

How to Protect Your Network Against the Nimda Virus

Document ID: 4615

Introduction

Prerequisites

Requirements

Components Used

Conventions

Background Information

Supported Platforms

How to Minimize the Damage and Limit the Fallout

Related Information

Introduction

This document describes ways to minimize the impact of the Nimda worm on your network. This document addresses two topics:

- The network is infected, what can be done? How can you minimize the damage and fallout?
- The network is not yet infected, or is only partially infected. What can be done to minimize the spreading of this worm?

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

This document is not restricted to specific software and hardware versions.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Conventions

For more information on document conventions, refer to the Cisco Technical Tips Conventions.

Background Information

For background information on the Nimda worm, refer to these links:

- http://www.cert.org/body/advisories/CA200126_FA200126.html
- http://vil.nai.com/vil/content/v_99209.htm
- <http://www.sarc.com/avcenter/venc/data/w32.nimda.a@mm.html>

Supported Platforms

The Network-based application recognition (NBAR) solution described in this document requires the class-based marking feature within Cisco IOS® software. Specifically, the ability to match on any part of an HTTP URL uses the HTTP sub-port classification feature within NBAR. The supported platforms and minimum Cisco IOS software requirements are summarized below:

Platform	Minimum Cisco IOS Software Version
7200	12.1(5)T
7100	12.1(5)T
3660	12.1(5)T
3640	12.1(5)T
3620	12.1(5)T
2600	12.1(5)T
1700	12.2(5)T

Note: You need to enable Cisco Express Forwarding (CEF) in order to use Network-Based Application Recognition (NBAR).

NBAR is also supported on some Cisco IOS software platforms starting with release 12.1E. See "Supported Protocols" in the Network-Based Application Recognition documentation.

Class-based marking and Distributed NBAR (DNBAR) are also available on the following platforms:

Platform	Minimum Cisco IOS Software Version
7500	12.1(6)E
FlexWAN	12.1(6)E

If you are deploying NBAR, be aware of bug id CSCdv06207 (registered customers only) . The workaround described in CSCdv06207 may be needed if you encounter this defect.

The Access Control List (ACL) solution is supported in all current releases of Cisco IOS software.

For solutions where you need to use the Modular Quality of Service (QoS) command line interface (CLI) (such as for rate-limiting ARP traffic or to implement rate limiting with policer instead of CAR), you need the Modular Quality of Service Command-Line Interface which is available in Cisco IOS software releases 12.0XE, 12.1E, 12.1T, and all releases of 12.2.

For use of Committed Access Rate (CAR), you need Cisco IOS software release 11.1CC and all releases of 12.0 and later software.

How to Minimize the Damage and Limit the Fallout

This section outlines the infection vectors that can spread the Nimda virus, and provides tips to reduce the spread of the virus:

- The worm can spread through Email attachments of the MIME audio/x-wav type.

Tips:

- ◆ Add rules on your Simple Mail Transfer Protocol (SMTP) server to block any email that has these attachments:

- ◇ readme.exe
- ◇ Admin.dll

- The worm can spread when you browse an infected web server with Javascript execution enabled and using a version of Internet Explorer (IE) that is vulnerable to the exploits discussed in MS01-020 (for example, IE 5.0 or IE 5.01 without SP2).

Tips:

- ◆ Use Netscape as your browser, or disable Javascript on IE, or get IE patched to SP II.
- ◆ Use Cisco Network-based application recognition (NBAR) to filter readme.eml files from being downloaded. Here is an example to configure NBAR:

```
Router(config)#class-map match-any http-hacks
Router(config-cmap)#match protocol http url "*.readme.eml"
```

Once you have matched the traffic, you can choose to discard or Policy Based Route the traffic to monitor infected hosts. Examples of the full implementation are found in Using Network-Based Application Recognition and Access Control Lists for Blocking the "Code Red" Worm.

- The worm can spread from machine to machine in the form of IIS attacks (it primarily attempts to exploit vulnerabilities created by the effects of Code Red II, but also vulnerabilities previously patched by MS00-078).

Tips:

- ◆ Use the Code Red schemes described in:

Dealing with mallocfail and High CPU Utilization Resulting From the "Code Red" Worm

Using Network-Based Application Recognition and Access Control Lists for Blocking the "Code Red" Worm

```
Router(config)#class-map match-any http-hacks
Router(config-cmap)#match protocol http url "*.ida*"
Router(config-cmap)#match protocol http url "*.cmd.exe*"
Router(config-cmap)#match protocol http url "*.root.exe*"
Router(config-cmap)#match protocol http url "*.readme.eml"
```

Once you have matched the traffic, you can choose to discard or Policy Based Route the traffic to monitor infected hosts. Examples of the full implementation are found in Using Network-Based Application Recognition and Access Control Lists for Blocking the "Code Red" Worm.

