Interested in learning more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Nimda Explained, and What You Can Do to Protect Your Sytem(s)

Nimda is considered to be the worst worm to date (September 26, 2001) and has caused lost time and revenue for many companies, not to mention headaches for many system administrators. Unfortunately, this is not the last case of widespread infection that we will see. However, some may view this occurrence as a learning experience, and we can be better prepared for future outbreaks if we learn from this and spend more time updating and hardening critical systems.

Copyright SANS Institute
Author Retains Full Rights

AD

Nimda Explained, and What You Can Do to Protect Your Sytem(s)

Greg Dzurinda

September 26, 2001

INTRODUCTION

In the wake of the September 11th terrorist attack, the Internet and its host systems suffered an attack of its own. **Nimda** as it was called was wreaking havoc for network administrators. Nimda is the latest worm that has exposed the vulnerabilities in not only Microsoft IIS, but also those in Microsoft's Internet Explorer on client systems. I will write about the details of this new threat and detail some things one can do to mitigate the damage and perhaps even avoid becoming infected by the worm. While researching material to use for this paper, I did notice that sources had varying information about Nimda. Because the worm is relatively new and network administrators are still trying to clean up the mess that was caused, we may not know the full potential of this worm at this time.

WHAT IS NIMDA?

Nimda is the nickname of the worm **W32.nimda.a@mm**, also named PE_NIMDA.A, I-Worm.Nimda, and W32/Nimda-A. Nimda is so nicknamed because it is admin spelled backwards. Admin is what this worm requires, as companies have lost millions of dollars because of the time spent repairing compromised systems and the subsequent denial of services the worm caused. Nimda is a worm (defined on http://www.whatis.com as a "self replicating virus that does not alter files but resides in active memory and duplicates itself and sometimes drains system resources") that takes advantage of several vulnerabilities in Microsoft's IIS and PWS (Personal Web Server-used in Windows 98 or Windows 2000 Professional). As you will note in the definition of "worm" I have provided, you will see that a worm "does not alter files". This is not necessarily the case with Nimda, as files are altered (not necessarily damaged) as a means to further propagation. For that reason, Nimda is also classified as a virus.

The following are ways by which Nimda spreads to victim hosts:

1.) Known vulnerabilities or other holes

Microsoft IIS is susceptible to such vulnerabilities like "Extended Unicode Directory Traversal Vulnerability", by which an anonymous user can substitute a "/" or a "\" with extended code and possibly read, write, or execute critical files and "Escaped Character Decoding Command Execution Vulnerability", by which a user can use a large number of characters in a URL, gain access to a system, and possibly cause a denial of service by consuming system resources. Nimda will attempt to gain access to a host system using those vulnerabilities and can also use holes that may have been left by earlier viruses.

As is the case with other web servers, systems running IIS are typically connected to broadband lines, so an incredible amount of scans can traverse networks in a short period

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

of time looking for vulnerabilities on other hosts. Aside from simply scanning networks, the worm also attempts to **automatically** gain access to a host by way of the aforementioned vulnerabilities. With certain network topologies, this can cause network congestion on a LAN and perhaps denial of service, since so much processing power and resources are being used to send packets looking for other hosts.

Once Nimda has exploited one of these vulnerabilities or backdoors, it uses TFTP (Trivial File Transfer Protocol) to transfer files from one infected host to the new host. One such file is **admin.dll**. This file and many copies of **.eml** and **.nws** files are copied to other locations on the server waiting to be copied to other infected hosts.

2.) E-mail

Like other worms and viruses, one way that Nimda spreads is by e-mail. Messages with random subjects and an attachment by the name of **readme.exe** are likely to be messages generated by the worm from a compromised system. If the attachment is opened, the mail recipient's computer will become infected. Microsoft Outlook and Outlook Express are the applications that are most susceptible.

Also, it is thought that the attachment does not necessarily have to be opened to execute its code. Older versions of Microsoft Outlook and Outlook Express include something called a preview pane. This may result in the code in the attachment to be executed in the background without the user being aware of it, and the system will become infected. The worm also records the users in the victim's address book and sends a copy of itself to each of those users. According to the virus code, the messages are resent to the persons in the address book **every 10 days**, although there have not been any significant cases of re-infection reported on any of the security sites on the Internet. That is not to say that systems have not been reinfected, but users are certainly now better equipped to handle and properly avert such a threat.

3.) From a web server, Nimda can infect another host that is running earlier versions of IE that will automatically execute MIME headers

Once Nimda infects a web server, it looks through directories for web files that are being hosted by the server. These files include **.htm**, **.html**, or **.asp** files. When those files are found, Nimda appends a java script. Once a page is displayed by a visitor of the web site hosted on the infected server, the java script will run, point to the directory of the **readme.eml** file that was added by the worm, and force download of the file to the client machine. The unsuspecting person browsing the web site will not know that he/she has been infected with the worm. By default, earlier versions of Internet Explorer allow **"Automatic Execution of Embedded MIME Types"**, and will be more susceptible with that setting enabled, because Nimda adds code to be executed in the MIME type header that is typically sent with a web page. Versions of IE that are most susceptible are 5.5 not using Service Pack 1 and versions of 5.01 not using Service Pack 2. Other versions of IE do not have this setting enabled and should prompt a user that a download is required in order to view the web page.

