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.

Overview of Nimda

A system administrator's perspective on Nimda to describe how the worm attacked, why the vulnerabilities existed and what could be done to prevent future infections.

Copyright SANS Institute
Author Retains Full Rights

AD
Symantec™
Endpoint Protection 12
The next generation of reputation-based security
Download the beta
Symantec.
Confidence in a connected world.

By John Phillips on February 13, 2003
Per the ADMINISTRIVIA Version 2.0 and GSEC Practical Assignment Version 1.2f standards

Overview of Nimda

Introduction

September 18th,2001 was my first encounter with Nimda along with many other people. I was researching a scan that had happened earlier that morning when the IDS began to flood me with alerts. This was just the beginning of a very long couple of days for a lot of people, including myself. This worm hit with such vengeance, I had problems gathering information as the logs and IDS alerts were growing so fast I could not read them effectively. I began to wonder, "was this a denial of service attack aimed at us?" or "was this another variant of Code Red?" I took a breath and began copying logs from different devices for evaluation of the situation. From scanning my logs and the quick glimpse that I was able to get at the IDS, I found this was not a targeted attack. It was randomly hitting our network and eventually hit every external IP address within the environment. I then checked my e-mails, etc to make sure this was not a planned scan. After a quick search I was confident that this was either another Code Red or someone running an extensive scan that we didn't pay for. Looking at my web logs, I was able to get a pretty good idea of what this thing did, or so I thought. The web piece of the worm was using exploits that had patches released months ago. I would have thought the Code Red would have taught people by now, guess not. I was seeing things like

```
2001-09-18 13:43:44 64.0.24.157 - GET /scripts/root.exe /c+dir 404 2 604 72 15 80 HTTP/1.0 - - -
2001-09-18 13:43:44 64.0.24.157 - GET /MSADC/root.exe /c+dir 404 2 604 70 0 80 HTTP/1.0 - - -
2001-09-18 13:53:55 64.90.45.189 - GET /scripts/root.exe /c+dir 404 2 604 72 16 80 HTTP/1.0 - - -
2001-09-18 13:53:55 64.90.45.189 - GET /MSADC/root.exe /c+dir 404 2 604 70 0 80 HTTP/1.0 - - -
2001-09-18 13:53:55 64.90.45.189 - GET /c/winnt/system32/cmd.exe /c+dir 404 3 604 80 0 80 HTTP/1.0 - - -
2001-09-18 13:53:59 64.90.45.189 - GET /d/winnt/system32/cmd.exe /c+dir 404 3 604 80 0 80 HTTP/1.0 - - -
2001-09-18 13:56:08 64.90.177.243 - GET /scripts/root.exe /c+dir 404 2 604 72 0 80 HTTP/1.0 - - -
2001-09-18 13:56:08 64.90.177.243 - GET /MSADC/root.exe /c+dir 404 2 604 70 0 80 HTTP/1.0 - - -
2001-09-18 13:56:08 64.90.177.243 - GET /c/winnt/system32/cmd.exe /c+dir 404 3 604 80 0 80 HTTP/1.0 - - -
2001-09-18 13:56:08 64.90.177.243 - GET /d/winnt/system32/cmd.exe /c+dir 404 3 604 80 0 80 HTTP/1.0 - - -
2001-09-18 13:56:08 64.90.177.243 - GET /scripts/..%5c../winnt/system32/cmd.exe /c+dir 404 2 604 96 15 80 HTTP/1.0 - - -
```

As I stated earlier, this traffic was coming in so fast, I decided to spend a few minutes communicating with my vendors, researching on the web, and contacting others in the area if they were seeing the same things at their sites. Everyone was seeing this and some were already in serious trouble. As I kept looking for an explanation, I began to see things being posted on places like http://www.cert.org/advisories and other sites like http://www.symantec.com/avcenter and http://vil.nai.com/VIL/newly-discovered-viruses.asp. As I found and began to read the documentation on this worm, I began to get worried. I had just finished up a checkup on all IIS servers just a few days before; but I found out that was only one avenue of infection. This worm can infect in four different ways and will be here on and off for a quite a while. So, what is this worm? What did we miss? What can we do in the future? These are the questions that I am going to try and answer as I help my organization and others cleanup from this worm.

What is NIMDA

Before we can define what the Nimda worm is, we need to know what a worm is. The best definition I could find was from a web site called searchSecurity.com. Their definition states: "A

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

worm is a self-replicating virus that does not alter files but resides in active memory and duplicates itself. Worms use parts of an operating system that are automatic and usually invisible to the user. It is common for worms to be noticed only when their uncontrolled replication consumes system resources, slowing or halting other tasks." Now that we know what a worm is, lets take a look at how Nimda fits into this category.

