GIAC
CERTIFICATIONS

# Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

## Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials (Security 401)"
at http://www.giac.org/registration/gsec

Heather Holick
Version 1.2f

# Nimda Worm

## Introduction

On Tuesday, September 18th at 9 a.m., a self-replicating piece of software started to infect IIS Web servers and users running Internet Explorer 5. This extremely virulent piece of software or known better as a "worm" rapidly spread through the Internet using multiple methods of infection. This worm came to be known as Nimda or one of it's many alias: Code Rainbow, Concept5, W32.nimda.A@mm, Minda, Nimbda, PE_NIMDA.A, I-Worm.Nimda, Readme, or Readme.exe. It exhibits many traits as other recently well-known worms- sadmind/IIS, Code Red and SirCam. Its' design takes advantage of the vulnerabilities that emerged from the Code Red and sadmind/IIS attacks and can spread itself at a ferocious pace through e-mail like SirCam.

This paper gives a basic overview of the Nimda Worm, the vulnerabilities it exploits, and protection against infection.

## Overview of the Nimda Worm

Definition:

Nimda worm- a reproducing program that runs independently and travels across network connections. It is the first reported worm to have to ability to modify existing web sites that could automatically download the worm, use end user workstations to scan for servers with vulnerabilities, and scan for intranet web sites for vulnerabilities.

Method of attacks:

1. **Email**- Nimda contains its own built in mass-mailing routine that can extract e-mail addresses from address books, mail in the inbox, web pages and web pages in the web cache. The mass-mailing routine can execute itself every 10 days and hence keep the e-mail propagation going.

   The e-mail contains no apparent text body or subject line; however, it contains a base64-encoded executable file named "readme.exe". The worm will use the e-mail addresses captured from the infected system and insert them into the To: and From: fields to appear as a trusted e-mail. Due to the automatic execution of embedded MIME vulnerability, infection can occur by opening the mail message or running the readme.exe. Deleting email can be difficult due to that the worm can activate once the mail message is opened.

2. **Web Server**- Nimda will attempt to infect Microsoft IIS Web Servers that have not been properly patched. The worm will traverse each directory is the system looking for HTM, HTML, and ASP files and append infected EML or NWS files to the code. This will allow for propagation through a web browser or through the network file system.

© SANS Institute 2000 - 2002, Author retains full rights.

3. **Web browser propagation**- Once Nimda has infected the HTM, HTML, and ASP files on the Web Server, web browsers and Windows Explore become vehicles for propagation. Once a user assesses a web site that uses HTM, HTML, and ASP files, they will fall victim to the worm.

4. **File Modification**- After Nimda is established in a system it spreads itself using shared network drives. The worm will imbed numerous files with EML and NWS extension. These files contain the identical contents as the readme.exe. If a user selects the one of the EML or NWS files from the share drive, the worm will compromise the system.

   Nimda also targets EXE files. It will scan the system for EXE files that have not been compromised. Then it will make a copy of the EXE file and of itself and place it into a temporary directory. Examples of the files are below:

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

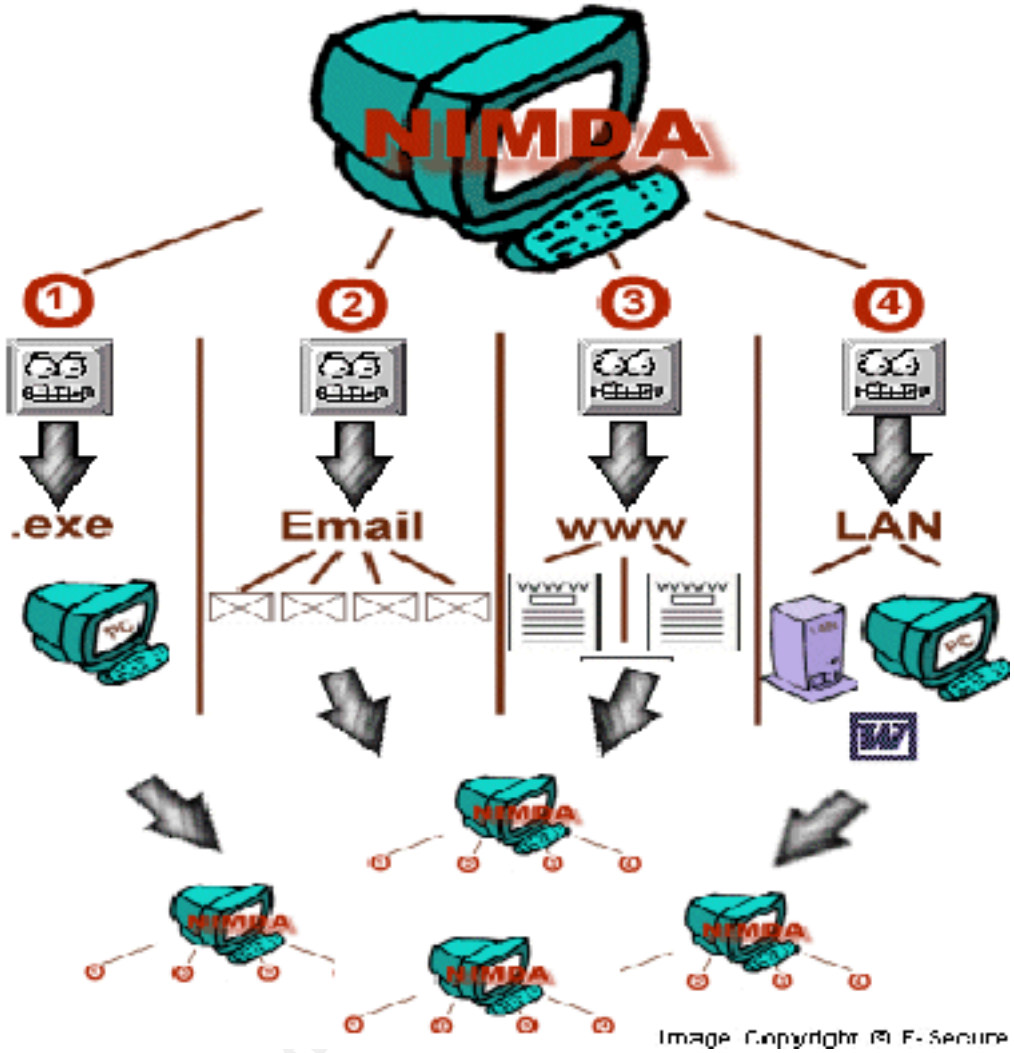
   When the infected EXE file is executed, the original EXE code will run and the Nimda worm will also execute in the background propagating itself again.

   If all of that was not enough, Nimda will also drop hidden files called RICHED20.dll or load.exe into directories containing DOC and EML files. When a user opens any of these files, Word, WordPad or Outlook will execute the infected DLL or EXE files to compromise the system.

   Also, it alters the system.ini file with the following shell line – **=explorer.exe load.exe – dontrunold.** The system.ini file is a Windows system file that configures hardware settings at startup and can execute Nimda as well.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

**Figure 1: Full Lifecycle of Nimda**




**Source**: F-Secure Information Center http://www.europe.f-secure.com/nimda/nimda.shtml

Systems and Applications that are vulnerable

1. Microsoft Window operating systems – 95, 98, NT 4, ME, and 2000
2. Microsoft Internet Information Services on Window 2000 and NT web servers
3. Mail service on any Windows platform
4. Microsoft Internet Explorer 5.01 SP1 or earlier and 5.5 SP1 or earlier
5. Microsoft Outlook or Outlook Express

**Note**: IE 5.01 SP2, 5.02 SP2, IE 6 and Netscape browser and communicator are not vulnerable to Nimda.

Ports that are involved

1. **TCP 137-139, 445-** NetBios File Shares
2. **TCP 80-** HyperText Transfer Protocol

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

3. **TCP 25 SMTP-** Simple Mail Transfer Protocol
4. **UDP 69 TFTP-** Trivial File Transfer Protocol

Payload

1. **Degrades network performance**- Nimda can consume large amounts of bandwidth during the propagation phase. Nimda can also spread at a considerable rate and denial-of-service attacks and impaired network connectivity have been reported.

