# Global Information Assurance Certification Paper

# A Little Worm Goes a Long Way

By

Grant Jewell

**Advanced Incident Handling and Hacker Exploits**

**SANS GCIH Practical Assignment v.2.0**

# I Introduction

My recent move into the field of Information Assurance has brought to light the enormous learning curve that exists between a system administrator position and a security professional. The amount of information that must be learned can be overwhelming. Understanding that the ratio of hackers to security professionals is nearly 1,000:1 makes the task even more challenging. My current role in our organization is to perform security monitoring of perimeter devices including monitoring the logs of Intrusion Detection Sensor (IDS), firewalls and Critical Extranet Servers. Along with system administrators, I'm the first line of defense in incident identification and escalation.

My first opportunity to learn about standard industry practices for Incident Handling and recommended policies and procedures was with SANS. In discussing these best practices with co-workers, I realized some of the standards were achievable in our organizational structure, while others would always remain out of reach.

This paper discusses an incident involving of Code Red II infection within my company. I will discuss the strengths of our incident handling process during this event, areas for improvement, as well as additional outcomes as a result of the attack.

# II Exploit Details

**Name –** Code Red II

**CVE (Common Vulnerabilities and Exposure):** CAN-2001-0500
**CERT Advisory** – CA-2001-13 used by the malicious code
**CERT Incident** – IN-2001-09

**References**
http://www.cert.org/incident_notes/IN-2001-09.html
http://www.symantec.com/avcenter/venc/data/pf/codered.ii.html

**Operating Systems** – Windows NT 4.0 with IIS 4.0 or IIS 5.0 enabled
Windows 2000 (Professional, Server, Advanced Server, Datacenter Server) with IIS 4.0 or IIS 5.0 enabled
Cisco CallManager, Unity Server, uOne, ICS7750, Building Broadband Service Manager (these systems run IIS)
Cisco 600 series DSL routers (Cert, CA-2001-03)

**Services** – Index Server 2.0
Indexing Service 2000

**Protocols/Ports** – TCP and HTTP

**Brief Descriptions** – Code Red II exploits a known vulnerability in Microsoft Index Server 2.0 or Indexing Service 2000 ISAPI Buffer Overflow. This self-propagating code creates an interruption of service on NT 4.0 machines and installs backdoors on certain Windows 2000 servers. The compromised host uses a random number generator to continue to connect to servers via TCP port 80 and infect IIS servers with the same first octet of the victim IP address.

**Variants**

Several different variants have emerged as a result of the original Code Red worm. These variants have utilized the same vulnerabilities in IIS servers as well as taken advantage of backdoors left behind after Code Red II.

Code Red was one of the first worms to take advantage of the IIS buffer overflow vulnerability in the Indexing Server Service. Code Red II is a hybrid of Code Red due to the use of the same buffer overflow technique, however, that is the only similarity between the two. The Code Red worm attempts to connect to TCP port 80 based on a random selection of a host. Once a web server is found and a TCP connection is established, the worm sends a crafted HTTP GET request to the victim computer, and attempts to exploit the buffer overflow on IIS Index Server. This scenario will be described later in more detail. After a victim is compromised, the same crafted HTTP GET request exploit is used on another set of randomly generated hosts unless the server has already been infected. In that case, the worm will go into an infinite sleep mode. If the server is vulnerable to the buffer overflow and has not been patched, it has the potential to infect other servers and have the web pages on the host server defaced with HTML displaying: "Welcome to http:// www.worm.com !
Hacked By Chinese!" Code Red's purpose appears to be to overtake as many zombie IIS servers as possible in an effort to launch a massive Denial of Service (DoS) attack against an particular Whitehouse web site on July 19, 2001. (Chien, 2001)

Code Blue has similar characteristics of Code Red and Code Red II in the way it handles the random number generator and the way it propagates. However, unlike Code Red II, Code Blue is spread via a single .dll and executed via an .exe file. This worm appears to be less malicious and less destructive than Code Red II because it does not install backdoors, but it does create a less stable environment by installing a script which removes Internet Server API (ISAPI) mappings for .ida. Code Blue actually helps prevent re-infection of Code Red or Code Red II by removing the buffer overflow vulnerability with Microsoft IIS. (Xforce Advise96, 2001)

Code Nimda (also known as Code Rainbow) is a combination of Code Red and other worms used to infect a larger base of operating systems. Code Rainbow has the capability to infect systems running Windows NT/2000 and ME. This worm takes advantage of any backdoors left behind from "Code Red II", infects computers via email clients, compromises the client-to-client relationship via network shares, and spreads from web servers to clients through compromised web sites. Nimda uses a random number generator like Code Red II to infect IIS servers via port 80 by using HTTP port

probes to search for an available web server to infect. In addition to the known unicode vulnerabilities, Nimda uses email and other known vulnerabilities for worm propagation. Since its inception, several new variants of Nimda have been released which have been more malicious because they fixed some flaws in the earlier version of the Nimda code. (CA 2001-26, 2001)