Nimda infects any version of Microsoft Windows through four different methods. This self-propagating worm distributes itself via email, web server attacks, web browsing code, and open network shares. This worm's attack was to infect as many machines as fast as it could, using many exploits and backdoors that have been successful in the past. As noted in the press and my own data collected at my organization, I would say it proved to be very successful. The web server attacks ended up causing a denial of service; and in some cases all propagated methods caused serious security breaches for many companies. As this worm infected machines, it provided remote access with full admin rights and file access to the system. With this window of opportunity open, anything could have been done to that machine in the time it was or still is infected. Along with all of this, it infected many critical system files and .htlm files by putting the original executable code inside of itself.

Details of Infection

Now, that we know general characteristics of this worm, lets see how each of these methods works. The four methods again are infection via web server attack, browser infection via JavaScript, email, and also open network shares.

The first method that impacted companies that I talked with at the beginning of the attack, was the web server attack against the IIS 4.0 and 5.0 servers. This attack used a lot of old exploits and even the successful results of infection still left around from other worms like Code Red. As the worm finds IIS web servers through its own random generation of IP addresses, it tries to run Unicode Web Traversal exploits that have patches available. If successful, the worm will copy itself to the server as admin.dll through TFTP. Once initially infected, the worm will create and listen on the TFTP server ports to copy the file for infection of another system.

This admin.dll file is then executed locally and copied to multiple locations within the system. In addition, the worm attempts to exploit already compromised web servers by using the root.exe backdoor left behind more than likely from Code Red II. As the worm executes, it also attempts to modify files by adding a small piece of JavaScript with in the code like default, index, main or readme, and also other files with the extension .htm, .html, or .asp,. This JavaScript causes a browser window to open outside the viewable desktop and download Readme.eml to the user browsing. This allows the worm to execute when a browser opens the file and without the visitor seeing the window as the JavaScript executes and infects the browser. From this state the client machine is now infected and the email propagation and system file infection begins.

The email method is the one method that will be with us for a while. Along with becoming infected through the browser, you can become infected through emails sent to you as well. This worm gathers email addresses from .htm and .html files as well as through the Messaging Application Programming Interface (MAPI). The advantage of using MAPI, Nimda is able to query email addresses from multiple email clients like Outlook Express. As these lists of email

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

addresses are created from the two methods noted above, the worm sends itself to as an attachment of README.EXE through it is own SMTP engine. When a recipient opens the email or even views it in the case of Outlook or Outlook Express that is not patched, the executable is run and that machine is now infected. The clever thing about this email method of the worm is that it is encoded as a MIME message with 2 parts and also retries its infection every 10 days. One last thing to note about the mail propagation, according to McAfee, is that Windows NT and Windows 2000 cannot be infected via the email message.

Finally, the most significant reason why this worm was so damaging to local networks and workstations is its potential to spread through your system files and network shared files. Once a machine is infected, the worm infects all sorts of different system files. Some of common files infected are load.exe, mmc.exe, and readme.exe, Riched20.dll. But, it could be any file on your system or network. The file infection by Nimda is through the malicious code being wrapped around the original code. This allows the execution of the malicious code along with the original intended code. If the worm is not completely removed from the system, the worm will keep executing as a user tries to open their files. Along with file infections that execute the worm, the system.ini file is also edited to allow execution on restarts. It has also been noted that Nimda could use all available disk space rendering the system useless. If all of this is not enough, another outcome documented is the readme.eml and desktop.eml files that are copied to almost every folder. These files could also be named with a .nwl extension. Not only is the system itself vulnerable to re-infecting itself over and over through any means listed; but there is a large chance of your local network to be infected also. As Nimda peruses the registry it finds, and uses to its advantage, paths found. These are then used to walk through all drive mappings on a system and infect them as well.

Solution that would have Stopped Nimda

I was still surprised how easily this worm propagated through the Internet. How can this happen with the attacks from Code Red and all of its variants just slowing down? I would have thought we knew better. As I read through the different vulnerabilities that this worm uses, I found some of the individual vulnerability patches were released up to 18 months ago. The largest item that would have stopped this attack would be securing IIS. This is not a difficult task as there are many articles on the Internet and books like Stephen Northcutt's book "Windows Security: Step-by-Step". If that is too much work, then you can look toward Microsoft, In the last couple of months they have released a tool for administrators of IIS called the "IIS Lockdown Tool" which is available at http://microsoft.com/technet/security/tools/locktool.asp. I suggest using all of the above tools and testing of your own to come up with a system that works for you and is secure.