2. **Compromise security settings**- Nimda creates a Guest account in the system giving it administrative privileges. An unauthorized remote user can access the network and read, modify or delete files on the system. It also grants full access privileges to everyone to the C: drive.

3. **Modifies the system.ini file**- Nimda will modify the system.ini file, so once the system starts up the worm will execute.

4. **Modifies executable files**- Nimda will imbed infected code into EXE files. Once the file is executed the worm will propagate.

5. **Embeds code in files for further propagation**- Nimda will imbed malicious javascript code to the end of the following files names – index, readme, main, default with the following extensions - HTM, HTML, and ASP. If a user browses a web site with an insecure Internet Explorer, the worm will automatically download and execute the readme.eml file to the users computer.

   Also, it will copy hidden files load.exe and RICHED20.dll into network shares. Once a user access these files through a Internet Explorer or Windows Explorer or opens a DOC file, the worm infiltrates the system.

6. **Deletes subkeys of the registry key**- Nimda will circumvent the network share security feature by deleting subkeys in the registry. The registry key that is targeted is SYSTEM\CurrentControlSet\Services\Ianmanserver\Shares\Security.

**Description of Microsoft Vulnerabilities**

1. **Microsoft IIS/PWS Escaped Characters Decoding Command Execution Vulnerability**- This vulnerability effects both the IIS Web Server and Personal Web Server and allows unauthorized user the gain access to these systems through the IUSR_*machinename* account. This vulnerability could possibly allow a malformed file name to circumvent initial security checks and allow the file to execute within the system.

2. **Microsoft IE MIME Header Attachment Execution Vulnerability**- Microsoft Internet Explore is susceptible to attack because of a vulnerability to MIME attachments. An attacker could potentially run a program of choice if a user browsed a web site or opened

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

an e-mail that the attacker sent or developed. The attacker would use the audio/x-way MIME to propagate the infect readme.exe and IE will automatically run the executable without displaying are warning.

3. **Microsoft IIS and PWS Extended Unicode Directory Transversal Vulnerability-** This vulnerability is quite similar to the Microsoft IIS/PWS Escaped Characters Decoding Command Execution Vulnerability in that an attacker can gain access to the systems through the IUSR_*machinename* account. This vulnerability will allow executables in the directory to execute if the parent directory is marked as executable. It takes advantage of the fact that the IIS server has executable directories within its Web folder. If an attacker uses Unicode characters to reference the executable is the directory and the IUSR_*machinename* account has privileges to run executables, then the attacker can easily infect the system.

4. **Microsoft Office 2000 DLL Execution Vulnerability**- Users can unknowingly execute hidden DLL files when Nimda has infected the system. Nimda will copy an infected RICHED20.dll or load.exe to network directory where Microsoft Office documents may be located. Once these documents are opened the infected DLL file is activated causing infection to the system.

**Protection from Infection**

The best defense against the Nimda Worm is to apply the appropriate patches from Microsoft and change certain settings in Microsoft Office and Internet products.

**Microsoft Outlook:** Nimda can execute by opening an e-mail message so, before trying to delete an infected message, ensure that the e-mail application's security is enabled. To properly secure Microsoft Outlook the "Active Scripting" must be disabled to prevent the worm from exploiting the MIME vulnerability. This can be accomplished through Tools/options/security tab/secure content/internet/zone settings/customize level. Disable scripting for Internet, Local Intranet, Trusted Sites and Restricted Sites.

**Internet Explorer:** For Microsoft Internet Explorer 5.01 SP1 or earlier and 5.5 SP1 or earlier, download versions of IE 5.01 SP2 http://www.microsoft.com/windows/ie/downloads/recommended/ie501sp2/default.asp , 5.5 SP2 http://www.microsoft.com/windows/ie/downloads/recommended/ie55sp2/default.asp , or IE 6 http://www.microsoft.com/windows/ie/default.asp. Then in the browser disable the "Active Scripting" through Tools/internet options/security tab/custom level. Disabled scripting for Internet, Local Intranet, Trusted Sites and Restricted Sites.