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

4.) Network shares

Once this worm infects a host machine, it scans the local network to find shared folders. Several ARP requests will be sent, and **ARP flooding** may result. Once a network share is found, the worm scans for **.doc**, **.eml**, or **.exe** files that can be written. When those files are found, the worm attaches a file called **riched20.dll** (a file needed to run MS Office applications) if the file does not already exist in the directory. When a user attempts to run those shared files, they also download and execute the **.dll** file that will infect their machine and will subsequently execute the program code.

Also, the Nimda worm will attempt to open holes by creating a guest account with administrator privileges and create open shares on the infected system. Once that guest account is created, the user ID and password for the guest account may be sent to an attacker, and access could be gained through terminal services or other remote control software.

Additional Technical Details

To summarize the technical details included in the last section, there are two ways by which this Nimda will start executing:
Admin.dll is the common method the worm is first run on a web server, and **readme.exe** is often the file that infects client machines.

On a server, once a worm is executed, it will overwrite the **mmc.exe** file in the %Windows/System% directory (in Windows NT, the exact directory location is WINNT/System32). With the exception of **winzip.exe**, the worm also infects all other executable files on both local and network drives, creates copies of .eml and .nws files, and replicates itself by attaching riched20.dll in all folders containing **.doc** files that were found in a search of specific registry keys. The worm runs as a process and can act as a remote thread to **Explorer.exe,** so the worm can continue to execute regardless of whether a user is logged in.

The worm then opens network shares for all drives by changing the registry key:

HKLM\Software\Microsoft\Windows\Current Version\Network\LanMan \[C$ -> Z$]

The worm searches for all open shares on the network by parsing through Network Neighborhood, and starts scanning NetBIOS names and select IP addresses. It has been documented that the worm first scans for hosts on the local subnet. In other words, if a host with an IP address of 10.1.1.5 is infected, the worm will first search for additional hosts within the 10.1.1.x subnet. All files on any open network shares are examined for possible infection.

Next, .eml and .nws files are copied to the open network shares and the worm copies

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

itself over as **riched20.dll** to any folder that contains .doc files. The worm will also make a copy of itself as a file named **load.exe** in the %Windows/System% directory. Finally, Explorer settings are modified to "hide file extensions for known file types", so a user may not see the added files.

Nimda is the first worm to utilize both client and host machines to run scans to find vulnerable systems, and it is also the first worm to have the ability to propagate through browsing of web pages.

WILL NIMDA STRIKE AGAIN?

Nimda may not rear its ugly head again. However, there will certainly be more worms and viruses that we will have to battle, possibly hybrids or variations of Nimda, and they may be coded to take advantage of back doors or vulnerabilities that were left behind by the original version. Vendors are still studying the affects of Nimda, and may not be completely aware of all the effects of the worm.

HOW TO MITIGATE RISK AND DAMAGE

Removal tools

There are several ways in which you can minimize the risk of becoming infected by this worm. If the worm has already compromised your system or network, Symantec has a great removal tool, **fixnimda.com**, which you can download from their web site at http://www.symantec.com/avcenter/venc/data/w32.nimda.a@mm.removal.tool.html. There are other sources where you can find this tool. You can also download the removal tool from the following FTP site:
ftp://ftp.f-secure.com/anti-virus/tools/fsnimda1.exe
The removal tool will repair as many damaged or altered files as it can, and it will remove any **.eml**, **.doc**, or **.nws** files that have been infected. It is recommended that you run this fix more than once until there are no infected files found by the program.

Beware of e-mail attachments and educate users about the dangers of opening attachments from both trusted and untrusted sources

It is good practice to warn users of opening any attachments, especially those from untrusted sources. To completely avoid becoming infected by the Nimda worm, be sure that you and the users within your company remain cognizant of any e-mail messages containing an attachment called **readme.exe**. As a matter of fact, it would be wise to configure e-mail filters or firewalls to reject messages with this attachment.

Hardening your web servers and installing the newest patches

In reading the several articles about Nimda, it occurred to me that the vulnerabilities that were exploited have been well known by vendors and administrators. The vendors have done their part in releasing patches and fixes that address those vulnerabilities, but not all

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

administrators have done their part in downloading and installing those patches and fixes on their systems. So the question should be asked: if administrators put forth more time and effort in actual maintenance of critical servers, how much effect would Nimda have had? There are many ways that a system (host or client) can be "hardened". Administrators should first address the more obvious holes and backdoors that are inherent in OS' like Microsoft Windows. Microsoft has a tool available on its web site that is called **"IIS Lockdown Tool"** that will automate most of these tasks and still allow for some customization. After systems are hardened, administrators should then install additional patches and anti-virus software that can prevent system compromise. Obviously, since this worm also infects client machines, there would have still been some "casualties" from this latest virus outbreak, but much of the damage could have been avoided.