Other than just creating the secure server, administrators and users alike must keep their systems, including workstations and applications, up to date on patches. The Patch would have stopped the web server attack against IIS servers, was released from Microsoft on August 15th, 2001. This patch is a cumulative patch for all previous patches of IIS. The patch is Microsoft Security Bulletin 01-044 and available at http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS01-044.asp. The second part of infection through backdoors left by Code Red II. There was a tool released by Microsoft specifically to detect and remove the Code Red II backdoors. This tool is available from Microsoft at

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

http://www.microsoft.com/technet/treeview/default.asp?url=/technet/itsolutions/security/tools/redfix.asp.

Now that the IIS has been patched, you still needed to be diligent and keeping the operating system and any other applications residing on that machine and all workstations like Win9x, WinNT, WindowsME, and Win2000 up to date. The 2nd largest culprit, in my opinion, was un-patched versions Internet Explorer, particularly anything previous to IE 5.5 SP2 and even IE6.0 if you upgraded from a previous install. The IE 6.0 installation can be effected if the Outlook Express files are not updated, depending on how you upgraded. There was a patch released for "Automatic Execution of Embedded MIME Types" vulnerability in March of this year. This patch can be found at http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS01-020.asp would have stopped this propagation of the worm.

There are a few things that we all should be prepared to do to mitigate worms like this. The couple of things for this worm would have been disabling JavaScript within the browser; or disable the TFTP ports TCP 69 and UDP 69 at the routers or firewalls, for those that have them, to stop the web servers from getting the worm files. With this being such a complex worm with many avenues of propagation, it required all of us, administrators and users, to be conscious of what resources we have available to the Internet and ask ourselves: "am I one of those contributing to this damaging worm?" If I am guilty of contributing to this worm's success, how do I get cleaned up and keep this from happening again?

Cleanup of an Infected System

Because of the versatility of this worm, cleanup is not easy to say the least. The recommended option for cleaning a system infected is to format the system drive(s) and reinstall the system software from a trusted medium. Then, after all software is installed, apply all the updates and patches for the system. Finally, after installation and updates connect the machine back onto the network.

If there is no backup of the system and the machine has data that cannot be lost, then you can try to clean the machine manually or with some tools that have been made available by the different anti-virus vendors. From the readings that I have completed, even with using the tools and manually looking for files, there is no guarantee that your system is clean. Since there was a compromise of the security of the system, a remote user could have made changes to your system. Some examples gathered from Symantec's document on Nimda are:

- stealing or changing passwords or password files
- Installing backdoors
- Installing keystroke logging software
- Configuring firewall rules
- Stealing credit card numbers, banking info, personal data, etc.
- Deletion or modification of multiple files throughout your system and network
- Sending of inappropriate or incriminating material from a customer's e-mail
- Modifying access rights on user accounts or files
- Deleting information from log files to such activities

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

Along with the threat that a remote user may still be using your computer, there is the problem making sure that you caught all the files. The tools could take hours to run since every file must be examined and then rebuilt to make sure they are not infected. Also the tools will not remove any .eml of .nwl files, as some of them could be your legitimate files. Also, the tools may not remove the administrative rights and shares that were created from the infection.

With all of this information in front of you and you will want to clean the system, I will give you the general steps, but if you want better details, contact your virus protection vendor. The first thing to do is update your virus protection's definition file. Next check your system.ini file located in the system root (i.e. c:\windows\ folder) and make sure your shell statement only has explorer.exe within it. Then restart your system and run your virus protection software to clean your system. This will only quarantine or delete files, so you may still end up re-installing software.

Finally as another note, Windows ME users should be aware that this operating system utilizes a backup utility that backs up selected files automatically to the _RESTORE folder. This means that an infected file could be stored there as a backup file, Any repair attempts to this folder will fail. In order to disable this function and clean your system, info is available at http://securityresponse.symantec.com/avcenter/venc/data/w32.nimda.a@mm.html.

