Last Updated on: September 20, 2001 at 01:32:14 PM PDT

Symantec Security Response has received a number of submissions on W32.Nimda.A@mm and is rating it as a Category 4.
Symantec Security Response has posted a tool to remove infections caused by W32.Nimda.A@mm. Please go here to download the tool.

Virus Definitions may be downloaded using LiveUpdate or from the Symantec Security Response Web site at this location.

W32.Nimda.A@mm is a mass-mailing worm that utilizes multiple methods to spread itself. The worm sends itself out by email, searches for open network shares, attempts to copy itself to unpatched or already vulnerable Microsoft IIS web servers, and is a virus infecting both local files and files on remote network shares.

The worm uses the Unicode Web Traversal exploit. A patch and information regarding this exploit can be found at http://www.microsoft.com/technet/security/bulletin/ms00-078.asp.

When the worm arrives by email, the worm uses a MIME exploit allowing the virus to be executed just by reading or previewing the file. Information and a patch for this exploit can be found at http://www.microsoft.com/technet/security/bulletin/MS01-020.asp

If you visit a compromised Web server, you will be prompted to download an .eml (Outlook Express) email file, which contains the worm as an attachment. You can disable "File Download" in your Internet Explorer internet security zones to prevent this compromise.

Also, the worm will create open network shares on the infected computer, allowing access to the system. During this process the worm creates the guest account with Administrator privileges.

NOTE: Microsoft has released a cumulative roll up for IIS 4.0 on NT 4.0 SP5 and later as well as all security patches released to date for IIS 5.0. This can be found at http://www.microsoft.com/technet/security/bulletin/MS01-044.asp.

Also Known As: W32/Nimda@mm, PE_NIMDA.A, I-Worm.Nimda, W32/Nimda-A, Win32.Nimda.A

Type: Virus, Worm

Infection Length: 57344

Virus Definitions: September 18, 2001

Threat Assessment:

Wild:	Damage:	Distribution:
High	Medium	High

Wild:

- Number of infections: More than 1000
- Number of sites: More than 10
- Geographical distribution: Medium
- Threat containment: Moderate
- Removal: Moderate

Damage:

- Payload:
  - Large scale e-mailing: Uses MAPI to send itself out as Readme.exe (Readme.exe may NOT be visible as an attachment in the email received)
  - Modifies files: Replaces multiple legitimate files with itself.
  - Degrades performance: May cause system slowdown
  - Compromises security settings: Opens the C drive as a network share

Distribution:

- Name of attachment: README.EXE (This file may NOT be visible as an attachment in the email received)
- Size of attachment: 57344
- Shared drives: Opens network shares
- Target of infection: Attempts to infect unpatched IIS servers

Technical description:

Infection by way of a Web Server

W32.Nimda.A@mm attempts to infect unpatched Microsoft IIS web servers. On Microsoft IIS 4.0 and 5.0, it is possible to construct a URL that would cause IIS to navigate to any desired folder on the logical drive that contains the web folder structure, and access files in it. A patch and information regarding this exploit can be found at http://www.microsoft.com/technet/security/bulletin/ms00-078.asp.

Successful exploitation of the Directory Traversal Vulnerability gives the attacker the ability to install and run code, as well as add, change or delete files or web pages on the compromised server. The limitations of the original vulnerability include:

1. The server configuration. The vulnerability only allows files to be accessed if they reside on the same logical drive as the web folders. For example, if a Web administrator had configured the server so that the operating system files were installed on the C drive and the Web folders were installed on the D drive, the attacker would be unable to use the vulnerability to access the operating system files.
2. The attacker must be logged onto the server interactively.
3. The privileges gained would be only those of a locally-logged-on user. The vulnerability only would allow the malicious user to take actions in the context of the IUSR_machinename account.

However, by using the W32.Nimda.A@mm worm as a delivery mechanism, the attacker is able to compromise a vulnerable IIS server remotely and once compromised, create a local account on the targeted server with administrator privileges **regardless of which drive the IIS server is installed**

on. The worm uses directory traversal techniques to access cmd.exe on unpatched IIS servers. The worm also attempts to use IIS servers that had previously been compromised by CodeRed II to propagate and to access root.exe from the inetpub/scripts directory.

The worm searches for Web servers using randomly generated IP addresses. Using the Unicode Web Traversal exploit, the worm copies itself to the Web server as admin.dll via TFTP. Infected machines create a listening TFTP server (port 69/UDP) to transfer copy of the worm.

This file is then executed on the Web server and copied to multiple locations. In addition to this exploit, the worm attempts to exploit already compromised web servers using the files root.exe or cmd.exe that are located in remotely executable web directories.

The worm then attempts to modify files named default, index, main or readme, or files with the extensions .htm, .html, or .asp, by adding JavaScript. The JavaScript causes visitors who open infected pages to be presented with Readme.eml, which was created by the worm. Readme.eml is an Outlook Express email file with the worm as an attachment. The email messages utilizes the MIME exploit. Thus, a computer may be infected simply by browsing the infected Web page.