# III Attack Details

### Background

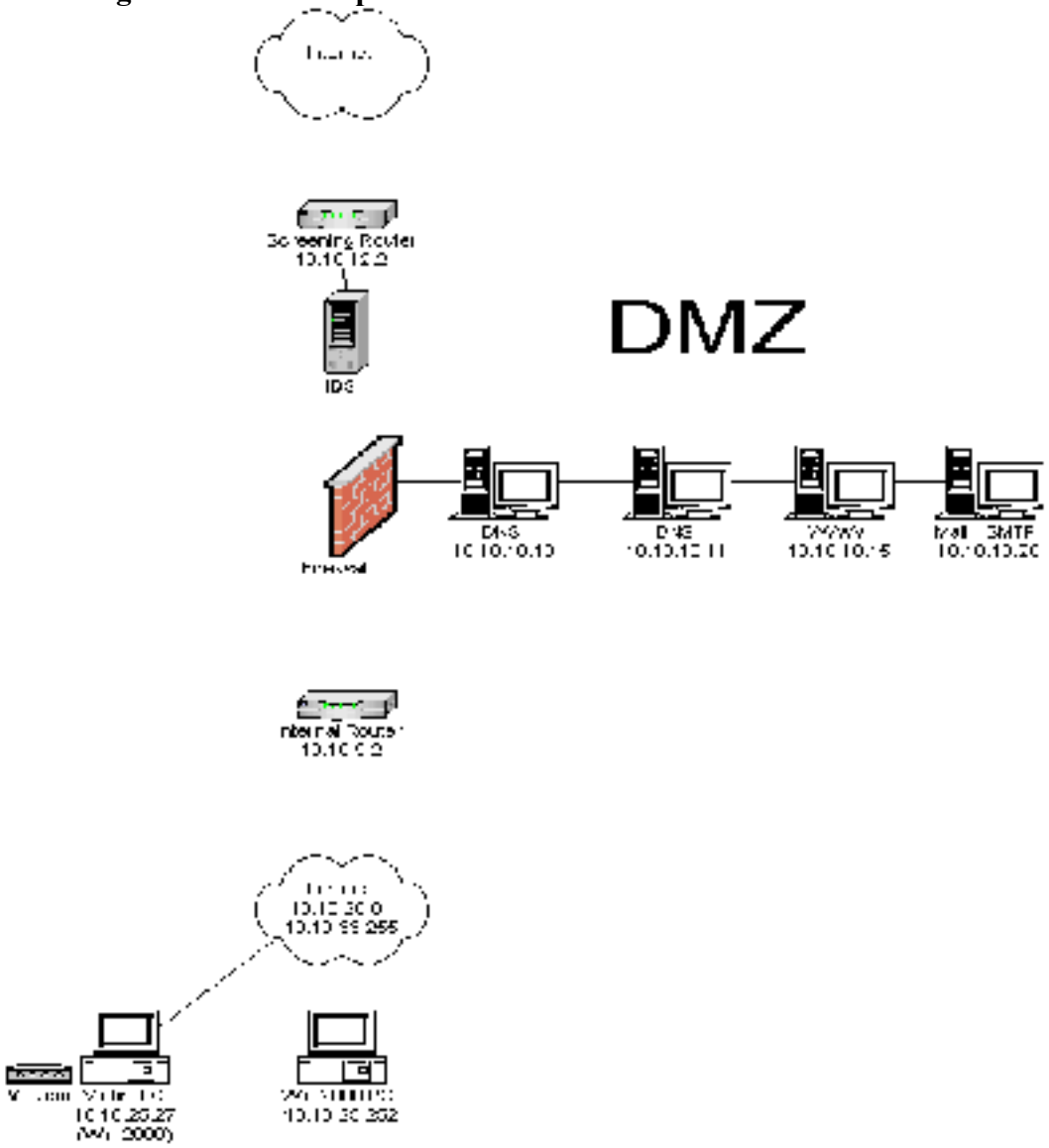
Since this was an actual incident involving the use of malicious code, I can only speculate about the hacker's motivation. The worm infected several thousands of machines throughout the world, so I believe it is safe to say that our company was not the direct target of attack. The original Code Red's intent was to hijack as many machines as possible in an effort to perform a major Denial of Service (Dos) attack against a specific Whitehouse web server. No specific target host was identified with Code Red II; therefore, I can only assume that this worm's intent was to attack various web servers throughout the world in attempt to leave Trojan backdoors and cause major disruption of services.

After reviewing all the logs associated with our Code Red II infection and analyzing these logs against the countermeasures in place during the time of the attack, it appears that the exposed Windows 2000 workstation was randomly selected. Given the broad scope of exposure throughout the Internet as a result of this self-propagating worm, my organization has concluded that the compromised system's external connection was the initial point of infection of our internal network. This workstation had an unauthorized modem that accepted inbound calls as well as having IIS server installed on the machine by default. This combination of errors provided the entry point into our internal network. This backdoor enabled a worm that would normally be detected and blocked at our intrusion detector sensor to propagate throughout our internal network compromising hosts and attempting to make connections with external machines.

The only thing that ended up helping us minimize the damage incurred by Code Red II was the flawed nature of the random number generator that ultimately limited the worm's exposure to one particular location on our network. If a more intelligent number generator would have been used, the impact on our network could have been 100 times worse than the impact of a small spread of Code Red II.

For purposes of example our company network will be depicted throughout this paper as several class-C networks within the 10.10.0.0 range.

**Network Diagrams and Descriptions**




My company network utilizes a four-tiered approach to defense against unwanted traffic and attacks. The first layer of defense (depicted above) is the Internet screening router, which has a very limited access control list (ACL). This ACL allows specific traffic/service connections to servers in the DMZ for Web, DNS, SMTP, and other traffic. On average the Internet screening routers throughout my organization block eighty percent of the unwanted packets through the use of well-defined ACLs. .

**Internet Screening Router ACL**

!
clock timezone EST –5
clock summer-time EDT recurring

```
ip domain-list company.com
ip name-server 10.10.10.10
ip name-server 10.10.10.11
!
interface FastEthrnet 0/0
        description Internet Network
        ip address 10.10.12.2 255.255.255.0
        ip access-group 115 out
!
access-list 115 permit tcp any any established
access-list 115 deny udp any any eq snmp
access-list 115 permit tcp any 10.10.10.0  0.0.0.255 eq smtp
access-list 115 permit udp any 10.10.10.0  0.0.0.255 eq domain
access-list 115 permit tcp any 10.10.10.0  0.0.0.255 eq ident
access-list 115 permit udp any 10.10.10.0  0.0.0.255 eq ntp
access-list 115 permit tcp any host 10.10.10.15 eq www
access-list 115 permit tcp any host 10.10.10.15 eq 443
```

The second layer of defense within our company consists of Intrusion Detection Sensors located between the Internet screening router and the external firewall. These Intrusion Detection Sensors provide real-time packet analysis, relying on both automation response and human intervention. The IDS offers the capability to issue TCP Resets to terminate unauthorized data transmissions as needed or requested. Out of the remaining twenty percent of unauthorized data packets it is believed that the IDS sensor is able to record close to one hundred percent of that traffic and deflects approximately eighty percent of the remaining packets.

