Global Information Assurance Certification Paper

W32/Nimda.A.mm Worm Analysis Practical

GIAC Certified Incident Handler (GCIH)
Version 1.5c

November 11, 2001

Submitted by: Christine Vecchio-Flaim

Exploit Details

W32/Nimda.A.MM Worm

The W32.Nimda.A@mm is a mass-mailing worm that began spreading on September 18th, 2001 at 8:30am. This self-propagating worm quickly infected PCs and servers around the globe in many cases causing Denial of Service (DoS) to servers. The name Nimda is the reverse spelling of "admin". The Nimda worm is the first worm that utilizes four methods to infect PC's running Microsoft Windows and IIS Web Servers. It combines the most successful features of the Code Red, Kournikova, ILOVEYOU, and Melissa viruses.

The Nimda worm was responsible for problems at large corporations such as Siemens, US Bancorp, Booze Allen & Hamilton, and General Electric. Reportedly, the Nimda worm made its way into over one million computers in the USA, Europe, and Asia.

Name: W32.Nimda Worm

Exploit: Unicode Web Traversal, Escaped Character Decoding, MIME, Open Network Shares

Alias:

Concept5
Code Rainbow
Minda

Variants :

W32/Nimda.b@MM
W32/Nimda.c@MM
W32/Nimda.d@MM
W32/Mimda.e@MM
W32/Nimda.f@MM
W32/Nimda.g@MM

Protocols/Services: HTTP, SMTP, TFTP, NetBIOS

Operating Systems: Win 9X/ME/NT/2000/IIS Servers

Advisories:

National Infrastructure Protection Center Advisory 01-022, September 18th, 2001

Carnegie Mellon CERT Coordination Center Advisory CA-2001-26, September 18th, 2001

Protocol/Services Description

Hypertext Transfer Protocol (HTTP)

HTTP is the set of rules for sharing files on the Internet including text, images, and multimedia files. This is an application-level protocol which is generic, stateless, object-oriented and can be used for many tasks. An important feature of HTTP is that it allows systems to be built independently of the data being transferred.

The Nimda worm can exploit the following HTTP security vulnerabilities in IIS Web Servers.

- Microsoft IIS 4.0/5.0 File Permission Vulnerability
- Microsoft IIS/PWS Escaped Characters Decoding Command Execution Vulnerability
- Microsoft IIS and PWS Extended Unicode Directory Traversal Vulnerability

Trivial File Transfer Protocol (TFTP)

TFTP is a file transfer protocol that provides its delivery with the User Datagram Protocol (UDP) as its transport protocol. TFTP provides performance over paths that have a small delay bandwidth product. The TFTP file interface is very simple, providing no access control or security.

The Nimda worm uses Unicode exploit to copy itself to the Web Server as admin.dll via the TFTP protocol. Infected machines also create a listening TFTP server (Port 69/UDP) to transfer a copy of the worm.

Simple Mail Transfer Protocol (SMTP)

SMTP is a TCP/IP protocol used in sending and receiving email. It is normally used in conjunction with either the POP3 protocol or the Internet Message Access Protocol (IMAP). Typically, SMTP is used for sending email and either POP3 or IMAP is utilized for receiving messages. The Nimda worm utilizes its own SMTP code to email copies of itself to email addresses found on the infected computer.

Network Basic Input/Output System (NetBIOS)

NetBIOS allows applications on different computers to communicate within a Local Area Network (LAN). NetBIOS provides the session and transport services described in the

Open Systems Interconnection (OSI) model. NetBIOS must use another transport mechanism such as the Transmission Control Protocol (TCP) on a Wide Area Network (WAN) because it does not support a routing mechanism.

The Nimda worm exploits the NetBIOS protocol to access open file shares and infect files over a Local Area Network.

Description of Variants

W32/Nimda.b@MM

In this version of Nimda, the file has been compressed by PCShrink Win 32 PE EXE file compressor and is considerably smaller that W32/Nimda.A.mm. This variant does not infect files; it overwrites them with the virus.

Additionally, the filenames README.EXE and README.EML have been replaced with PUTA!!.SCR and PUTA!!.EML.

W32/Nimda.c@MM

This version is identical in functionality and file names as the W32/Nimda.A.mm version but is compressed by the UPX compressor.

W32/Nimda.d@MM

This version of the worm was mailed to the Internet at the end of October 2001. This file was compressed from the PECompact compressor.

The copyright text is replaced with:

Holocaust Virus.! V.5.2 by Stephan Fernandez.Spain

W32/Nimda.e@MM

This is a recompiled Nimda variant. This variant uses different filenames to mimic Windows filenames and reduce the chances of being alerted by anti-virus scans. In this version, the README.EXE is now SAMPLE.EXE, MMC.EXE is now CSRSS.EXE, and ADMIN.DLL is now HTTPODBC.DLL. This version had several minor routines fixed or optimized.

The copyright text is replaced with:

Concept Virus (CV) V.6, Copyright © 2001, (This's CV, No Nimda)
.

W32/Nimda.f@MM

This variant is functionally the same as the D variant.