Who is Affected

As previously noted in the "What is Nimda" section, this worm infects all machines running Microsoft Windows 95, 98, NT, ME, and 2000 operating systems. The reason this infects so many types of machines is because of its many methods of infection. Nimda is able to infect through un-patched Internet Explorer version previous to 5.5 SP2 and all IIS and PWS installations that have not been patched. My personal observation from the researching my IDS and logs showed that most of the attacks came from machines that were running Personal Web Server (PWS) and were located within broadband networks. As this was also being transmitted through e-mail, I very quickly stopped all incoming mail with an attachment with a .exe extension. I also updated my virus protection as soon as it was available. Other administrators that I communicated with also found the mail to be less a threat. I find this more and more the case because many companies and users are getting better about keeping their anti-virus up to date and deleting any emails they do not recognize or expect.

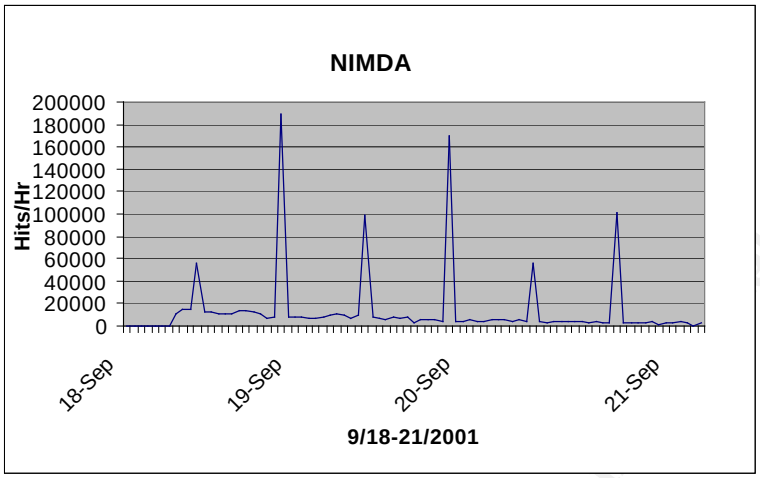
What was the impact

The impact to the Internet community was tremendous. According to eUSAToday.com "The worm, which surfaced in the U.S. last week, has wiggled into more than 1 million computers in the USA, Europe and Asia, clogging Internet traffic and resulting in computer shutdowns for some firms. "It's the most serious Internet attack on the business community," says Jack Danahy, vice president of server security at WatchGuard Technologies. Experts say Nimda could inflict more damage than the Code Red worm, which first surfaced in July and cost firms an estimated $2.4 billion in cleanup costs".

As I read articles like USATOday's, I was grateful that our company has taken security seriously in the last year, and we were only minimally affected. While others I know were not. Even with our security conscious, It was very difficult to combat. There was so much static from this worm

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

that it was very difficult to sort through and find other attacks that may be aimed specifically at us. Below is a chart of what I saw in just the first few days, which from a few comments that I have read in news groups is consistent across the country.



Another good example is from CNN.com article on Nimda. It stated "In a four-hour period starting at approximately 9 a.m. EDT Tuesday, the University of Chicago's Web servers were scanned by nearly 7,000 unique IP addresses looking for vulnerabilities to exploit, said Larry Lidz, a senior network security officer at the university. As a result of the attacks, about 20 university servers were infected with the Nimda worm and had to be disconnected from the network, Lidz said. Now, he is recommending that the infected systems be reformatted and all software reinstalled." This was in a very short amount of time. With infections like this and administrators to busy to watch for remote access and understanding their traffic, this worm will be around for some time to come.

Conclusion

As I finished my analysis of this worm, checking my organizations systems, and writing this paper I to ask myself: "was I prepared?" and "what lessons have I learned?" I was not completely prepared, but I was more prepared that only a few months ago. I found flaws in policies and procedures that hindered us reacting properly and quickly. Let me explain. On one hand, I was lucky enough to have the capability to watch the organization's traffic, watch our different system logs, watch for new vulnerabilities, and even research to help our support staff to be proactive in this fight against the ever elusive black hats. So, I had a pretty good understanding of "regular" traffic. But on the other hand, the procedures and implementation of updates and checks to the systems needs some serious rework. One positive result is that as of this writing, we are already working toward new ideas for fixing the problems that came up during this attack.

The most important lesson that I learned is that documentation, knowledge of the network infrastructure, systems, and traffic are critical to mitigating and responding to attacks like Code Red and Nimda. Another lesson that I learned was that worms like Nimda and Code Red are not going away. Until we as users and Administrators of systems connected to the Internet understand the responsibility that we have to security when we do business on the Internet.