The third layer of defense includes stateful firewalls with specific, limited rulesets allowing internal access to servers in the DMZ. A properly written firewall should drop the remaining unsolicited data packets. The firewall rulesets allow limited access for internal users as well as permitting only critical services to pass from the Internet through the DMZ to the appropriate users. An excerpt of the firewall rules follows:

| NO | Source | Destination | Service | Action | Comment |
|---|---|---|---|---|---|
| 1 | Any | Bad_web_sites | Any | Drop | |
| 2 | 10.10.10.10<br>10.10.10.11<br>10.10.10.15 | Any | Traceroute<br>Whois | Accept | Network Troubleshooting Rule |
| 3 | FW | Any | Any | Drop | Stealth rule |
| 4 | 10.10.12.2<br>10.10.11.15<br>10.10.10.10<br>10.10.10.11<br>10.10.10.15 | Syslog Server<br>Monitoring Server | Snmp-trap<br>Syslog | Accept | Syslog and SNMP trap rule. |
| 5 | XYZ-SMTP | Any | Ident<br>Smtp | Accept | SMTP outbound rule. |
| 6 | Any | XYZ-SMTP | Ident | Accept | SMTP inbound rule #1 |
| | Any | XYZ-SMTP | Smtp | Accept | SMTP inbound |

| | | | | | |
|---|---|---|---|---|---|
| | | | | | rule #2 |
| 8 | Any | Any | Smtp | Reject | SMTP cleanup rule |
| 9 | Proxy | Any | Any | Accept | Proxy Server rule |
| 10 | XYZ | Any | ftp<br>telnet<br>pop-3<br>ssh-tcp | Accept | Normal XYZ outbound access. |
| 11 | 10.10.12.2 | DMZNTP | Accept | | Network time protocol rule. |
| 12 | Any | Any | Any | Drop | Cleanup rule |

The company utilizes proxy servers; therefore, web traffic as well as other services can be filtered through the company's DMZ.

The fourth layer of defense is internal screening router with specific ACLs, which limit the access for internal machines to the DMZ. This is the final layer of defense to block any unwanted traffic that managed to slip by the other three layers of the architecture.

**Internal Screening Router ACL**

```
!
clock timezone EST –5
clock summer-time EDT recurring
ip domain-list company.com
ip name-server 10.10.10.10
ip name-server 10.10.10.11
!
interface FastEthrnet 0/0
        description Internet Network
        ip address 10.10.9.2 255.255.255.0
        ip access-group 120 in
!
access-list 120 permit tcp any any established
access-list 120 permit udp 10.10.10.0 0.0.0.255 any host eq snmp-traps
access-list 120 permit tcp 10.10.10.20 any host eq smtp
access-list 120 permit tcp 10.10.10.0  any host eq ident
```

Although a four-tiered architecture is implemented at the location where the attack occurred, the unauthorized modem connection created the vulnerability that was ultimately exploited by Code Red.

**Protocol/Service Descriptions**

The protocols and services that were involved with the Code Red Worm are**:**

TCP/IP - Transmission Control Protocol/Internet Protocol is used to establish a reliable connection over a network between two computers to facilitate the transfer of information. TCP is used for error checking during the transfer of packets through the established connection.

HTTP – Hypertext Transfer Protocol is used by web servers to provide stateless connections between a web server and web browser to transmit packets of hypermedia between the Application levels of the Open System Interconnect (OSI) model.

Index Server – This service used by Microsoft IIS and Peer Web Services enables a user to cache visited web pages into a temporary virtual directory. This virtual directory allows a user to quickly perform text searches with just a single mouse click.

**Exploit Description**

Code Red II contains two parts: the initial buffer overflow used to obtain access to the system, and the payload of the malicious code.

1) Code Red II utilizes a known IIS Index Server buffer overflow to gain access to the machine. The initial stages of Code Red II starts by using the built in random number generator to identify a series of IP addresses to attempt to establish a TCP connection with these IP's via port 80. By attempting to connect to IP's via port 80 the random number generator discovers which servers are running web services. Then Code Red II utilizes the buffer overflow to gain access control. The number of threads attempted by Code Red II depends on the variant of the worm and the base language of the infected server. For example, IIS server with Chinese as the default language will cause the random number generator to create 600 threads. Any other language triggers the worm to generate 300 threads. Once a web server is located, an HTTP Get request is made to the destination server using a malformed HTTP (see below) to overflow the Indexing Service on the IIS server. This buffer overflow provides the worm or hacker with the ability to execute code in the Local System security context. In essence, the worm or a hacker is able to gain full system control via the use of the below code to create a buffer overflow in the IIS 4.0 or 5.0 unpatched server. (IN-2001-09, 2001)

2) Once a system has been compromised via the buffer overflow the payload of the worm is issued. The first step after the system is compromised is to check for an existing presence of Code Red II atom. Upon discovery of the atom the worm goes into an infinite sleep. If the Code Red II atom is not present the worm duplicates itself and initiates the propagating nature of the worm. The duplicate version of the worm checks for the default language of the web server. If Chinese is the default language the propagation of 600 threads begins to scan for the next 48 hours. However, if English or any other language is the default language, 300 threads will be created for scanning over the next 24 hours. The initial copy of the worm begins generating the system level compromise by copying %SYSTEM%\CMD.EXE to

root.exe in the IIS scripts and MSADC folders enabling the execution of various commands. The worm utilizes the IIS server privileges to create a copy of explorer.exe in both the c:\ and d:\ and then uses the Trojan horse explorer copy to create a virtual drive mapping if drive c:\ and d:\ exist. These final two steps usually only occur on Windows 2000 servers running IIS 4.0 or 5.0 with Indexing Service installed. This is the malicious part of the Code Red II because the installation of the backdoor enables a hacker the means to destroy files systems as well as read and compromise critical data. (IN-2001-09, 2001)