How the Exploit Works

Methods of Propagation

The Nimda worm is complex because it propagates through a variety of methods. The most significant methods are as follows:

Mass Email

The worm locates email addresses from the email client and by searching local .HTML files. It sends an email that contains a README.EXE attachment to each address it locates. The subject of the email varies and the sender's identity may be spoofed to make it appear to come from a trusted source. The body of the email appears to be empty but actually contains code to use an exploit that will execute the virus when the user views the message.

The email propagation of the Nimda worm is reactivated every ten days after the original activation. Every ten days, the worm collects email addresses from the default Message Application Program Interface (MAPI) client and Internet Explorer cache and tries to mail itself to the addresses found. Nimda uses it's own SMTP protocol email code and completely circumvents the client email program.

LAN

The worm will search for open file shares in the local network. When an open file share is found, either on a file server or on a workstation, Nimda will put a hidden file called RICHED20.DLL into any directory that has DOC and EML files. Subsequently, when a user opens a DOC or EML file from these directories, Microsoft Word, WordPad, or Outlook will execute RICHED20.DLL causing an infection on the users machine. If the worm is started on a server, it will also infect remote files.

Nimda also searches the open network shares for EXE files. When found, the worm infects these files. The worm appends the code of the .EXE file and modifies its resources so the program uses the same icons as the original program. Any other host that accesses the share and loads one of these files can also become infected.

Web Server Attacks

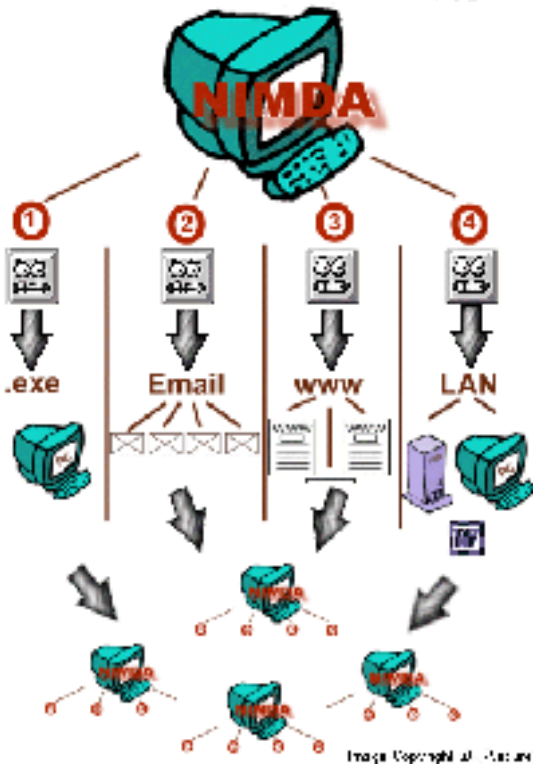
The Nimda worm searches the Internet via randomly selected IP addresses looking for vulnerable Microsoft Web servers. The worm specifically searches for Web Servers that have previously been compromised by the Code Red II and Sadmind infections. The scanning is performed by the worm's own copy of

MMC.EXE. Infected computers that are performing these scans will experience degradation of their system performance when this process is running. The worm will also copy itself as ADMIN.DLL to the root directories of accessible drives. It attempts to gain control of Web Servers using the Extended Unicode Directory Traversal, File Permission Canonicalization Vulnerability, and the Escaped Character Decoding vulnerabilities in IIS.

Once the worm gains control over the server, the worm uses TFTP to transfer its code from the attacking machine to the compromised Web Server.

Web Browsing Code

If the worm is successful in compromising a server, it uses the HTTP service and Multipurpose Internet Mail Extensions (MIME) vulnerability to propagate itself to clients that browse the Web Servers pages The TFTP protocol is used to transfer its code to the compromised web server. The worm searches the Web Server directory for files with HTM, HTML, and ASP extension. Nimda will append each of these files with a JavaScript that forces a download of README.EML to any client that views the file via a vulnerable browser. As a result, users who visit these infected web servers can also fall victim to the NIMDA worm.



Step-by-Step Analysis of the Nimda Worm

Nimda on Windows 95/98/NT/2000 Workstations

The workstation receives an infected file named README.EXE that is attached to an email message. If the user is using an unpatched version of Outlook or Outlook express, the README.EXE file will automatically execute if:

Using Outlook – the user opens the email.
Using Outlook Express – if the user previews the email.

The worm executes the README.EXE file and is copied to a temporary folder with a random name that includes MEP*.TMP. The worm runs itself with the "–dontrunold" command line option and is loaded as a Dynamic Link Library (DLL).

The worm begins running its propagation and payload routines. Nimda searches for the EXPLORER process to utilize for this purpose. Dependent upon the Windows version, the worm may run its own routines as a background process of Explorer.

Nimda prepares a Multipurpose Internet Mail Extension (MIME) encoded copy with a random name and places it in a temporary folder. MIME is a specification for formatting non-ASCII messages so they can be sent over the Internet.

Nimda creates a Mutual Exclusion Object (mutex) named "fsdhqherwqi2001". A mutex is a program object that allows multiple program threads to share the same resource, such as file access. This mutex starts Winsock services and obtains the host information from the infected computer.