**Anti-Virus Software:** Anti-Virus Software companies are aware of the Nimda worm and development a signature file to prevent infection. Keep anti-virus software up-to-date by visiting the vendor's web site to download the latest virus definitions. Examples below.

- Symantec – http://www.symantec.com/downloads/

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Also, sign up to receive advisory e-mails from CERT® Coordination Center (CERT/CC) at http://www.cert.org/contact_cert/certmaillist.html and check for alerts from National Infrastructure Protection Center (NIPC) at http://www.nipc.gov/cybernotes/cybernotes.htm to keep fully abreast of new incidents.

**Microsoft IIS Web Server:** Need to load the following patches:

Patch the back door from the Code Red and sadmind/IIS attacks:
http://www.microsoft.com/technet/security/bulletin/MS01-044.asp

Patch the Unicode Web Traversal exploit:
http://www.microsoft.com/technet/security/bulletin/MS01-044.asp
http://www.microsoft.com/technet/security/bulletin/MS00-057.asp
http://www.microsoft.com/technet/security/bulletin/ms00-078.asp

Patch the MIME exploit:
http://www.microsoft.com/technet/security/bulletin/MS01-020.asp
http://www.microsoft.com/technet/security/bulletin/ms01-027.asp

Patch the Decoding exploit:
http://www.microsoft.com/technet/security/bulletin/MS01-026.asp

Information on securing Microsoft IIS Web Server:
http://www.microsoft.com/technet/security/iis5chk.asp
http://www.microsoft.com/technet/security/tools.asp

## Conclusion

Nimda is the first of its kind to have the ability to travel and propagate through networks shares, e-mails, web sites, and web servers. The best defense against infection is to be fully informed with the last vulnerabilities and alert information, load patches, disable scripting in browsers and email programs, keep a look out for unexpected or unfamiliar e-mails especially with non-recognizable subject lines, and properly secure servers. Never assume you're safe from an attack.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

**References**


Chien, Eric. W32.Nimda.A@mm. 12 Nov. 2001. Symantec. http://securityresponse.symantec.com/avcenter/venc/data/pf/w32.nimda.a@mm.html

Excerpts: New Worm Spreads Trough Internet, Experts Warn. 19 Sept. 2001. U.S. Department of State International Information Programs.http://usinfo.state.gov/topical/global/ecom/01091902.htm

F-Secure Virus Description. F-Sucure. http://www.europe.f-secure.com/v-descs/nimda.shtml

FedCIRC Advisory FA-2001-26 Nimda Worm. 25 Sept. 2001. FedCIRC. http://www2.fedcirc.gov/advisories/FA-2001-26.html

Information on the "Nimda" Worm. Microsoft. http://www.microsoft.com/technet/treeview/default.asp?url=/TechNet/security/topics/nimda.asp

L-144b: The W32.nimda Worm. 25 Sept. 2001. U.S. Department of Energy Computer Incident Advisory Capability. http://ciac.llnl.gov/ciac/bulletins/l-114.shtml

Mackie, Andrew, Roculan, Jensenne, Russel, Ryan, and Van Velsen, Mario. Nimda Worm Anaylsis. 21 Sept. 2001. Attack Registry & Intelligence Service. http://aris.securityfocus.com/alerts/nimda/010919-Analysis-Nimda.pdf

Mass Mailing worm W32.Nimda.A@mm. 18 Sept. 2001. National Infrastructure Protection Center. http://www.nipc.gov/warnings/advisories/2001/01-022.htm

Microsoft Security Bulletin (MS01-020) Incorrect MIME Header Can Cause IE to Execute E-mail Attachment. Microsoft. http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS01-020.asp

Nimda Worm Protection ABCs. Computer Protection Program Ernest Orlando Lawrence Berkeley National Laboratory http://www.lbl.gov/ITSD/Security/vulnerabilities/nimda-background.html#prevents


© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.