**Source Code**

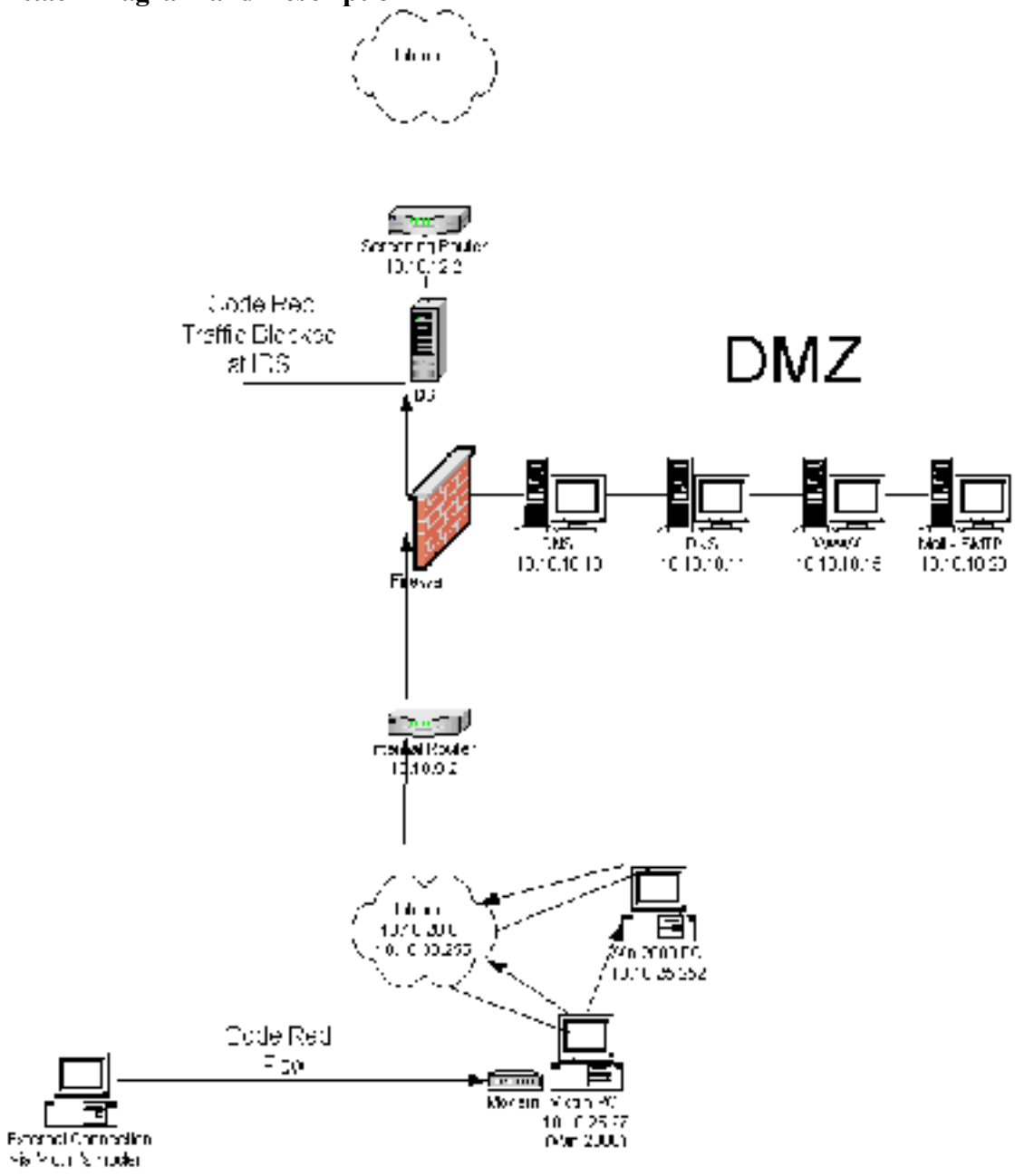
#Software: Microsoft Internet Information Services 5.0
#Version: 1.0
#Date: 2001-08-14 15:20:22
#Fields: date time c-ip cs-username s-ip s-port cs-method cs-uri-stem cs-uri-query sc-status cs(User-Agent)

2001-08-14 15:20:22 192.168.27.30 – 192.168.25.252 80 GET /default.ida
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXX%u9090%u6858%ucbd3%u7801%u90
90%u6858%ucbd3%u7801%u9090%u6858%ucbd3%u7801%u9090%u9090%u8190%u
00c3%u0003%u8b00%u531b%u53ff%u0078%u0000%u00=a 200 -

2001-08-14 15:22:40 192.172.250.127 – 192.168.199.157 80 GET /default.ida
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXX%u9090%u6858%ucbd3%u7801%u90
90%u6858%ucbd3%u7801%u9090%u6858%ucbd3%u7801%u9090%u9090%u8190%u
00c3%u0003%u8b00%u531b%u53ff%u0078%u0000%u00=a 200 -

Above is an example of the source code used on servers to exploit the buffer overflow vulnerability within IIS and propagate Code Red II.

**Attack Diagram and Description**




The attacker was able to circumvent my organization's countermeasures by finding a workstation running Windows 2000 with 2000 Index Server installed. The victim PC had Windows 2000 Professional installed using Indexing Service 2000 and a modem. The point of compromise was the modem and PcAnywhere software. A contractor originally configured the machine for a member of a small information technology group. All the initial default settings for Windows 2000 were installed (including IIS). The user had no need of the IIS server nor was aware that it was resident on the machine.

The modem was connected to an external partner already infected by Code Red II. The random number generator of the worm connected to the victim PC with index service 2000 running. The self-propagating nature of the worm spawned the spread of the worm from the external customer to our internal victim machine. Once the worm discovered IIS 5.0 installed on our Windows 2000 workstation, it attempted to connect via TCP port 80. After a TCP connection was established, the worm was able to utilize the ISAPI buffer overflow in the Indexing Service 2000 and gain access to an internal machine.