When the worm resumes, it checks to see what platform is running and copies itself as LOAD.EXE in the Windows system directory. It also modifies the SYSTEM.INI file by adding "explorer.exe load.exe –dontrunold" after SHELL=variable in the [Boot] portion of the SYSTEM.INI file. This string will ensure that worm will start each time that Windows starts.

The worm will also copy itself as RICHED20.DLL to the system folder. Nimda sets hidden and system attributes to this file as well as to the LOAD.EXE file. The worm then scans shared network resources looking for .DOC and .EML files. The worm copies its image with the name RICHED20.DLL into the directories where these files are located. The infected RICHED20.DLL file will be used to open OLE files from the directory that it is launched.

Nimda creates EML and NWS files while browsing the remote computer's directories using the names of documents or Web page files that the worm found on the remote system. These EML and NWS files are multi-partite messages with a worm MIME-encoded in them. Nimda can delete the messages it previously created.

When started from a workstation, Nimda does not attempt to infect other .EXE files on the system.

The worm will create open network shares on the infected computer, allowing full access to the system. During this process the worm activates the Guest account with Administrator privileges. This account is given a blank password and Administrator rights. It also shares the C:\ drive with full privilege and disables sharing security.

The Nimda worm on Windows 9X/ME/NT/2000 systems creates hidden file shares. The shares are c$=c:\ through z$=z:\ are normally accessible only to members of the Administrator group and are created only for drive letters that exist on the system. The Nimda worm gives full access to these shares to everyone with access to the system.

Nimda scans HTM and HTML files, the email client inbox and address book, and temporary Internet directories searching for email addresses to further its spread. When completed the worm creates a list and sends out the infected message to the addresses in the list. It uses its own version of the SMTP protocol to send the infected messages and as a result is able to replicate regardless of the type of email client that is installed on the infected host. It can replicate even if the host has no email client installed. The Nimda worm email propagation event is reactivated every ten days after the original activation.

The infected messages are in HTML format. The subject line may be empty or may be a random name collected from the name of a file from the "My Documents" directory of the host computer.

Sample Message Header

Subject: (Empty or Random)
Message Text: (Empty)
Attachment: README.EXE

It is important to note that the malicious JavaScript may also affect the auto-signature HTML file in the client email program. If this is the case, all messages from the infected machine will have the worm's JavaScript attached to the end of the signature. This would allow the worm to spread in the same manner as the "KakWorm". The KakWorm attached itself to all outgoing messages using the signature feature of Outlook Express and Internet Explorer newsgroup reader.

Nimda also scans the Internet using random IP addresses. It is specifically looking for existing backdoors (like the ones installed by Code Red II and Sadmind) on IIS servers. When a backdoor is found, Nimda instructs the machine to download the infected file ADMIN.DLL from the infected system and executes the worm on the target machine.

Nimda on Servers

In most cases, the Nimda worm stars as the ADMIN.DLL file on infected servers. The server downloads this file from an infected server using TFTP. If the ADMIN.DLL file is located on the server, the worm creates a mutex with the name "fsdhqherwqi2001". It copies itself as MMC.EXE into the Windows directory and starts the file with the "-qusery9bnow" command line.

Nimda will activate the Guest account and add it to the Administrator group and will open the C drive with full share privileges.

The worm scans and infects all files on all accessible drives including any removable and network drives. The EXE files on all drives will be infected with the exception of the WINZIP32.EXE file. The virus does not infect any files larger than 8,338,608 bytes.

Nimda reads all subkeys from the Windows Application Paths software registry and infects all files listed in the subkeys. It also scans for user's personal folders and infects the files in these folders.

The worm modifies all HTML, ASP, and HTM files with a small malicious JavaScript code and creates a README.EXE files in these directories. This code will automatically download the README.EXE file when a web browser loads the infected HTML file. The Nimda virus will then infect users that are browsing with certain un-patched versions of Internet Explorer.

Nimda will put EML and NWS files in almost all folders of computers it accesses. The RICHED20.DLL files will be placed in all directories where DOC or EML files are found and Nimda will attempt to replace the original Windows RICHED20.DLL with its own infected version.

The worm will then begin scanning for other servers to infect. When these servers are found, the process is repeated in the newly infected server.

Signature of the Attack - Evidence of a Nimda Infection

The Nimda worm can be difficult to detect because the infections are different dependent upon the name of the file that started the infection process. Additionally, the Nimda worm attempts to hide itself on the infected system. The best way to test a system is to run an anti-virus scanner on the system to test for infected files.

Nimda changes registry entries that control viewing hidden files and extensions. It is therefore necessary to choose the View, Folder Options, View Tab in the Windows Explorer when looking in directories. Check these settings whenever you search a different directory. Nimda will continue to change the settings back to the hidden, so you must check the settings each time you begin a new directory search. If you change these settings and a few minutes later find out that the same directory has been changed back, it is a good indication that the worm is active in your system.

The worm has a copyright text string that is never displayed but reads, "Concept Virus (CV) V.5, Copyright ©2001 R.P. China".

IIS Web Servers

An infected Web Server will experience a dramatic increase in outbound traffic originating from the infected server. It will also experience an increase in dropped outbound traffic bound for port 80 at the firewall. The firewall may report or display unusual activity or cease functioning as a result of high traffic volume.

The server Intrusion Detection System (IDS) may show an increase in IDS alerts matching Unicode and CodeRed signatures. These alerts will have a consistent attacker IP address and inconsistent victim IP addresses.

Check for the admin.dll file in the web server's \scripts directory. This file should be found in the _vti_bin_vti_adm directory because this is the FrontPage extension for administering a website. It should not be found in the \scripts directory.

If the file is found, open the suspect admin.dll file in notepad, you will find the following strings:

(--====_ABC1234567890DEF_====), the string after src= in the <iframe> tag (3Dcid:EA4DMGBP9p), and the name of the attachment (name="readme.exe").

boundary="====_ABC1234567890DEF_===="
X-Priority: 3
X-MSMail-Priority: Normal
X-Unsent: 1

--====_ABC1234567890DEF_====

```
Content-Type: multipart/alternative;
        boundary="====_ABC0987654321DEF_===="

--====_ABC0987654321DEF_====
Content-Type: text/html;
        charset="iso-8859-1"
Content-Transfer-Encoding: quoted-printable


<HTML><HEAD></HEAD><BODY bgColor=3D#ffffff>
<iframe src=3Dcid:EA4DMGBP9p height=3D0 width=3D0>
</iframe></BODY></HTML>
--====_ABC0987654321DEF_====--

--====_ABC1234567890DEF_====
Content-Type: audio/x-wav;
        name="readme.exe"
Content-Transfer-Encoding: base64
Content-ID: <EA4DMGBP9p>
```

Run a search for the RICHED20.DLL and README.DLL in directories that contain .DOC or .EML files. Remember to turn off file hiding to ensure that you see them. Look in the web folders that contain .HTM, .HTML, or .ASP files for README.EML.

Clients

Run a search for the README.EXE in the email attachments directory. Also, look for files in the temporary directory (\temp, \windows\temp, \winnt\temp) with the name MEP*.TMP and MEP*.TMP.EXE. Look for LOAD.EXE in the \windows or \winnt directories. Open the \windows\system.ini file with a text editor like notepad and look for the line: "shell=explorer.exe load.exe -dontrunold". If you find any of these files, your system is infected. You also may experience unexpected launches of Windows Media Player or RealPlayer on infected client machines.

Detecting Infected Packet Traffic

To detect infected packet traffic you must find unique strings. The following strings are detectible in the unpacked ADMIN.DLL and README.EXE executables, and in the infected e-mail message. Some easy to spot markers are the mime tags

(--====_ABC1234567890DEF_====), the string after src= in the <iframe> tag (3Dcid:EA4DMGBP9p), and the name of the attachment (name="readme.exe").

```
boundary="====_ABC1234567890DEF_===="
X-Priority: 3
```

```
X-MSMail-Priority: Normal
X-Unsent: 1

--====_ABC1234567890DEF_====
Content-Type: multipart/alternative;
        boundary="====_ABC0987654321DEF_===="

--====_ABC0987654321DEF_====
Content-Type: text/html;
        charset="iso-8859-1"
Content-Transfer-Encoding: quoted-printable


<HTML><HEAD></HEAD><BODY bgColor=3D#ffffff>
<iframe src=3Dcid:EA4DMGBP9p height=3D0 width=3D0>
</iframe></BODY></HTML>
--====_ABC0987654321DEF_====--

--====_ABC1234567890DEF_====
Content-Type: audio/x-wav;
        name="readme.exe"
Content-Transfer-Encoding: base64
Content-ID: <EA4DMGBP9p>
```

Infected Web server attack packets contain some well-known ISS exploits. The following traffic is used to scan a web server for vulnerability. If a server gives a positive response for any of these attacks, the worm sends over attack code that attempts to download ADMIN.DLL using TFTP from the attacking site.

The scanning activity of the Nimda worm produces the following log entries for any web server listing on port 80/tcp:

```
GET /scripts/root.exe?/c+dir
GET /MSADC/root.exe?/c+dir
GET /c/winnt/system32/cmd.exe?/c+dir
GET /d/winnt/system32/cmd.exe?/c+dir
GET /scripts/..%5c../winnt/system32/cmd.exe?/c+dir
GET /_vti_bin/..%5c../..%5c../..%5c../winnt/system32/cmd.exe?/c+dir
GET /_mem_bin/..%5c../..%5c../..%5c../winnt/system32/cmd.exe?/c+dir
GET
/msadc/..%5c../..%5c../..%5c/..\xc1\x1c../..\xc1\x1c../..\xc1\x1c../winnt/system32/cmd.exe
?/c+dir
GET /scripts/..\xc1\x1c../winnt/system32/cmd.exe?/c+dir
GET /scripts/..\xc0/../winnt/system32/cmd.exe?/c+dir
GET /scripts/..\xc0\xaf../winnt/system32/cmd.exe?/c+dir
GET /scripts/..\xc1\x9c../winnt/system32/cmd.exe?/c+dir
GET /scripts/..%35c../winnt/system32/cmd.exe?/c+dir
```

GET /scripts/..%35c../winnt/system32/cmd.exe?/c+dir
GET /scripts/..%5c../winnt/system32/cmd.exe?/c+dir
GET /scripts/..%2f../winnt/system32/cmd.exe?/c+dir

Note: The first four entries in these sample logs denote attempts to connect to the backdoor left by Code Red II, while the remaining log entries are examples of exploit attempts for the Directory Traversal vulnerability.

How to Protect Against Nimda

It is essential to implement multiple lines of defense for the new generation of exploits, vulnerabilities, and malicious code. The Nimda worm attack utilizes several methods to infiltrate systems and these types of attacks are likely to become more damaging as new variants emerge.

Organizations must employ best practices throughout their networks to assist in the protection against these damaging viruses. It is also important that these best practices be applied to remote/home employees because these systems are often the weak link in an organization's defense strategy.

Patches and Upgrades

The first line of defense is to apply the appropriate patches to servers and systems prior to their infection. Users and systems administrators must maintain vigilance in keeping up with these important security updates.

Patches for Internet Explorer

The Nimda worm can spread itself through email by taking advantage of the MIME exploit. The MIME exploit allows the virus to be executed by reading or previewing the infected email, even if the attachment is never opened. Microsoft Security Bulletin MS01-020 describes the vulnerability that is found in un-patched versions of Internet Explorer but is exploited via email.

These patches will also protect the system from infected Web sites that can pass on the Nimda virus to unsuspecting users browsing the infected Web site. This vulnerability is due to a flaw in Web Server certificate validation that enables spoofing of URLS and is detailed in MS01-027.

Links to appropriate security patches and additional information relevant to the Nimda virus is available at the following website:

http://www.microsoft.com/technet/security/bulletin/MS01-020.asp

A system would be adequately updates by installing any of the following patches:

- Microsoft Security Bulletin MS01-020.
- Microsoft Security Bulletin MS01-027.
- Internet Explorer 5.01 Service Pack 2.
- Internet Explorer 5.5 Service Pack 2.

- Internet Explorer 6. – Note: If you are installing IE 6 as an upgrade on a Windows 95, 98, 98SE or ME system, be sure to select Full Install as the installation type.

In addition, the auto-preview in Outlook and Outlook Express should be disabled in client systems. The "Preview Pane" and "Auto Preview" should be disabled in client systems. Set the Attachment Security option to high. In the tools menu, select Options, and Security and verify "High Security" is enabled. This will verify that you want to open an attachment.

Patches for IIS Web Servers

It is also import that systems administrators apply appropriate patches to IIS 4.0 and 5.0 Web Servers. The Nimda worm attacks these servers in one of two ways.

Nimda first checks to determine if the Code Red II worm previously infected the server. The Code Red worm creates a "back door" that attackers use to gain control of the system. When Nimda finds these "back doors", it is able to infect the system.

A tool is available to remove the back door created by the Code Red II worm. However, the best course of action is to prevent the Code Red II worm altogether, by taking any of the following steps:

- Microsoft Security Bulletin MS01-033 Patch
- Microsoft Security Bulletin MS01-044 Patch
- Windows NT 4.0 Security Roll-up Package
- Running IIS Lockdown Tool in its default mode
- Installing URLScan tool with its default rule set.

If the Nimda worm is unsuccessful infecting the system via a Code Red "back door", it attempts to infect the system utilizing another vulnerability. The Nimda worm uses the Unicode Traversal vulnerability to attempt to infect vulnerable IIS Web servers. The Unicode Traversal vulnerability is explained in Microsoft Security Bulletin MS00-078. The server will not be vulnerable if any of the following patches are applied:

- Microsoft Security Bulletin MS00-057 Patch
- Microsoft Security Bulletin MS00-078 Patch
- Microsoft Security Bulletin MS00-086 Patch

- Microsoft Security Bulletin MS01-026 Patch
- Microsoft Security Bulletin MS01-044 Patch
- Installing Windows 2000 Service Pack 2
- Installing Windows NT 4.0 Security Roll-up Package
- Running IIS Lockdown Tool in its default mode
- Installing URLScan tool with its default rule-set.

Once a server is infected, it attempts to pass the infection to any machines that visit the web sites it hosts. To accomplish this the worm uses the MIME vulnerability discussed in Microsoft Security Bulletin MS01-020. Systems that apply the patches identified in protection of email will also be protected against web browsing infection

Open File Shares

Windows systems are often configured to allow other users to read or write files from them. Machines that are infected with the Nimda worm will search for systems that have been configured to allow anyone to add files to them. When found, Nimda will insert infected files on it.

Prevent spread through file shares by ensuring that your workstations and servers do not have unprotected file shares. Minimize the number of users who can access your system. If you have file shares that you do not need, remove them. If you need to have some, only give the users as few privileges as possible.

Use encryption to protect confidential files. The Nimda worm will share your computer with the world.

Ensure that a strong password is used for the Administrator account for Windows NT and Windows 2000.