- ◆ Rate-limit TCP synchronize/start (SYN) packets. This does not protect a host, but it allows your network to run in a degraded manner and still remain up. By rate-limiting SYNs, you are throwing away packets that exceed a certain rate, so some TCP connections will get through, but not all. For configuration examples, refer to the "Rate Limiting for TCP SYN Packets" section of Using CAR During DOS Attacks.
- ◆ Consider rate-limiting Address Resolution Protocol (ARP) traffic if the amount of ARP scans is causing problems in the network. To rate-limit ARP traffic, configure the following:

```
class-map match-any arp
```

```

        match protocol arp
    !
    !
    policy-map ratelimitarp
        class arp
            police 8000 1500 1500 conform-action transmit exceed-action drop violat

```

This policy then needs to be applied to the relevant LAN interface as an output policy.

Modify the figures as appropriate to cater for the number of ARPs per second that you want to allow on the network.

- The worm can spread by highlighting either an .eml or .nws in Explorer with Active Desktop enabled (W2K/ME/W98 by default). This causes the THUMBVW.DLL to execute the file and attempt to download the README.EML referenced in it (depending on your IE version and zone settings).

Tip: As recommended above, use NBAR to filter readme.eml from being downloaded.

- The worm can spread through mapped drives. Any infected machine which has mapped network drives will likely infect all of the files on the mapped drive and its subdirectories

Tips:

- ◆ Block Trivial File Transfer Protocol (TFTP) (port 69) so that infected machines cannot use TFTP to transfer files to non-infected hosts. Ensure that TFTP access for routers is still available (as you may need the path to upgrade code). If the router is running Cisco IOS software version 12.0 or later, you always have the option of using File Transfer Protocol (FTP) to transfer images to routers running Cisco IOS software.
- ◆ Block NetBIOS. NetBIOS should not have to leave a local area network (LAN). Service providers should filter NetBIOS out by blocking ports 137, 138, 139, and 445.
- The worm makes use of its own SMTP engine to send e-mails out to infect other systems.

Tip: Block port 25 (SMTP) on the inside portions of your network. Users who are retrieving their e-mail using Post Office Protocol (POP) 3 (port 110) or Internet Mail Access Protocol (IMAP) (port 143) do not need access to port 25. Only allow port 25 to be open facing the SMTP server for the network. This may not be feasible for users using Eudora, Netscape, and Outlook Express, among others, as they have their own SMTP engine and will generate outbound connections using port 25. Some investigation might need to be applied to the possible uses of proxy servers or some other mechanism.

- Clean Cisco CallManager/Applications Servers

Tip: Users with Call Managers and Call Manager application servers in their networks have to do the following to stop spreading of the virus. They must not browse to infected machine from the Call Manager and also they must not share any drives on the Call Manager server. Follow the instructions provided in Cleaning Nimda Virus from Cisco CallManager 3.x and CallManager Applications Servers for cleaning the Nimda virus.

- Filter the Nimda Virus on the CSS 11000

Tip: Users with CSS 11000 must follow the instructions provided in Filtering the Nimda Virus on CSS 11000 for cleaning the NIMDA virus.

- Cisco Secure Intrusion Detection System (CS IDS) response to the Nimda Virus

Tip: The CS IDS has two different components available. One is the Host-based IDS (HIDS) which has a Host Sensor and the Netowrk-based IDS (NIDS) which has a Network Sensor, both of which respond in a different manner to the Nimda virus. For a more detailed explanation and the recommended course of action, refer to How Cisco Secure IDS Responds to the Nimda Virus.

Related Information

- **Using Network–Based Application Recognition and Access Control Lists for Blocking the "Code Red" Worm**
 - **Dealing with mallocfail and High CPU Utilization Resulting From the "Code Red" Worm**
 - **Using CAR During DOS Attacks**
 - **Cisco Security Advisories and Notices**
 - **Technical Support – Cisco Systems**
-

[Contacts & Feedback](#) | [Help](#) | [Site Map](#)

© 2008 – 2009 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)

Updated: Mar 06, 2008

Document ID: 4615