Once inside the corporate infrastructure the worm began propagating and attempted to spawn another 300 threads. The worm that infected the network seemed to have a bug because the random number generator kept the Class A and B address the same while propagating throughout our network. This flaw helped reduce the number of infections and enabled us to better contain the spread of the worm. Once Code Red II was present in our network, the compromised victim's PC IP address of 10.10.25.27 began spawning and infecting several other machines within our internal network as well as attempting to connect to IP's outside our company. The attempted port scans via port 80 to external addresses triggered the identification of the worm in our network. The worm actually caused a Denial of Service condition on a firewall and the IDS box in place was able to identify and terminate the attempted TCP connections of the worm.

**Attack Signatures**

Several different signatures exist for the identification of Code Red II or one of its variants. Each signature depends on the type of IDS or sniffer used to identify the malicious code. For purposes of example, I will discuss two popular IDS products: RealSecure produced by ISS, and Network Century by Network ICE.

RealSecure

To identify Code Red II with RealSecure, custom signatures need to be created for the appropriate source code patterns. Below is the main signature recommended by ISS to help identify the presence of Code Red II activity.

> HTTP_IIS_Index_Server_Overflow – This custom signature identifies attempts to utilize the known buffer overflow of the ISAPI extension by identifying any signature with the string of "\ida$" in the header. (Xforce Advise 90, 2001)

NetworkICE

> 2004602 – "The Code Red II worm consists of self-propagating malicious code which exploits a vulnerability in the Microsoft IIS service. This detection is a special case of the more generic detection described under ISAPI index extension overflow." (Network ICE, 2001)

### Protection

Since Code Red II utilizes a known ISAPI buffer overflow with the Indexing Service on IIS 4.0 & 5.0 servers as well as the Index 2000 Service, the obvious way to protect from this vulnerability is to apply Microsoft's patch to resolve the buffer overflow issue. The appropriate patch for this issue is q300972 for Windows NT 4.0 and q296576 for Windows 2000. These patches are located online at www.microsoft.com/downloads/search.asp, which is Microsoft's Download Center. A user whose machine has been infected with Code Red II can also download a "Code Red II Cleaner" from this web site to help eradicate the worm from their network. (Microsoft, 2001)

## IV Incident Handling

### Preparation

My company has several policies and procedures in place to facilitate proper incident handling as well as several countermeasures to help prevent an incident from occurring. As described earlier in the network design the most obvious countermeasures include a four-tiered network architecture. Using a four-tiered approach with well-written access control lists and firewall rule sets can prevent many incidents from ever occurring. In addition to the network architecture, all email servers and personal desktops have virus software installed, which is updated weekly or more frequently, as required. However, as we saw in this situation, it only takes one machine that doesn't adhere to the established policies and procedures to make the entire network vulnerable to attack.

Several company policies and procedures either failed in this instance or were violated by the workstation owner, thereby rendering the system vulnerable to attack. The most important policy violated, which I believe granted the attacker access to the Windows 2000 machine, was the installation and use of a modem. Company policy specifically states, "Modems cannot be used on systems connected to our network. Any exceptions must be approved by Information Assurance." Another policy that is implemented throughout most of the corporation is the standardization of the company's operating system and applications. This provides the opportunity to test software and operating systems before final deployment to end users to help resolve conflicts as well as identify major security problems with the applications or operating systems. Currently the company's standard tested operating system is Windows NT 4.0 and not Windows 2000. The standardization of tested operating system loadsets takes the guesswork out of depending on individual desktop professionals or contractors to secure each individual desktop upon installation.

As discussed in our seminar our organization has an Incident Handling Process procedure written to deal with a variety of situations. Malicious worms is just one of the areas covered in this document, which states that in the event of a computer worm the processes that need to occur are identification of the worm, containment, eradication, recovery, and follow up. Each one of these main categories is outlined in the procedure.

The CIRT (Cyberattack Incident Response Team) Procedure document discusses ways to identify the malicious code and the steps that must be performed by the network administrators upon discovery of the malicious code from the initial disconnection from the network to the paging of Security Information & Analysis Center (SIAC) personnel for further instructions. This document provides an overview of the steps that need to be performed by network personnel in order to minimize the damage incurred by malicious code worms and other security incidents. Once a compromised machine is discovered, IT personnel are instructed to do only three things: 1) disconnect the machine from the network 2) Call the SIAC and 3) begin a full, byte-by-byte backup of the system.

Although there were several countermeasures and procedures in place to deal with an incident under normal circumstances, this incident involved a workstation in a small work group, which did not comply with or adhere to published company policies and standard. It was discovered at a later time that a contractor had performed the installation of Windows 2000 and all of the default services were implemented. The user of this machine was unaware that her machine was even running the IIS and the Indexing Service. Therefore the incident response team was faced with many additional unexpected problems. .

Microsoft attempts to assist users by implementing additional services without specifically asking during installation in effort to make their product more convenient. However, this "convenience" often causes headaches for security personnel because every additional service results in the possibility of exploitation of added vulnerabilities.

Our Security Information and Analysis Center works as a team with system administrators to assist with security issues. Although the ideal situation, as discussed at SANS, would be for one of our team members to be on site to handle the events that arise, we are a virtual organization and must rely on IT personnel at each site to gather logs, make copies of files, and restore the systems. Information Assurance acts as the lead incident handlers making every attempt to control and monitor the situation from our remote location without travelling onsite except in critical situations. Due to the structure of our organization, the SIAC team members do not maintain a toolkit for recovery of infected systems as recommended during our conference. We have to rely on the network administrators on site at each location to control the situations as they occur and forward the critical information to our team for analysis and instruction. In cases involving legal investigations or critical violations of security policies, a member of our team will travel onsite to help maintain the chain of custody of the evidence and perform further investigations as required.

**Identification**

Code Red II began infecting our network on the morning of August 14, 2001. During that morning a SIAC team member noticed that the IDS traffic in one of our locations was alarmingly high compared to the normal state of traffic. On average we see about 1,000 records per week on that particular IDS, however during this morning the IDS reported

close to 75,000 alerts in a very short period of time. In addition to the increased number of traffic from external addresses the IDS was reporting a staggering amount of internal Synflood signatures. After monitoring the activity for a short time, the firewall administrator and network engineer for that location were contacted and informed about the increased network activity.

After discussing the issue with the network engineer, the SIAC member was informed that there were some firewall problems with that particular Internet pipe and that the firewall had been taken down due to a hardware problem. In addition to the removal of the firewall, the Internet connection was disconnected while maintenance was performed on the firewall. All the parties involved concluded that the traffic being reported on the IDS must have been a false positive because the Internet connection had been disconnected at the screening router. Following our current operating security procedure, our IDS manager informed the Information Assurance manager of the unusual activity and the network maintenance activity at this location. She informed our IDS manager to continue monitoring the activity and provide an update if any other suspicious activity occurred.

About an hour later in the early afternoon our IDS manager attempted to download the database of alerts from the appropriate IDS, however he was unable to connect to the IDS to retrieve the relevant information. We later discovered that the network engineer had powered down the intrusion detection sensor that in turn corrupted the IDS database and destroyed some of the initial evidence.

At 6:21 PM EDT on the 14th of August 2001, the Security Information and Analysis Center (SIAC) received a page from a network administrator who reported unusual activity on the logs of some web servers. The Information Assurance manager and lead incident handler was on-call that evening and she contacted the network administrator regarding the page. The network administrator reported activity that he believed to be Code Red II on several of the web servers throughout the 10.10.0.0 TCP/IP domain. My manager requested examples of the logs from the network administrator for analysis. However, due to network upgrades and outages, the mail servers were down in this location so the network administrator is unable to forward the appropriate information. Once the network connectivity was restored the network administrator forwarded the server logs, which revealed the following:

2001-08-14 15:20:22 10.10.25.27 – 10.10.25.252 80 GET /default.ida
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXX%u9090%u6858%ucbd3%u7801%u90
90%u6858%ucbd3%u7801%u9090%u6858%ucbd3%u7801%u9090%u9090%u8190%u
00c3%u0003%u8b00%u531b%u53ff%u0078%u0000%u00=a 200 -

2001-08-14 15:22:40 10.10.25.27 – 10.10.199.157 80 GET /default.ida
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXX%u9090%u6858%ucbd3%u7801%u90
90%u6858%ucbd3%u7801%u9090%u6858%ucbd3%u7801%u9090%u9090%u8190%u
00c3%u0003%u8b00%u531b%u53ff%u0078%u0000%u00=a 200 -

From the initial information relayed over the phone, our lead incident handler confirmed this incident and began the incident handling process. My manager was faced with the decision of whether or not we should continue monitoring the incident or contain and eradicate the problem. Knowing that Code Red II was a malicious worm and there was a potential that our servers could be used in attacking other companies, my manager decided to contain and eradicate the problem. Sometimes, containment and eradication may destroy critical information needed during a legal investigation. However, in cases of common worms, our CIRT procedure states that the focus of the team should be to minimize the affect on our network by containing the problem.

At 6:45 PM EDT, after discussing the situation with the network administrator, the lead incident handler took down all the information and told the administrator to wait until he heard from her before taking action. She then notified her manager of the situation and paged the division's network manager in order to get personal contact information of the supervising network manager at that location. Unfortunately, the Information Assurance manager was unable to contact the East Coast network manager. She contacted two other network managers to obtain the contact information, but no one had it. Because he was new to the job and contact lists had not been updated since he assumed that position. She then called the West Coast IT manager for that site and asked that he take the technical lead on this incident until other managers were located.

Around 8:00 PM EDT, the firewall was repaired and the Internet connection was restored. Once the external connection was restored the IDS at that location began reporting over 200,000 Synfloods. These Synfloods were the first available records confirming some of the activity of Code Red II in addition to the log activity observed by the network administrator. Below is a small sample set of the activity recorded by the IDS at the infected location.

| ID | EventDate | EventName | SP | DP | DP Name | SIP | DIP | Kill |
|---|---|---|---|---|---|---|---|---|
| 52096 | 8/14/01 8:52:47 PM | SYNFlood | 0 | 80 | HTTP | 0.0.0.0 | 10.49.104.20 | Yes |
| 52096 | 8/14/01 8:52:47 PM | SYNFlood | 0 | 80 | HTTP | 0.0.0.0 | 10.203.11.107 | Yes |
| 52096 | 8/14/01 8:52:47 PM | SYNFlood | 0 | 80 | HTTP | 0.0.0.0 | 10.178.125.48 | Yes |
| 52096 | 8/14/01 8:52:47 PM | SYNFlood | 0 | 80 | HTTP | 0.0.0.0 | 10.4.248.137 | Yes |
| 52096 | 8/14/01 8:52:47 PM | SYNFlood | 0 | 80 | HTTP | 0.0.0.0 | 10.118.83.12 | Yes |
| 52096 | 8/14/01 8:52:47 PM | SYNFlood | 0 | 80 | HTTP | 0.0.0.0 | 10.155.127.20 | Yes |
| 52096 | 8/14/01 8:52:47 PM | SYNFlood | 0 | 80 | HTTP | 0.0.0.0 | 10.115.4.77 | Yes |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| 52096 | 8/14/01 8:52:47 PM | SYNFlood | 0 | 80 | HTTP | 0.0.0.0 | 10.194.69.58 | Yes |
| 52096 | 8/14/01 8:52:47 PM | SYNFlood | 0 | 80 | HTTP | 0.0.0.0 | 10.56.240.82 | Yes |
| 52097 | 8/14/01 8:52:47 PM | SYNFlood | 0 | 80 | HTTP | 0.0.0.0 | 65.238.90.219 | Yes |
| 52097 | 8/14/01 8:52:47 PM | SYNFlood | 0 | 80 | HTTP | 0.0.0.0 | 10.64.60.55 | Yes |

**Containment**

Since the decision was made to contain and remove the malicious code as promptly as possible, my manager instructed a thorough inspection of all the server logs and Windows 2000 machines in that location.

At 8:51 PM EDT the West Coast IT manager directed all server personnel to remain onsite until further notice and to begin analyzing the logs to develop a list of possible infected servers. Upon discovery of infected servers or traces of the worm in the log all server personnel were instructed to promptly disconnect the servers from the network until they could be promptly tested.

At 9:15 PM EDT the Information Assurance manager located a tool on the Symantec web site that scans for Code Red and Code Red II. She downloaded the FixCRed.exe tool and checked the digital signature to verify the tool had not been adjusted and then she forwarded the tool and instructions to the West Coast via email. Once he received the tool, he promptly distributed it to his staff and server administrators at that location. All of the administrators scanned their servers and PCs using the FixCRed.exe tool in an effort to verify infection and eradicate the worm.

This tool scans for the worm and then eradicates it if it is found in the system. Once the tool is finished running on Windows servers, a message is displayed indicating if the server is infected with the Trojan.VirtualRoot or Code Red worm and any variants. An additional message is displayed stating whether or not the server is vulnerable to reinfection of the worm. (Ferrie and Sevcenco, 2001)

This tool performs the following steps according to Symantec:(taken directly from Symantec documentation)

1. It scans memory for the presence of all known Code Red variants.
2. It performs a vulnerability assessment of the computer. If the computer is vulnerable, the tool opens the Web browser and loads the Microsoft page that contains the patch.
3. It attempts to terminate the Code Red and Trojan.VirtualRoot processes.
4. It scans and deletes the Trojan.VirtualRoot files dropped by Code Red II.
5. It removes the IIS mappings for /Scripts or /MSADC and restores the System File Checker.
6. It deletes the following four files, if they exist:

C:\inetpub\Scripts\Root.exe
D:\inetpub\Scripts\Root.exe
C:\progra~1\Common~1\System\MSADC\Root.exe
D:\progra~1\Common~1\System\MSADC\Root.exe

7. It detects and automatically removes the open shares created by the Trojan.VirtualRoot.
8. It deletes the values /MSADC and /Scripts from the registry to prevent them from being placed in the IIS Metabase if they did not exist already. If these values existed already, then the deletion is harmless, because IIS will restore the default values.
9. It logs its activity in the file FixCRed.log. This file is stored in the same folder as the tool.

Administrator-level privileges are required to unmap the virtual roots created by Code Red. (Ferrie and Sevcenco, 2001)

At 11:21 PM EDT a list of the infected servers were compiled and 140 servers were identified as potentially vulnerable. My manager and other members of our organization used the list of potentially vulnerable machines to monitor the spread of the worm. By that time, the Enterprise NT/2000 manager had been located and he instructed his staff to begin scanning potentially vulnerable enterprise servers in effort to determine that the worm had been appropriately contained.

**Eradication**

On Wednesday August 15, 2001 in the early morning the results of the scan of this location and the enterprise servers was reported to the SIAC. Nineteen machines were identified as infected. All nineteen instances of the Code Red II variant were removed using the Symantec FixCRed.exe tool. Once the Symantec tool removed the worm, the machine was rescanned to see if any traces of the worm still existed. Upon a positive result of the scan the infected machine was reconnected to the network and the server administrators continued to monitor the logs for an unusual activity.

**Recovery**

On Wednesday morning my manager called a meeting of all the SIAC members and high level networking and server personnel throughout the corporation. During this meeting the incident was described in full detail with several main points outlined. The lead incident handler reinforced these aspects of our Incident Response procedure:

1) Everyone must remain calm
2) Any requests for information from the media must be forwarded to the SIAC.
3) The infection has been identified as the Code Red II worm.
4) The team must stay focused
5) The SIAC will be the interface to the corporate Security, Legal, and Communications organizations.

These steps were the objectives she covered during our meeting, informing all members of the incident as well as the possible threat of additional infections. On the second point of interest regarding media, it is our company's policy not to discuss such events with the media. However, a press release was developed and forwarded to the Corporate Communications Department to be used if word leaked to the press:

.

"*On August 14th, XYZ Company experienced a small outbreak of the Code Red II worm. Insuring that every networked workstation is proactively protected is a challenge for large corporations. A single unpatched server can allow the introduction of opportunistic malevolent program code into our networks. The XYZ Company's Internal Information Services was able to locate the infected workstation, contain the spread of the worm and rectify the underlying problem." (Internal Company document)*

The third area highlighted was to inform the team that if we discover that we have been both targeted and deliberately breached by an intruder, the SIAC will contact the FBI or other law enforcement agencies. In order to involve the FBI, we would have to prove that we had suffered a monetary loss of greater than $1000. . Therefore, all members involved were informed to note all time spent on this investigation as "CODERD" on their time sheets.

The outcome of this meeting was several action items for all individuals involved to help ensure that all occurrences of the worm were removed.

After the meeting, a member of the SIAC team launched a Code Red II check via a popular vulnerability scanner and began scanning all machines IIS servers and Windows 2000 machines throughout our corporation.

In addition to running the vulnerability scanner to check for the presence of Code Red II, I launched the vulnerability scanner on the small information technology group where the first occurrence of Code Red II was discovered to evaluate the vulnerabilities on their workstations. This area of the network had not been scanned previously. The vulnerability scanner reported a few issues that needed to be resolved in the small group; however, there was no discovery in either scans of any other instances of the Code Red II worm.

**Summary**

On Tuesday August 14, 2001, our corporation fell victim to an infection of Code Red II. A Windows 2000 machine installed with the standard defaults and a modem provided a path for the malicious code to self-propagate within our network. The worm was identified initially by the IDS manager in my organization due to the increased HTTP requests from one location. The increased Synflood traffic was a direct result of the random number generator of the worm propagating throughout our network and attempting to connect to external machines. However, due to the increased traffic firewall administrators thought that there was a firewall problem and they disconnected the Internet pipe at the infected location.

In the early evening hours of the 14th my organization was contacted and an outbreak of Code Red II was reported at one of our locations. The malicious code took approximately 24 hours to be discovered and eradicated from our network with nineteen hosts infected. Fortunately in our situation the worm's random number generator was the downfall of the worm because as the worm attempted to spread to external networks, the worm created a Denial of Service attack on the network firewall. The denial of service attack created a situation, which led the firewall administrator to disconnect the firewall and the Internet pipe at this location. The Internet outage produced minimal effect on our business communications on that particular day and overall I would interpret the damage of the worm to be minimal.

## Lessons Learned

### Areas for Improvements

#### Cyber Incident Response Team

One of the main areas of improvement is the establishment of a Cyber Incident Response Team to include a representative member from each site location. Although we currently have a SIAC team to help assist with incidents, the establishment of a formalized team like the incident handling teams discussed at SANS is required to successfully contain and control any incidents that occur in our organization. This formalized team would have an established protocol and procedures for escalation of an event as well as maintaining up to date contact information for all team members and backups. During this particular event, the inability to contact the Enterprise NT/2000 manager only cost our team minimal time delay. If this incident had involved a more malicious worm or other attack, the delay of a few minutes could have meant the difference of thousands of dollars in lost revenue due to business disruption.

#### Security Training

Another area for improvement is the establishment of an information security training class to educate all of our system administrators on the need and importance of securing the servers they administer and identifying possible incidents. System administrators need to regularly review their logs for potential security threats as well as consider security incidents when diagnosing networking and firewall problems. In this case, we believe the firewall problems were a direct result of Code Red II. The network engineer was not familiar with the symptoms of a Denial of Service attack and erroneously assumed that the problem was a hardware failure. Although taking down the firewall helped reduce the threat of spreading the worm through our network to external connections, we could have contained the situation much sooner if the network engineers had identified the presence of Code Red II earlier on the 14th.

IDS

Our IDS manager believed the network engineer's assertion that the numerous alerts being seen were false positives. Knowing that the firewall was having problems, he should have recognized the possible relationship between the firewall situation and a Denial of Service attack.

Remote Access Security

Information Assurance has been stressing the need for personal firewalls on all remote access machines whether personal or corporate. This event enabled management to better understand how a single vulnerability can lead to the infection of our entire internal network and gotten us senior management's backing for this policy.

IDS Update Process

The current IDS procedure is to update our sensors on a monthly basis with releases from the vendor. However, as a result of this instance we have to have the knowledge and the ability to create custom signatures on the fly as new threats are announced to the security community. If the custom signatures had been in place in this instance, quicker identification of the worm may have occurred. As in any incident, prompt response is required to minimize the amount of damage incurred.

Network Device Identification

The current process of computer registration needs to be updated and improved to make sure that all systems are accurately accounted and the system administrators are identified. The lack of documentation in the case of the department that was initially infected prolonged the process of response and disconnection of the infected system from the network, enabling the worm to self-propagate throughout our network.

## Strengths

Incident Handling Process

Although our incident handling process was created over a year ago this high level document covered all the issues faced by the incident handlers and provided the guidance required for all the members involved. Having a lead incident handler with over 10 years of experience handling this incident provided the appropriate leadership and control required to promptly and efficiently eradicate the worm from our network.

Security Monitoring

Even though our IDS update procedure had some weaknesses, this incident showed the value of human intervention when working with intrusion detection. The ability of our IDS manager to promptly recognize the unusual traffic from this location displays the

critical nature of hiring educated security personnel to monitor perimeter and critical servers.

## Additional Outcomes

As a result of the spread of Code Red II on August 14, 2001, many issues and action items have been identified by our organization as areas for improvement. Management has become more aware of the critical need for more enhanced IDS and security perimeter monitoring devices to help reduce the number of infections and minimize the damage occurred. Senior management has also realized that our company will continue to see malicious worms and virus attacks that could potentially disrupt business transactions and cost the organization thousands to millions of dollars in future revenues. The infection of Code Red II and several other events has led senior management to recognize the need for strengthened security procedures and a more educated information technology staff. Since this infection, the Vice President has made security a priority for the upcoming fiscal year and is willing to increase the security monitoring presence ten fold.

In addition to the increased security monitoring of devices, management has approved the implementation of intrusion detection sensors on second layer perimeters and customer connections to insure that all points of connection into our network are being monitored. Management also recognizes the need for addition security personnel at various site locations and has approved the hiring of several more security engineers who will be deployed throughout the organization. Although this will not provide onsite personnel at every location, this action is definitely a step in the appropriate direction.

Viruses and other malicious code outbreaks can cost a company millions of dollars for a single instance. Resources become unavailable, data may be lost, and project and proposal deadlines may be missed due to the need to contain an incident. It is critical to insure that all personnel who may need to address such an issue are properly training in the identification and containment of security-relevant events to minimize downtime to the corporation.

## References

CERT Coordination Center. (September, 2001) CERT Advisory CA-2001-26 Nimda Worm. [www document]. http://www.cert.org/advisories/CA-2001-26.html. Carnegie Mellon University. September 2001.

CERT Coordination Center. (August, 2001) CERT Incident Note IN-2001-09. [www document]. http://www.cert.org/incident_notes/IN-2001-09.html. Carnegie Mellon University. August 2001.

Chien, E. (July, 2001). CodeRed Worm. [www document]. http://www.symantec.com/avcenter/venc/data/pf/codered.worm.html

Ferrie, P. and Sevcenco, S. (September, 2001). CodeRed Removal Tool. [www document]. http://www.symantec.com/avcenter/venc/data/pf/codered.removal.tool.html

ISS Xforce Database. (September, 2001) Code Blue Worm. [www document]. http://xforce.iss.net/alerts/advise96.php

ISS Xforce Database. (August, 2001) Resurgence of "Code Red" Worm Derivatives. [www document]. http://xforce.iss.net/alerts/advise90.php

Microsoft.com (September, 2001). Microsoft Download Center. [www document]. http://www.microsoft.com/downloads/search.asp

Network ICE (September, 2001). Code Red II. [www document]. http://advice.networkice.com/advice/intrusions/2004602/default.htm

SANS (July, 2001). 4.1 Incident Handling: Step-by-Step and Computer Crime Investigation. SANS Institute. July 2001.