Disable the "File Download" in your Internet Explorer security zones to prevent the web browsing compromise.

Antivirus Software

Anti-virus software definitions must be diligently updated at the server and workstation level. New viruses and malicious code appear so often that it is no longer out of the question to update your virus definitions daily. Make sure that all users understand how to update their virus definitions in the office and on their home computers.

Security Awareness and Education

Security awareness and education is critical to your success. Security policies are of no value if employees don't understand them or know that they exist. The end-users must understand what is expected of them and the value of their actions.

Security policies should not be locked up in the security lab. Post them on your company intranet and make them available to all employees.

Ensure that the corporate anti-virus program is easy to understand and use. Users will get frustrated if it is cumbersome to perform virus updates. Consider using an automated process that will upgrade your users as they log in to the network.

A certain amount of creativity is required to implement an effective awareness program that users will respond to. Keep it simple, informative, and fun. Use a system of rewards and recognition to get the attention of your users. Finally, keep your users involved and let them know they have a stake in the success of your information security program.

Suspected Compromise

If a system is suspect to be infected by the Nimda worm, the following steps should be taken.

- Ensure you are using current anti-virus software with updated virus definitions to ensure detection.
- Remove the network connection to the compromised machine.
- Run anti-virus software to confirm the suspected compromise. Make sure your anti-virus software is configured to scan all files.
- If the system has been infected with the Nimda worm you will need to determine whether to attempt to do a manual cleanup or use an automated tool. Instructions and downloads are available at all of the major anti-virus software web sites.

If you decide to perform a manual cleanup the following files must be removed and/or deleted as shown in the following chart provided by http://www.ciac.org.

File	Operation	Location
*.EXE	Delete or replace infected files.	Anywhere
admin.dll	Delete	Root directories of disks and \scripts directory in a web server.
mmc.exe	Delete	\windows or \winnt
Wininit.ini	Delete	\windows or \winnt
Riched20.dll	Delete and replace the one in \winnt\system32 (NT) or \windows (9x)	Windows NT: \winnt\system32 Windows 9x: \windows
*.eml, *.ews	Delete infected files.	Anywhere
*.htm, *.html, *.asp	Remove virus from end or delete.	Anywhere
MEP*.tmp and MEP*.tmp.exe	Delete	\temp, \windows\temp, \winnt\temp
Readme.exe	Delete	anywhere
Readme.eml	Delete	web directories
load.exe	Delete	\windows or \winnt

System.ini	Change line: shell=explorer.exe load.exe -dontloadold to: shell=explorer.exe	\windows or \winnt

- Complete the cleanup and/or removal of the above files.
- Check all the shares on local drives to insure that the share is required and that the permissions are at an appropriate level.
- Remove the Guest account. If you must have a Guest account, reinstall it with the appropriate restrictions. The guest account should not be in the Administrators group.
- Nimda will attempt to replace deleted files so you must reboot and scan everything again to insure that all copies of the infected files have been removed.

An automated anti-virus software or cleanup tool will attempt to clean infected files, and disinfect the system. Because of the complexity of the Nimda worm, these cleanup tools may or may not be successful in cleaning your system. Additionally, the infection may be cleaned but there is no assurance that your system does not have backdoors created by Nimda. Therefore, the most effective way to eliminate the worm and avoid additional security compromises is to reformat and rebuild the system.

The following is an example of one of the available programs available. There are additional steps required for the various Windows operating systems. Detailed instructions will be found at the Tool Removal web site.

Trend Micro offers manual removal instructions as well as an automated tool at the following web site:

Trend Micro
http://www.antivirus.com/pc-cillin/vinfo/virusencyclo/default5.asp?VName=PE_NIMDA.A

Instructions located in Appendix

Symantec Security offers a Nimda Removal tool at the following web site:

Symantec Security
http://securityresponse.symantec.com/avcenter/venc/data/w32.nimda.a@mm.removal.tool.html

Instructions located in Appendix

Source Code/Pseudo Code

The Nimda worm was not available.

Additional Information

- CIAC – Advisory Notice, L-144b: The W32.nimda Worm
- CERT Coordination Center - CERT® Advisory CA-2001-26, Nimda Worm
- F-Secure – Virus Description, Nimda Virus
- Microsoft Security Bulletins
- Network Associates – Virus Alert, Nimda Virus
- Norman – Description of the Nimda Virus
- Symantec Security Response – Nimda Virus

References

Web References

Attack Registry & Intelligence Service (ARIS) Predictor – Nimda Worm Analysis, September 21st, 2001
URL: http://aris.securityfocus.com/alerts/nimda/010919-Analysis-Nimda.pdf

Carnegie Mellon – Software Engineering Institute – Cert Coordination Center – Advisory CA-2001-26 Nimda Worm
URL: http://www.cert.org/advisories/CA-2001-26.html

F-Secure Computer Virus Information Pages: Nimda
URL: http://www.europe.f-secure/v-desc/nimda.shtml
URL: http://www.datafellows.com/v-descs/nimda.shtml

Microsoft Security Bulletins MS01-020, MS01-033, MS00-078
URL: MS01-020.
URL: MS01-033
URL: MS00-078

Symantec Security Response, W32.Nimda.A@mm
URL: http://www.symantec.com/avcenter/venc/data/w32.nimda.a@mm.html

Trend Micro, Virus Encyclopedia
URL: http://www.antivirus.com/pc-cillin/vinfo/virusencyclo/default5.asp?Vname=PE_NIMDA.A

U.S. Department of Energy, Computer Incident Advisory Capability (CIAC) – Advisory Notice L-144B
URL: http://www.ciac.org/ciac/bulletins/l-144.shtml

Appendix

Symantec Security
W32.Nimda.A@mm Removal Tool
Updated October 9, 2001

What the tool does

The W32.Nimda.A@mm fixtool will perform the following steps:

1. Terminates all processes associated with the virus.

2. Terminates Explorer.exe process and relaunches it. The virus injects itself into Explorer.exe which makes this step necessary. Because of this, you may see the desktop flash (this is expected behavior).

3. Detects all types of W32.Nimda.A@mm infections. Repairs those files that can be repaired. Deletes .eml, .nws, .doc and .txt files that have been detected as infected.

   NOTE: *The tool will not delete .eml files in cases where the extension is not one of the four mentioned above. For example, a file with the double extension .eml.bad will not be deleted. You must manually delete such files.*

4. Repairs the System.ini file by removing the modifications made to the shell= line.

5. Removes the guest account from the Administrator group and disables the guest account in the Guests group.

6. Repairs multiple HTML infections.

7. Returns shared drives and folders to default security settings.

8. Deletes registry values which had been modified to prevent Windows Explorer from showing hidden files or known file extensions. Deleting these values resets them to their defaults. You should reconfigure these options to their desired settings. (To do this, in Windows Explorer, click the View menu (Windows 95/98/NT) or the Tools menu (Windows Me/2000), and then click Options or Folder options. Change settings as desired.)

IMPORTANT NOTES:

Windows NT/2000/XP. This tool will restore the original security of Windows NT/2000/XP shares as long as the computer has not been restarted since the virus was launched. The only exception to this are shares that have Everyone [Full Control] as the only rights on them - these cannot be distinguished from shares that the virus has modified and they will be set to Administrator Group [Full Control].

Windows 95/98/Me. On Windows 95/98/Me computers, if the computer has not been restarted, the tool will restore the pre-infection security settings of the shares. If the computer has been restarted, the tool will apply the following settings:

- The "Win9x Share Read Write Password" will be applied to shares with Access Type "Full"
- The "Win9x Share Read Only Password" will be applied to shares with Access Type "Read-Only"
- Both passwords will be applied to shares with Access Type "Depends on Password"

Command line switches available in this tool:
/NOFIXSHARE - will disable share repair (use of this switch is not recommended).
/NOFIXREG - will disable registry repair (use of this switch is not recommended).
/SILENT, /S - enables silent mode.
/LOG=pathname - creates a logfile where pathname is the location in which to store the output of the tool.
/RWPWD=password - apply this password to Win9x Read Write Shares
/ROPWD=password - apply this password to Win9x Read Only Shares

CAUTION: Once a computer has been attacked by W32.Nimda.A@mm, it is possible that your system has been accessed remotely by an unauthorized user. For this reason it is impossible to guarantee the integrity of a system that has had such an infection. The remote user could have made changes to your system, including but not limited to the following:

- Stealing or changing passwords or password files
- Installing remote-connectivity host software, also known as backdoors
- Installing keystroke logging software
- Configuring of firewall rules
- Stealing of credit card numbers, banking information, personal data, and so on
- Deletion or modification of files
- Sending of inappropriate or even incriminating material from a customer's email account
- Modifying access rights on user accounts or files
- Deleting information from log files to hide such activities

If you need to be certain that your organization is secure, you must reinstall the operating system, and restore files from a backup that was made before the infection took place,

and change all passwords that may have been on the infected computers or that were accessible from it. This is the only way to ensure that your systems are safe. For more information regarding security in your organization, contact your system administrator.

PE_NIMDA.A

Aliases:
NIMDA.A, W32/Nimda.A@mm, CV-5, Minda, Concept Virus, Code Rainbow

Risk rating: medium risk

Virus type: File Infector

Destructive: Yes

Description:
This is Trend Micro's detection for files infected with the original viral code of a fast-spreading Internet worm and file infector PE_NIMDA.A-O. It arrives as an embedded attachment, README.EXE file, in an email that has an empty message body and, usually, an empty subject field. It does not require the email receiver to open the attachment for it to execute. It uses a known vulnerability in Internet Explorer-based email clients to execute the file attachment automatically. This is also known as Automatic Execution of Embedded MIME type.
The infected email contains the executable attachment registered as content-type of audio/x-wav so that when recipients view the infected email, the default application associated with audio files is opened. This is usually the Windows Media Player. The embedded EXE file cannot be viewed in Microsoft Outlook.
More information about this vulnerability is available at Microsoft's Security Bulletin.
It has four modes of spreading: via email, via network shared drives, via unpatched IIS servers and via file infection.

