

FILTERING NIMDA WORM

Overview

W32/Nimda ("Nimda") worm is similar to the Code Red worm that was unleashed on the public data network during the summer of 2001. Nimda does not itself destroy or corrupt data but it does leave behind executable files that leave client and server machines compromised and unknowingly made to act as agents for: 1) further propagating Nimda and; 2) unauthorized remote users to launch Distributed Denial of Service Attacks (DDoS).

The Nimda worm has been reported spreading using multiple mechanisms including email propagation, browser propagation, and file system propagation. File system propagation is made possible by vulnerabilities in Microsoft's Internet Information Server (IIS) Web server and openings left by the Code Red worm (for more information see Foundry's Field Advisory on Code Red).

This Foundry Advisory addresses mitigating the spread of Nimda through file system propagation only. Customers are advised to work with their email and Web browser software vendors to implement policies that disable features that allow viruses to spread through opening and reading email and browsing Internet sites. Customers are also advised to promote virus-free networks by updating their anti-virus software on a regular basis for detecting and isolating new outbreaks of viruses, worms and other malicious code. For customers currently using the Microsoft IIS Web server, more information about patching vulnerabilities is available at: <http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/topics/Nimda.asp>

File System Propagation

One of the ways the Nimda worm is propagating is by taking advantage of vulnerability in Microsoft's IIS servers that allows unauthorized users to gain control of system-level commands. The attacking agent establishes a TCP connection with IIS and then sends a request that renders the system's security void and complete control is given to the agent.

Once control is established, the worm files are saved on the system and permission levels are changed to grant remote access. The Nimda worm alters the system in 4 ways:

- Enables the sharing of the c: drive
- Creates a "Guest" account on Windows NT and 2000 systems
- Add this account to the "Administrator" group thereby providing full access to the compromised system
- Creates Trojan horse versions of applications, such as Internet Explorer, which can further infect any machine accessing the application

More information about his vulnerability can be found at the CERT Coordination Center:
<http://www.cert.org/advisories/CA-2001-26.html>

Customers utilizing Foundry's line of ServerIron switches can take advantage of ServerIron features to protect Web servers from worm infections and Denial-of-Service (DoS) attacks. ISPs can also prevent the code red worm from entering their network and tying up costly peer / transit links as well as protecting their customers.

FILTERING NIMDA WORM

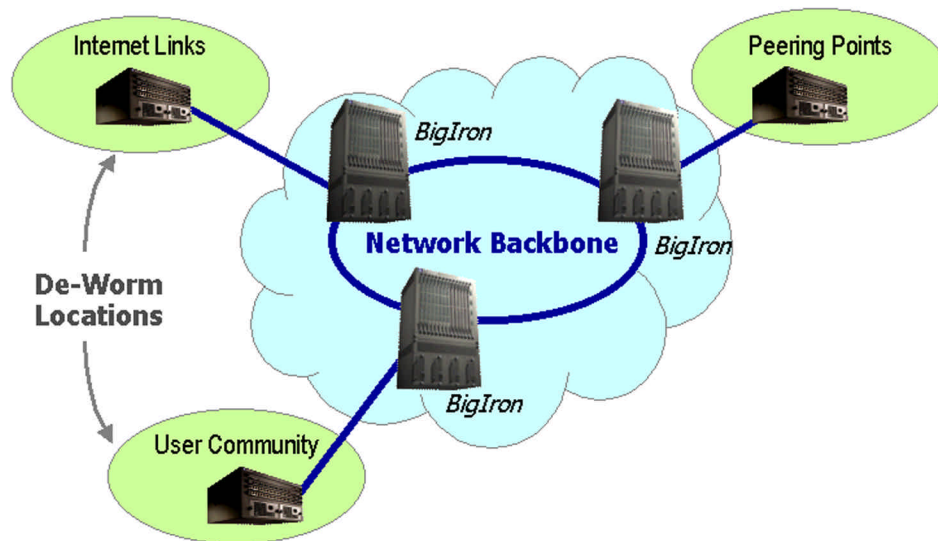
This field advisory provides a configuration example for detecting and isolating Nimda worms thereby preventing file system propagation.

De-Worming Traffic through Transparent URL Segment Matching

To prevent un-wanted worm solicitations reaching web servers, URL switching can be deployed. Similar to previous examples, a pattern match for the offending worm signature can be applied to all HTTP traffic directed to the web server. Upon a successful match, the http request can be directed to a server group for discard or logging.

The Nimda worm uploads specific files through HTTP requests that are visible in the URL. Namely, "cmd.exe" and "root.exe". The ServerIron can scan URLs for this pattern. If they are found in the URL, the packets can be forwarded to a worm-tracking server, such as a dedicated cache or plain vanilla PC. With current release of ServerIron code, this server must be able to reply to Layer 4 health checks. It is recommended that 2 "servers" belong to the group that can respond to ARP and PING health checks (for redundancy) regardless if they are listening on port 80. The ServerIron's TCS functionality is utilized in this process.

ServerIrons can be placed in front of servers, on internal networks, in front of user communities, or at peering points to de-worm ALL port 80 traffic.



The benefit is clear: ISPs can protect peers and customer groups from transmitting or receiving the Nimda worm; large enterprise / campus networks can prevent the user community from becoming infected.

FILTERING NIMDA WORM

Sample Configuration

```

!
!
server source-ip 192.168.0.1 255.255.255.0 0.0.0.0
server source-ip 206.124.144.184 255.255.255.0 206.124.144.254
!
url-map "nimdafiliter"
method pattern
default "letgoby"
match "cmd.exe" 99
match "root.exe" 99
!
url-map "letgoby"
default 0
!
!
server cache-name Nimda 206.124.144.183
port http
port http no-health-check
port http url "HEAD /"
port http l4-check-only
!
!
!
server cache-group 99
cache-name Nimda
url-map nimdafiliter
no-group-failover
no http-cache-control
url-switch
!
ip policy 1 cache tcp http local
!

```

Defines pattern to look for in the traffic and where to send successful hits.

If traffic does not contain offending pattern, continue to forward.

Nimda "cache server" receives Nimda Red worms. Multiple servers can be used.

The "no http-cache-control" command is used to insure all traffic that matches the url-map will always go to the Nimda cache group.

Caveats

The current version of the Nimda worm utilizes certain know patterns in the URL string to deploy files on the IIS server. As new worms emerge, additional pattern matches may need to be configured. This also allows the ServerIron to be used in future worm prevention. See Microsoft Security Bulletin MS01-033.

Legitimate traffic may also be dropped if it is requesting the file pattern that is being isolated. Always discuss solutions with your Web managers.

With the current version of IronWare for the ServerIron, the "cache server" must be present (and capable of receiving Ping requests) in order to pass health checks.



FILTERING NIMDA WORM

More Information

For questions or further assistance, please contact a Foundry sales office near you (<http://www.foundrynet.com>)

Existing Foundry customers can contact the toll free technical support line at 877-887-2622.

© 2001 Foundry Networks, Inc.