If an IIS vulnerability is exploited, only the folders on the same logical drive as the web folders can be accessed. In other words, if you have your web folders and IIS set up on D:\ and your system partition with the OS files is on C:\, critical system files may not be harmed if the web server is compromised. I just wanted to make quick mention of this preventive practice, as there is plenty more documentation on securing a web server in other sources.

Upgrading your version of Internet Explorer

Vendors were originally suggesting upgrading Internet Explorer versions to 6.0, but the latest news is that IE 6 may also be vulnerable. IE 6 is at least more thorough about warning the user about automatic downloads from web sites. The user can opt not to download the file and be safe. There are more patches available now, so be sure to keep your system with the latest downloads from vendor sites.

Another interesting note I should mention is the response time of the vendors when this occurred. Incidents.org and other sites were notified of heavy traffic on the morning of September 18th, but appropriate fixes and patches were not released until hours later. When the news was spread of the virus, time still passed until all the specific symptoms were announced and patches and fixes were released. This is understandable, as vendors can only react to such catastrophes and rush for solutions, but administrators were not aware of the proper way to deal with the worm and were scrambling for answers.

CONCLUSION

Nimda is considered to be the worst worm to date, and has caused lost time and revenue for many companies, not to mention headaches for many administrators. Unfortunately, this is not the last case of widespread infection that we will see. However, some may view this occurrence as a learning experience, and we can be better prepared for future outbreaks if we learn from this and spend more time updating and hardening critical systems.

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

WORKS CITED

RFC 1521 "MIME (Multipurpose Internet Mail Extensions) Part One: Mechanisms for Specifying and Describing the Format of Internet Message Bodies" September 1993. URL: http://www.rfcdoctor.com/ (22 September 2001)

K. Tocheva, G. Erdelyi, A. Podrezov, et al. "F-Secure Virus Descriptions" September 2001. URL: http://www.datafellows.com/v-descs/nimda.shtml (28 September 2001)

Symantec Press Center. "Symantec Provides Comprehensive Protection Against W32.NIMDA.A@MM" September 2001. URL: http://www.symantec.com/press/2001/n010919.html (30 September 2001)

Microsoft. "Information on the 'Nimda' Worm" September 2001. URL: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/topics/Nimda.asp (28 September 2001)

SANS Institute. "Nimda Worm/Virus Report – Interim". September 2001. URL: http://www.incidents.org/react/nimda-update-sept27.pdf (28 September 2001)

Kevin Poulsen. "'Nimda' Worm Hits Net: Self-Executing Virus Attacks IIS and Microsoft Outlook" September 2001. URL: http://www.securityfocus.com/news/253 (24 September 2001)

TechTarget.com. Definition. "Worm" URL: **http://www.whatis.com** (24 September 2001)

Svidergol, Brian. Phone Interview. 28 September 2001.

© SANS Institute 2001, Author retains full rights

Last Updated: June 19th, 2013

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

Digital Forensics & Incident Response Summit 2013	**Austin, TXUS**	**Jul 09, 2013 - Jul 16, 2013**	**Live Event**
SANS London Summer 2013	**London, GB**	**Jul 09, 2013 - Jul 16, 2013**	**Live Event**
SANS Rocky Mountain 2013	**Denver, COUS**	**Jul 14, 2013 - Jul 20, 2013**	**Live Event**
SEC528 SANS Training Program for the CompTIA® New Advanced Security Practitioner (CASP) Certification	**Washington, DCUS**	**Jul 22, 2013 - Jul 26, 2013**	**Live Event**
SANS Mumbai 2013	**Mumbai, IN**	**Jul 22, 2013 - Jul 27, 2013**	**Live Event**
SANS San Francisco 2013	**San Francisco, CAUS**	**Jul 29, 2013 - Aug 03, 2013**	**Live Event**
SANS Boston 2013	**Boston, MAUS**	**Aug 05, 2013 - Aug 10, 2013**	**Live Event**
SANS SEC 560: Network Penetration Testing @ Bangalore 2013	**Bangalore, IN**	**Aug 05, 2013 - Aug 10, 2013**	**Live Event**
Critical Security Controls Summit	**Washington, DCUS**	**Aug 12, 2013 - Aug 18, 2013**	**Live Event**
Industrial Control Systems Security Training - DC	**Washington, DCUS**	**Aug 12, 2013 - Aug 16, 2013**	**Live Event**
SANS Virginia Beach 2013	**Virginia Beach, VAUS**	**Aug 19, 2013 - Aug 30, 2013**	**Live Event**
SANS Thailand 2013	**Bangkok, TH**	**Aug 19, 2013 - Aug 31, 2013**	**Live Event**
SANS Melbourne 2013	**Melbourne, AU**	**Sep 02, 2013 - Sep 07, 2013**	**Live Event**
SANS Capital City 2013	**Washington, DCUS**	**Sep 03, 2013 - Sep 08, 2013**	**Live Event**
Network Security 2013	**Las Vegas, NVUS**	**Sep 14, 2013 - Sep 23, 2013**	**Live Event**
SANS Canberra 2013	**OnlineAU**	**Jul 01, 2013 - Jul 13, 2013**	**Live Event**
SANS OnDemand	**Books & MP3s OnlyUS**	**Anytime**	**Self Paced**