Email Exploit
The email sending routine is perpetually done in 10 day cycles. In rare instances, the worm's email routine may be reactivated after 11 days. To do this, the worm stores a value computed from the current system time in a counter saved in the following registry entry

```
HKCU\Software\Microsoft\Windows\CurrentVersion\
Explorer\MapMail, Cache
```

When the worm is run, it checks this value to find whether 10 (or occasionally 11) days have passed. If so, it executes its email propagation routine and resets the counter to begin the 10-day countdown again. To send copies of itself to others, this worm retrieves email addresses through the use of Messaging APIs or MAPI. It also gathers email addresses from .HTML and .HTM documents found in the folder referred to by the following registry entry:

```
HKCU\Software\Microsoft\Windows\CurrentVersion\
Explorer\Shell Folder, Cache
```

The email addresses are stored in a linked list that is passed to an SMTP engine in the virus code that sends the unsolicited email.

Please continue on to the "Technical Details" section for more information about this worm.

Solution:
This worm shares your local drives to compromise the security of your file system. Please check and remove these shares with the instructions at Unsharing Folders On Windows. You may disable all your shared drives or limit the shares to READ access since this worm may perpetually infiltrate your system via the shared drives.

For Automatic Cleaning and Removal:

1. Please download and apply the fix tool.
2. Trend Micro requests that all users download and read the readme_nimda.txt before using this tool.
3. Scan your system with Trend Micro antivirus. To do this Trend Micro customers must download the latest pattern file and scan their system. Other email users may use HouseCall, Trend Micro's free online virus scanner. Some infected files may be corrupted. Delete these files.
4. For additional information on the NIMDA worm, and suggestions for preventing future infections, you may also visit Microsoft's NIMDA Information page.

Manual Removal Instructions

1. Disconnect system from the network.
2. Click Start>Run, type SYSTEM.INI then hit Enter.
3. Look for the "Shell =" line and modify as follows:
   From:
   Shell = explorer.exe load.exe –dontrunold
   To:
   Shell = explorer.exe
4. Save and then close SYSTEM.INI.
5. Click Start>Run, type WININIT.INI then hit the Enter key.
6. Look for and then delete the lines that contain the following text string:
   mepXXXXX.tmp.exe
7. Save and close WININIT.INI file.
8. Scan your system with Trend Micro antivirus and clean all files detected as PE_NIMDA.A. To do this Trend Micro customers must download the latest pattern file and scan their system. Other email users may use HouseCall, Trend Micro's free online virus scanner. Some files may be corrupted or contain only a pure strain of the worm and are detected as PE_NIMDA.A-O. Delete these files.
9. Restart your system and repeat step 8.
10. Restore the RICHED20.DLL file by performing any of the following:
    Note:Change the <%drive%> entry with the drive letter of your CD-ROM drive.
    - Using Windows 98 SE installation CD, click Start>Run. On the window that pops out, type:
      extract /a <%drive%>:\win98\setup\win98_37.cab riched20.dll /L c:\windows\system
    - Using Windows ME installation CD, click Start>Run. On the window that pops out, type:
      extract /a :\win9x\win_14.cab riched20.dll /L c:\windows\system
    - Using Office 2000 Premium Edition, click Start>Run. On the window that pops out, type:
      extract /a <%drive%>:\office1.cab riched20.dll /L c:\windows\system
11. Make sure you have installed the latest patches available:
    - Update to Internet Explorer 5.01 SP2
    - Update to IE 5.5 SP2

- Update to IE 6.0

12. If any of the above is not possible, download the below patches. Before you do, please read Microsoft's Security Update page:
    - Service Pack (6a) for NT 4 users.
    - Security Fix Rollup Package
    - IIS-related Security Patch

Additional Clean Instructions On Windows ME

NOTE: Windows ME backs up selected files automatically to a C:_Restore folder. This means that an infected file could be stored there as a backup file, and will not be cleaned during the scan. To remove the infected files from the C:_Restore folder:

1. Right click the My Computer icon on the Desktop and select Properties.
2. Click the Performance Tab>File System button.
3. Click the Troubleshooting Tab.
4. Put a check mark next to Disable System Restore.
5. Click Apply>Close>Close.
6. Click Yes when prompted to restart the system. The Restore Utility is then disabled.
7. Restart in Safe Mode.
8. Run a scan and delete the file(s) detected as PE_NIMDA.A, or browse the files located in the C:_Restore folder and remove the file(s) there.
9. After removing the files, restart the computer normally.
10. Re-enable the Restore Utility and repeat steps 1-3.
11. Remove the check mark next to Disable System Restore at step 4.
12. Continue with steps 5 and 6. Your System Restore is active again.

For IIS Users:

1. For IIS 5.0 (Windows 2000 Server), get the Service Pack 2
2. The worm uses the Microsoft IE MIME Header Attachment Execution Vulnerability to drop emails. For an explanation and to download the patch please visit Microsoft's Web site.
3. The worm also uses the Microsoft Web Server Folder Traversal vulnerability. An explanation and patch is available at Microsoft's Web site.
4. Trend Micro recommends that customers also use Microsoft's Cumulative IIS patch.