System Modifications

When executed the worm determines from where it is being executed. The worm then overwrites Mmc.exe in the \Windows folder, or creates a copy of itself in the Windows Temporary folder.

The worm then infects executables, creates itself as .eml and .nws files, and copies itself as Riched20.dll in folders that contain .doc files on the local drive. The worm searches for files in the paths listed in the registry keys:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\
Windows\CurrentVersion\App Paths

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\
Windows\CurrentVersion\Explorer\Shell Folders
```

The worm hooks the system by modifying the System.ini file as follows:

```
Shell = explorer.exe load.exe -dontrunold
```

It also replaces the file Riched20.dll. Riched20.dll is a legitimate Windows .dll file that is used by programs such as Microsoft Word. By replacing this file, the worm is executed each time programs such as Microsoft Word are executed.

The worm also registers itself as a service process or adds itself as a remote thread to the Explorer process. This allows the worm to continue to execute even when a user is not actively logged on.

The worm copies itself as the file:

%Windows\System%\load.exe

NOTE: %Windows\System% is a variable. The worm locates the \Windows\System folder (by default this is C:\Windows\System) and copies itself to that location

Next, the worm creates open network shares for all drives on the computer by modifying the registry key:

```
HKLM\Software\Microsoft\Windows\
CurrentVersion\Network\LanMan\[C$ -> Z$]
```

A reboot of the computer is required for these settings to take effect.

The worm searches for all open shares on the network by iterating through Network Neighborhood and by utilizing randomly generated IP addresses. All files on any open network shares are examined for possible infection. All .exe files are infected by the worm except Winzip32.exe.

Next, .eml and .nws files are copied to the open network shares and the worm copies itself over as Riched20.dll to any folder that contains .doc files.

The worm changes Explorer settings to not show hidden files and known file extensions.

The worm adds the user Guest under the groups Guests and Administrators. This gives the guest account Administrative privileges. In addition, the worm actively shares C$ = C:\ No reboot is required.

Mass-Mailer

The worm begins the mass-mailing routine by first searching for email addresses. The worm searches for email addresses in .htm and .html files on the local system. The worm also uses MAPI to iterate through all messages that are contained in any MAPI-compliant email clients. Any MAPI supporting email clients may be affected including Microsoft Outlook and Outlook Express. The worm uses these email address for the To: and the From: addresses. Thus, the From: addresses will not be from the infected user.

The worm uses its own SMTP server to send out emails using the configured DNS entry to obtain a mail server record (MX record).

When the worm is received by email, the worm uses a old known MIME exploit to auto-execute itself. The worm will be unable to execute using Microsoft Outlook or Outlook Express if the system has been patched against this exploit. Information regarding this exploit can be found at http://www.microsoft.com/technet/security/bulletin/MS01-020.asp

Infecting Executables

The worm also attempts to infect .EXE files. First, the worm checks to see if the file is already infected. If the file is not infected the worm makes a copy of itself in the Temporary directory. The victim file is embedded inside the copy. This new file is then copied over the victim file replacing the originally clean file with an infected version. Infected executables will be approximately 57344 bytes larger. When an infected file is executed, the worm will extract the original clean file to a temporary file and execute it along with itself. Thus, one may not notice their executable has become infected.

During execution, the worm may attempt to delete copies of itself. If the file is in use or locked, the worm will create WININIT.INI with an entry to delete itself upon reboot.

When infecting files, the worm may create two temporary files in the Windows Temporary folder as:

- mep[nr][nr][letter][nr].TMP.exe
- mep[nr][nr][letter][nr].TMP

Both files will be hidden and have the system attribute set.

The worm contains bugs and can be resource intensive. Thus, not all actions may occur and system instability may be noticeable.

Removal instructions:

Symantec Security Response has posted a tool to remove infections caused by W32.Nimda.A@mm. Please go here to download the tool.

NOTE: Once a computer has been attacked by W32.Nimda.A@mm, it is very difficult to determine what security settings have been compromised. Unless, by reading the logs, you can be absolutely sure that nothing else malicious has been done to the computer, it may be best to backup all data files, reformat the hard drive, and then completely reinstall the operating system and all programs. This is the only way that you can be 100 percent certain that the computer is clean.

Manual Removal Instructions

If you cannot obtain the removal tool, or if it does not work in your situation, follow these steps:

1. Run LiveUpdate to make sure that you have the most recent virus definitions.
2. Do one of the following:
   - If you are running Windows NT/2000/XP, skip to step 3.
   - If you are running Windows 95/98/Me, edit the System.ini file as follows:
     1. Click Start, and click Run.
     2. Type the following, and then click OK:

        ```
        edit c:\windows\system.ini
        ```

        The MS-DOS Editor opens.

        NOTE: If Windows is installed in a different location, make the appropriate substitution.

     3. Locate the line that begins with shell=\
     4. Position the cursor immediately to the right of the equal sign.
     5. Press Shift+End to select all of the text to the right of the equal sign, and then press Delete.
     6. Type the following text:

        ```
        explorer.exe
        ```

        The line should now look like:

        shell=explorer.exe

        NOTE: Some computers may have an entry other than Explorer.exe after shell=. If this is the case and you are running an alternative Windows shell, then change this line to shell=explorer.exe for now. You can change it back to your preferred shell after you have finished this procedure.

     7. Click File, click Exit, and then click Yes when you are prompted to save the changes.

3. If AutoProtect is not enabled, enable it before restarting the computer. For instructions on how to do this please read the document How to enable and disable Norton AntiVirus Auto-Protect.
4. Restart the computer.

NOTE: When your computer restarts, it is likely that infected files will be found. We recommend that you attempt to repair the infected file. Quarantine any file that is not repairable.

5. Start Norton AntiVirus (NAV), and make sure that NAV is configured to scan all files. For instruction on how to do this, read the document How to configure Norton AntiVirus to scan all files.
6. Scan your system with NAV. For instruction on how to run a scan with NAV, read the document How to scan for viruses.
7. For each file detected as infected by W32.Nimda.A@mm or W32.Nimda.A@mm (html), choose Repair. Quarantine any file that is not repairable.
8. For each file detected as infected by W32.Nimda.A@mm (dr), W32.Nimda.enc, W32.Nimda.A@mm (dll), choose Delete.
9. Restore Admin.dll and Riched20.dll from backup, or from the Microsoft Windows or Office .cab files if necessary.
10. Remove unnecessary shares.
11. Delete the guest account from the Administrators group (if applicable).

Additional information:

Norton AntiVirus
Norton AntiVirus is the world's most trusted anti-virus solution. Now it repairs common virus infections automatically, without interrupting your work. Automatic updating of virus definitions over the Internet is just as easy. Symantec's exclusive Script Blocking technology defends against fast-moving threats by identifying and stopping new script-based viruses such as "ILoveYou" even between virus definition updates. To safeguard your PC and prevent it from spreading viruses to your friends and colleagues, Norton AntiVirus scans and cleans both incoming and outgoing email. And for instant access to the most-needed functions, it integrates into Windows Explorer. If you do not have anti-virus software, protect your computer from worms and viruses with Symantec's award-winning Norton AntiVirus 2002.

Norton Internet Security
Norton Internet Security is the integrated online security suite from Symantec. The Norton Internet Security suite includes Norton AntiVirus, Norton Personal Firewall, Norton Privacy Control and Ad Blocking. The ability to easily update the suite (for the latest virus definitions, firewall rules, etc.) via LiveUpdate ensures that Norton Internet Security continues to provide security to the user's computer from the latest online threats.

Symantec Enterprise Firewall
Symantec Enterprise Firewall and Raptor Firewall will, through proper configuration, analyze HTTP requests and responses to ensure they adhere to the Requests for Comments (RFC) defining Web protocol behavior. This mechanism effectively blocks many common attacks that take advantage of protocol violations. In addition, Symantec Enterprise Firewall/Raptor Firewall version 6.5 or later can be configured to use URL pattern matching on rules to block against quantified threats on specific web server platforms.

Symantec Enterprise Security Manager (ESM)
Symantec Enterprise Security Manager is a scalable security policy compliance and host-based vulnerability assessment tool. Using this tool you can detect systems that are running IIS server, detect systems that have the web Directory Traversal Vulnerability and can also detect modified files, new files and deleted files through its 'tripwire-like' snapshot technology. It can also detect other modifications in the registry, useful in forensic analysis. If you have not already deployed ESM within your enterprise it is of limited use in recovering from a widespread compromise like W32.Nimda.A@mm. However, it has tremendous strength in mitigating the risk of the next W32.Nimda.A@mm type worm since it enforces best practices, e.g., identifying inadequate patch levels, unneeded services, and weak passwords.

Symantec NetRecon
Symantec NetRecon is a network vulnerability assessment scanner with root cause analysis capabilities. It detects systems that are running Web services – specifically Microsoft IIS and also detect systems that have the web Directory Traversal Vulnerability.

Symantec NetProwler
NetProwler is Symantec's network-based intrusion detection tool that continuously and transparently monitors your network for pattern of misuse or abuse. With Security Update 8 installed, NetProwler will detect the CodeRed worm and variants operating on your network. The NetProwler logs will identify each system compromised by the W32.Nimda.A@mm worm. NetProwler can also assist in forensic analysis by reviewing log entries to provide clues as to which host(s) on the network were first compromised by the worm.

Symantec Intruder Alert
Intruder Alert is a host-based Intrusion detection tool that detects unauthorized and malicious activity, keeping systems, applications, and data secure from misuse and abuse. The FileWatch function in Intruder Alert can monitor and detect mission-critical files for any changes, deletions, or movements that may have resulted from unauthorized access after W32.Nimda.A@mm compromise. In addition, Intruder Alert provides utilities to develop custom rules that can restore the compromised/changed files to their original state. Intruder Alert also monitors a system for suspicious behavior such as rootkit or DDoS agent installation, account creation, or modification. Intruder Alert can centrally manage log file events from across the network to assist in forensic analysis of compromised systems.

Write-up by: Eric Chien