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

I have a gathered a couple of important suggestions to help mitigate worms like this from popping up again and again. First, most important, Make sure that you apply the patches. This includes every time that you update other software on the system. I find this the largest mistake by many administrators. By overwriting a .dll file or some other file, the patch applied can become ineffective. Second, take a few minutes out every day just to look at the latest vulnerabilities. This can be done though a news group or just going to sites like http://www.cert.org or http://www.securityfocus.com. Third, watch your logs. A lot can be learned from just a couple of minutes of review. Within a short time, you will begin to know what is normal and what may need further review. Fourth, understand and document your environment. Learn what servers are open to the internet, what ports each system is listening on, what service are running, what patches are applied, what types of traffic are flowing in and out of your network, and what software is being run. Fifth, create procedures for dealing with this type of situation. If you have these 5 items completed, combating situations like this will be much quicker and simpler.

I have learned a great deal about Nimda and worms in general. I hope that this document may help someone else understand this damaging worm and give them some ideas on how to mitigate it in the future within their home or organization. There is still very few resources put toward security, but I hope that after reading this and other articles on worms and securing your systems that people will begin to become aware and help us combat these damaging situations in the future.

© SANS Institute 2001, Author retains full rights.

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

References

ARIS Predictor Attack Registry & Intelligence Service. NIMDA Worm Reactivation URL:
http://aris.securityfocus.com/alerts/nimda/010926-Alert-Nimda-Reactivation.pdf

ARIS Predictor Attack Registry & Intelligence Service. NIMDA Worm Analysis URL:
http://aris.securityfocus.com/alerts/nimda/010919-Analysis-Nimda.pdf

SANS Emergency Incident Handler NIMDA Advisory URL:
http://www.incidents.org/react/nimda-update-sept27.pdf

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

CERT Coordination Center. CERT Advisory CA-2001-26 "Nimda Worm" URL:
http://www.cert.org/advisories/CA-2001-26.html

NAI/McAfee – W32/Nimda@MM Profile URL:
http://vil.mcafee.com/dispVirus.asp?virus_k=99209&

eUSAToday.com – "Nimda called most serious Net threat yet"
http://www.usatoday.com/life/cyber/tech/2001/09/26/nimda-serious-net-threat.htm

Microsoft TechNet – IIS Lockdown Tool URL:
http://microsoft.com/technet/security/tools/locktool.asp

Microsoft Security Bulletin 01-044 – IIS Cumulative Patch URL:
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS01-044.asp

Microsoft Security Bulletin 01-020 – Automatic Execution of Embedded MIME Types
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS01-020.asp

Microsoft TechNet – Code Red II Removal Tool URL:
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/itsolutions/security/tools/redfix.asp

Counterpane Security Alert – System recovery recommendations URL:
http://www.counterpane.com/alert-nimda-recovery.html

Overview of Code Red – Stephen T. Kelly URL:
http://www.sans.org/infosecFAQ/malicious/code_red2.htm

searchSecurity.com – Definition of a Worm
http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci213386,00.html

CNN.com – Nimda Worm is Tough, but patches are available
http://www.cnn.com/2001/TECH/internet/09/21/nimda.patches.idg/index.html

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

Last Updated: May 25th, 2013

Upcoming SANS Training

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

SANS Malaysia @ MCMC 2013	Cyberjaya, MY	Jun 03, 2013 - Jun 08, 2013	Live Event
SANS Pen Test Berlin 2013	Berlin, DE	Jun 03, 2013 - Jun 08, 2013	Live Event
Industial Control Systems Security Training - Houston	Houston, TXUS	Jun 10, 2013 - Jun 15, 2013	Live Event
Security Impact of IPv6 Summit 2013	Washington, DCUS	Jun 14, 2013 - Jun 16, 2013	Live Event
SANSFIRE 2013	Washington, DCUS	Jun 14, 2013 - Jun 22, 2013	Live Event
SANS Canberra 2013	Canberra, AU	Jul 01, 2013 - Jul 13, 2013	Live Event
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
SANS Mumbai 2013	Mumbai, IN	Jul 22, 2013 - Jul 27, 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 San Francisco 2013	San Francisco, CAUS	Jul 29, 2013 - Aug 03, 2013	Live Event
SANS SEC 560: Network Penetration Testing @ Bangalore 2013	Bangalore, IN	Aug 05, 2013 - Aug 10, 2013	Live Event
SANS Boston 2013	Boston, MAUS	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 Thailand 2013	Bangkok, TH	Aug 19, 2013 - Aug 31, 2013	Live Event
SANS Virginia Beach 2013	Virginia Beach, VAUS	Aug 19, 2013 - Aug 30, 2013	Live Event
Mobile Device Security Summit 2013	OnlineCAUS	May 30, 2013 - Jun 06, 2013	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced