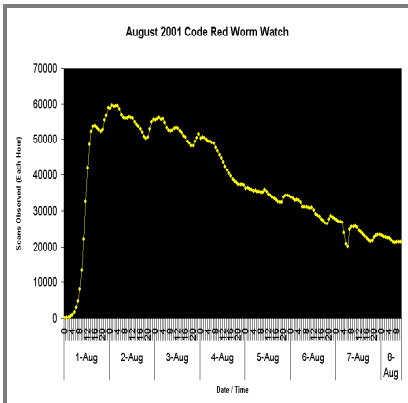
Global Information Assurance Certification Paper

GIAC GSEC

PRACTICAL ASSIGNMENT FOR SANS
GSEC VERSION 1.2E
CODE RED WORM INVASION

Prepared by
Sharon Bristow

TABLE OF CONTENTS

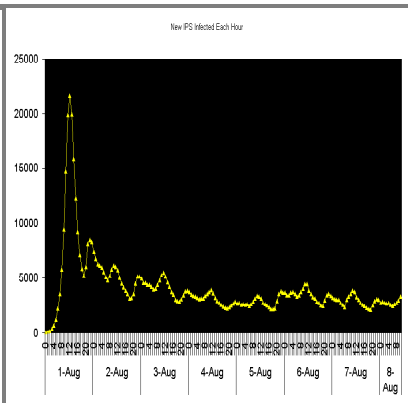


[Scans Observed Each Hour]

Number of Unique Source IP Addresses

Last Round
July 31st
Since Aug. 1st

280,391
124
661,044*



[New IP Addresses Scanning Each Hour (not new machines)]

Time (EDT)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10	10-11	11-12p	12p-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10	10-11	11-00
Aug 1	76	157	252	495	893	1591	2881	4792	8007	13487	22001	32502	41968	48489	52273	53643	53917	53332	52713	52167	52816	55509	56661	58814
Aug 2	58740	59517	59181	59336	59387	58573	56869	56226	56015	55919	56327	56132	56055	54885	54245	53708	53022	51968	50882	50304	50672	52961	55005	55642
Aug 3	55437	55738	56266	55617	55786	54721	53262	52603	52471	52673	53177	53372	53211	52355	51822	51037	50680	49321	48808	48105	48130	49309	50428	51426
Aug 4	50209	50617	50470	49854	49388	49403	48972	48816	47650	46698	45540	44748	43598	42311	41358	40417	39629	38725	38187	37947	37340	37386	37394	37112
Aug 5	36276	36456	36005	35842	35619	35694	35345	35306	35182	35182	35827	35303	34636	34310	33735	33298	33112	32531	32245	32375	33683	34280	34264	34037
Aug 6	33745	33366	32915	33083	32863	32267	31099	30992	30978	30857	30755	30806	30126	20934	28753	28293	27562	27303	26515	26380	27593	28462	28252	27800
Aug 7	27374	27145	26903	26782	23895	20736	20045	24792	25466	25520	25739	25339	24401	23968	23458	23018	22509	21867	21599	21716	22560	23084	23268	23268
Aug 8	23107	22832	22642	22352	22501	21963	21386	21116	21320	21335	21434													

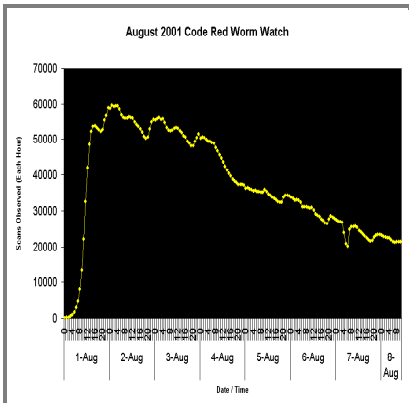
Introduction

A malicious worm has once again threatened our technological environment. The Code Red worm has broken down our security by attacking Microsoft's Internet Information Services tool. IIS is a network file and application server that transmits information in Hypertext Markup Language. IIS is used to connect client users to the Internet. The Internet has become an important tool for businesses and home users but it has also become a target for abuse and destruction. The Code Red worm is the latest attack that reminds us that security maintenance is crucial for our systems. Hackers are always going to look for opportunities to attack.

Origin and Infection Dates

Many believed that the Code Red worm was initiated at a university in GuangDong, China but studies show that there is no clear evidence to substantiate this claim. A study

compiled by Dshield.org, an intrusion detection system, claims that the Code Red worm hit the United States and other countries before it made its way to the server at Guangdong. The worm, which was discovered by the eEye Digital Security organization

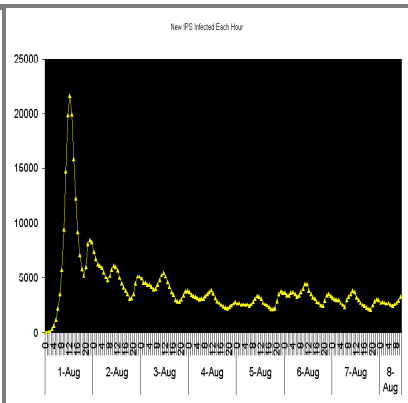


Scans Observed Each Hour

Number of Unique Source IP Addresses

Last Round
July 31st
Since Aug. 1st

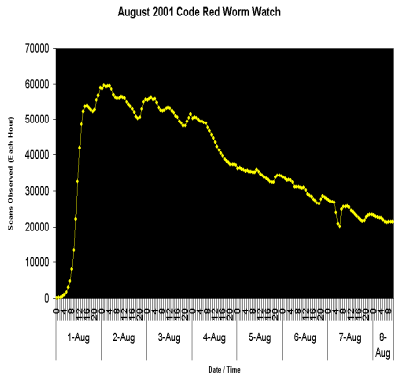
280,391
124
661,044*



New IP Addresses Scanning Each Hour (not new machines)

Time (EDT)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10	10-11	11-12p	12p-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10	10-11	11-00
Aug 1	76	157	252	495	893	1591	2881	4792	8007	13487	22001	32502	41968	48489	52273	53643	53917	53332	52713	52167	52816	55509	56661	58814
Aug 2	58740	59517	59181	59336	59387	58573	56869	56226	56015	55919	56327	56132	56055	54885	54245	53708	53022	51968	50882	50304	50672	52961	55005	55642
Aug 3	55437	55738	56266	55617	55786	54721	53262	52603	52471	52673	53177	53372	53211	52355	51822	51037	50680	49321	48808	48105	48130	49309	50428	51426
Aug 4	50209	50617	50470	49854	49388	49403	48972	48816	47650	46698	45540	44748	43598	42311	41358	40417	39629	38725	38187	37947	37340	37386	37394	37112
Aug 5	36276	36456	36005	35842	35619	35694	35345	35306	35182	35182	35827	35303	34636	34310	33735	33298	33112	32531	32245	32375	33683	34280	34264	34037
Aug 6	33745	33366	32915	33083	32863	32267	31099	30992	30978	30857	30755	30806	30126	20934	28753	28293	27562	27303	26515	26380	27593	28462	28252	27800
Aug 7	27374	27145	26903	26782	23895	20736	20045	24792	25466	25520	25739	25339	24401	23968	23458	23018	22509	21867	21599	21716	22560	23084	23268	23268
Aug 8	23107	22832	22642	22352	22501	21963	21386	21116	21320	21335	21434													

based in California, got its name from a Mountain Dew soda. Other names for it include W32/Bady, I-Worm Bady, and W32/Bady.worm. It was discovered on July 17, 2001 and infection began on July 19, 2001. It causes a denial of service security attack on the Internet. It was also designed to slow or shut down a computer system by flooding it with large amounts of data. From the 1st of the month to the 19th, the infected hosts attempt to connect to port 80 and propagate the worm. It starts spreading itself between the 20th and 27th of each month, and then it starts an attack against a specific address that was assigned to the White House. From Day 28 through the end of the month, the worm will not have any activity. The worm infected over 300,000 servers on the first day.

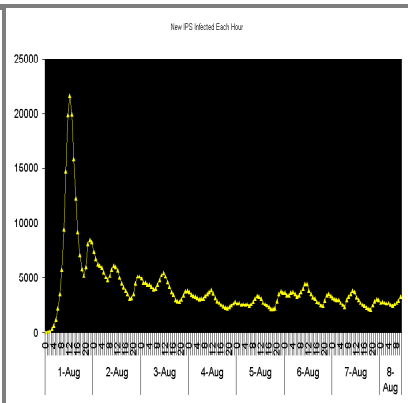


[Scans Observed Each Hour](#)

Number of Unique Source IP Addresses

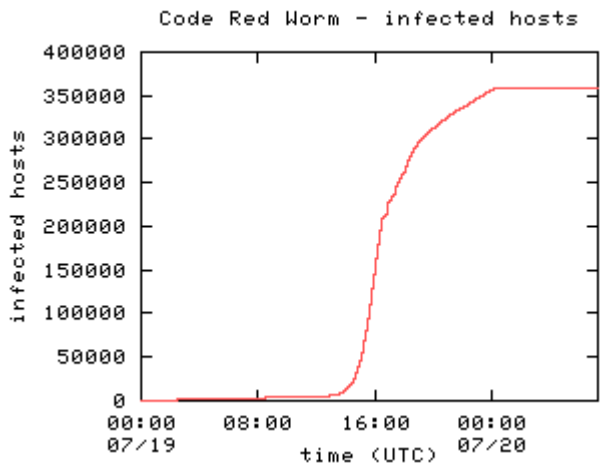
Last Round
July 31st
Since Aug. 1st

280,391
124
661,044*



[New IP Addresses Scanning Each Hour (not new machines)](#)

Time (EDT)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10	10-11	11-12p	12p-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10	10-11	11-00
Aug 1	76	157	252	495	893	1591	2881	4792	8007	13487	22001	32502	41968	48489	52273	53643	53917	53332	52713	52167	52816	55509	56661	58814
Aug 2	58740	59517	59181	59336	59387	58573	56869	56226	56015	55919	56327	56132	56055	54885	54245	53708	53022	51968	50882	50304	50672	52961	55005	55642
Aug 3	55437	55738	56266	55617	55786	54721	53262	52603	52471	52673	53177	53372	53211	52355	51822	51037	50680	49321	48808	48105	48130	49309	50428	51426
Aug 4	50209	50617	50470	49854	49388	49403	48972	48816	47650	46698	45540	44748	43598	42311	41358	40417	39629	38725	38187	37947	37340	37386	37394	37112
Aug 5	36276	36456	36005	35842	35619	35694	35345	35306	35182	35182	35827	35303	34636	34310	33735	33298	33112	32531	32245	32375	33683	34280	34264	34037
Aug 6	33745	33366	32915	33083	32863	32267	31099	30992	30978	30857	30755	30806	30126	20934	28753	28293	27562	27303	26515	26380	27593	28462	28252	27800
Aug 7	27374	27145	26903	26782	23895	20736	20045	24792	25466	25520	25739	25339	24401	23968	23458	23018	22509	21867	21599	21716	22560	23084	23268	23268
Aug 8	23107	22832	22642	22352	22501	21963	21386	21116	21320	21335	21434													



Graph According to CAIDA

Code Red Status

The data supplied by the SANS Internet Storm Center, the Early Warning System for Large Internet Attacks. (This data was supplied by Digital Island).

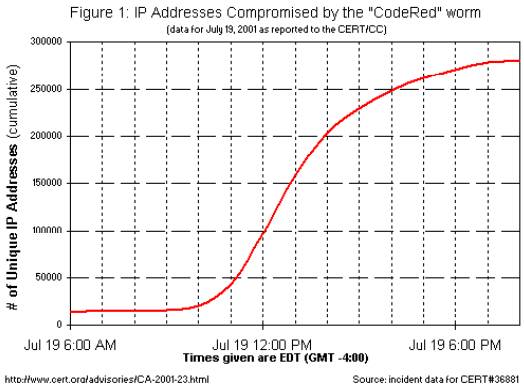
Last update: 8/8/2001 1600 GMT / 12:00pm US/EDT

How the Attack Works

The worm spreads by attacking random IP addresses and infecting all hosts with the IIS vulnerability. The vulnerability is an indexing service ida.dll buffer overflow problem, which causes a denial of service. This DLL is used to support the .ida and .idq files. There are two variations of the Code Red I worm. One uses a fixed static IP address targeted toward the White House and the other uses random IP's. The Code Red worm exploits the Microsoft IIS vulnerability by transferring a Uniform Resource Identifier (URI) to the TCP port 80, which is usually the default port for HTTP service. A URI is a set of characters that identifies a resource such as a file from anywhere on the Internet. It includes Uniform Resource Names, which identifies Internet resources by name, and Uniform Resources Locators, which are used as a linking mechanism between Web pages. A port number is used to identify a connection point to a specific Internet protocol. The URI causes the infected host to either scans other random IP addresses, passing it on to other systems that it may find along its path, or attacks the IP address 198.137.240.91. This IP address belonged to the www.whitehouse.gov web site. When the virus is received by a computer system the following message appears: **"HELLO! Welcome to HTTP://www.worm.com! Hacked By Chinese!"** This comment, of course, had analysts suspecting China of the attack, but it also could have been someone blaming the Chinese or someone trying to disguise the original identity. It affects machines with a default language of English. The United States was one of the major countries affected by the virus. Korea, China and Taiwan were also some of the countries infected by the virus. The Code Red worm is such a large threat to the computer world that there is a joint effort between Microsoft, The National Infrastructure Protection Center, Federal Computer Incident Response Center, Information Technology Association of America, Cert Coordination Center, SANS Institute, Internet Security Systems, and Internet Security Alliance to try and contain this attack.

Cert Graph of Infection Rate on July 19, 2001

Data reported to the CERT/CC indicates that the "Code Red" worm infected more than 250,000 systems in just 9 hours.



White House Response to Code Red

As mentioned earlier, there was a direct attack from the Code Red worm to hit the IP address of the White House. The White House simply switched IP addresses to avoid infection. Many Internet Service Providers are black-holing that address as well. Black-holing is discarding packets addressed to a specific IP address. Therefore when the Code Red worm tries to hit it will not do any damage.

Systems at Risk

The media coverage on this worm has been enormous causing a lot of computer users to panic. However, the worm doesn't affect workstations. Servers with Windows NT and Windows 2000 with IIS 4.0 or later could be the systems with the greatest vulnerability. Network devices that work with the IIS server may be affected by the worm as well. Cisco 600 series DSL Routers, Cisco 675 modems, and Cisco CSS 11000 series Content Service Switches maybe infected by Code Red. Also systems not running IIS but using HTTP, listening on TCP port 80 maybe infected such as the HP 4000 printers. The Cisco 600 series processes the HTTP requests. The worm problem results in the router not forwarding information properly. Patches for the Cisco router issues can be found at http://www.cisco.com/warp/public/707/cisco-code-red-worm-ub.shtml. The Cisco 675 modem assigns DHCP clients on the local area network. It uses IP addresses outside the range that is suppose to be used on the inside LAN. This causes a denial of service on the Internet. This problem is resolved by shutting the modem down and back up. You can also receive a CBOS upgrade directly from Cisco to resolve some of the issues. The HP Jetdirect Card J3111 is another victim of the virus. This software was shipped with the HP 4000 series LaserJet Printers. When scanned by the worm it will come up with an "EIO2" error message when the printer is reset. You have to turn the printer on and off to correct the problem or upgrade the Firmware to version G.08.32. The worm hits the network port of the printer's Jetdirect Card. The card thinks that it has the General Results of the First Code Red Worm Attack print job and does not know how to interpret the data causing

errors to occur. Another problem occurred with the freeware web server Quid Pro Quo 1.0.2. Code Red requests the default.ida file used by this software. This causes the QPP 1.0.2 to show errors. This is due to a buffer overflow problem. There is a plug in available to reject default.ida requests. It is called "Code Red Killer". It can be found on the web page http://www.macintouch.com/codered.html. Cayman Gator boxes appear to have a problem too. The worm overloads the system and either causes it to crash or causes it to go up and down.

General Results of the First Code Red Attack

The Code Red worm results in a decrease of the speed on the Internet and may even cause outages on all types of systems. A computer user may experience difficulty accessing certain web pages or ISP providers. It certainly has the potential to disrupt activity such as e-mail and electronic commerce. It should affect very few home computers itself. It does not affect computers with Windows 95, 98 or ME, and only affects Windows NT or Windows 2000 systems that are running the IIS.

Detection and fixes for the Worm

The Code Red I worm can't be detected by using any anti-virus software because it is not found on the hard drive. It only resides in memory. To get rid of it, all you have to do is reboot the computer. To prevent the worm from attacking your server again, you need to install a patch. This patch provides a fix for the Microsoft IIS vulnerability. The first patch that Microsoft made available was Bulletin MS-01-033. Several companies including Microsoft and Cisco are providing the patch for free. For Windows NT 4.0, you can find the patch at Microsoft web page at http://microsoft.com/downloads/release.asp?releaseID=30833 or for Windows 2000 under http://www.microsoft.com/downloads/release.asp?releaseid=30800. As a precaution, all administrators should check the servers to verify if IIS has or has not been installed on their systems. You may not be using IIS but it is installed by default on a Windows 2000 Server System. It should be disabled if it is not in use. To disable the IIS on a Windows 2000 server, access "Add/Remove Programs" from Control Panel. Choose "Add/Remove Windows Components" and deselect the check box under Internet Information Services. Follow the rest of the instruction to complete the uninstall process.

Some say that the first Code Red worm was actually flawed. It uses the same seed address by using the same IP addresses over and over again, therefore attacking the same systems over and over again. The second Code Red attack began in August 2001 but it was a different virus all together. It is a more dangerous worm. It is not the same as the first Code Red worm. It affects the Windows 2000 Web server the same as the first Code Red Code worm but it affects the Windows NT 4.0 web server differently. On the first worm, it infected the system and spreads but with the second worm the process will crash. The Code Red II worm contains more of a fixed randomizer that will attempt all possible IP addresses except those that begin with the 127 or 224 octet. (An octet is an Internet term for a unit of data containing exactly eight bits.) It also does not change the default web page and it does not try to use the old www.whitehouse.gov IP address. Code Red II drops a Trojan horse program too. This Trojan allows hackers to have remote access to the Web server. Antivirus software such as Norton, with updated definitions, can detect the Code Red II worm on a Web server by detecting the Trojan component of this worm. According to eEye Digital security, you can check to see if your system has been infected or not by looking for the existence of the file explorer.exe on the root of your hard drive or the root.exe file usually found in C:/Inetpub/scripsts/root.exe on your hard drive. You also know you have this worm by a string in the IIS log files. The string found is the following:

```
GET /default.ida?XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXX%u9090%u6858%ucbd3%u7801%u9090%u6858%ucbd3%u7801%
u9090%u6858%ucbd3%u7801%u9090%u9090%u8190%u00c3%u0003%u8b0
0%u531b%u53ff%u0078%u0000%u00=a
```

This log file indicates that the Code Red II worm attempted to infect the machine but does not mean that it caused a problem.

How Code Red II Works

The Code Red II worm leaves a "backdoor" open on the infected computer. This "backdoor" creates a pathway for attackers. This gives the attacker read/write access to the system as well as the ability to reboot the box and install any software he or she chooses, said Russ Cooper, "surgeon general" of TruSecure Corp., in Reston, VA. Instead of scanning the entire Internet at random for new machines to infect, the new worm first scans those machines on its current network, which Levy says gives it a greater chance of finding vulnerable machines. A system that is compromised by the Code Red II worm may have files destroyed or altered. It may also cause bandwidth denial of service problems in isolated parts of the network.

Qwest Digital Subscriber's Code Red Problem

There is a company in Minnesota, who is blaming the Code Red II worm for knocking out their Internet access. As a side effect of the virus, it mistakes Qwest digital subscriber line

modems for Web servers and disables them. The modem will assign DHCP clients on the local area network IP addresses. These IP addresses should be used for clients internally. This issue causes a denial of service to the Internet for these clients. To fix the problem, power off the modem and bring it backup. To permanently fix the problem, disable the web service on the modem.

Latest Patch for IIS Vulnerability

A new security patch came out in August 2001 for the NT 4.0 with SP5 and greater or Windows 2000 original release. This patch should be applied to systems running personal web servers and outlook web. It is Bulletin number MS01-044. It addresses five new vulnerabilities and three of the denial of service issues that the MS01-033 patch did not address. The newest patch can be found at http://www.microsoft.com/technet/security/bulletin/MS01-044.asp When the Code Red worm infects an IIS 4.0 computer, the W3SVC (web service) service fails. When the MS01-033 is applied, this should not occur, the service should continue to operate despite Code Red attacks. However, if the IIS4.0 box has configured a web site to perform URL redirections such as an IP addressed web site, Code Red attacks that IP address causing the W3SVC service to fail. The MS01-033 patch does not prevent this attack from happening. Many speculate that that this problem is a result of the MS01-033 patch. Microsoft claim that this is not true but they offer a fix for this vulnerability. There are other web sites available that you can use to download service packs and patches: Some of these sites are:http://www.microsoft.com/windows2000/, http://www.microsoft.com/ntserver/, http://microsoft.com/technet/security/current.asp, and http://microsoft.com/technet/security/tools.asp.

Security Tools for Code Red

Code Red Cleanup

Microsoft released several new tools designed to aid administrators with the problems that occurred during the Code Red outbreak. One of the tools eliminates malicious files and "mappings" from the Code Red worm once attack has been made. It is called "Code Red Cleanup". It offers the option of permanently disabling IIS software and it reboots your machine to get rid of the virus. The tool does not install the Microsoft patch that protects your machine from becoming infected. It also does not protect against any malicious codes from Code Red II. This tool is available free from Microsoft and may be found on the web at http:/www.Microsoft.com/technet/itsolutions/security/tools/redfix.asp.

IIS Lockdown Tool

There is another security tool from Microsoft called "IIS Lockdown tool". It is used to protect web servers against threats such as the Code Red Worm. This tool allows users to choose the features they want enabled or disabled but the tool doesn't allow users to shut down the File Transfer Protocol and Simple Mail Transfer Protocol services that are

installed by default on IIS servers. It addresses both IIS 4.0 and 5.0 web servers. Two modes are available for the "IIS Lockdown tool". The Express Lockdown automatically chooses secure options for your server. The Advanced Lockdown mode allows you to pick and choose the options that you need for your system. This option helps address vulnerabilities with printing and scripting by automatically configuring web servers to provide only the services that are needed by your system. This reduces the accessibility for viruses and worms to attack your machine. This tool is available free from Microsoft at http://www.microsoft.com/technet/treeview/default.asp?url=/technet/itssolutions/security/tools/locktool/asp

HFNETCHK and MPSA Checker

Microsoft and Shavlik Technologies LLC worked together to come out with a network security hotfix checker called HFNETCHK. It is a checker that will allow business users of the company's software to assess the status of security patches for the Windows NT and Windows 2000 operating systems. It will also check for fixes of the Internet Information Server 4.0 and 5.0, SQL Server 7.0 and SQL server 2000, and Internet Explorer 5.01 and later. The tool scans the machines on the network to see if they have the latest security patches and a report is generated giving you a list of patches that is needed on your machine. There is a home-based checker called Microsoft Personal Security Advisor (MPSA) application. The Microsoft Personal Security Advisor (MPSA) tool is used for home computers that would like to check their computers for patches. This tool will allow users to scan Windows NT 4.0 and Windows 2000 operating systems. It will give you a report on their computers' security and how to improve on it. The report will give you information on missing security patches, weak passwords, Internet Explorer, Outlook express security settings, and office protection settings. Microsoft has been criticized for not having protection for Internet servers and software. They are trying to put these tools out to help and protect your system

Code Red Removal Tool

The Code Red Removal Tool removes all variants of the Code Red worm and checks the computer for other security vulnerabilities. This tool called FixCRed.exe and can be found under http://www.sarc.com/avcenter/FixCRed.exe.
This tool scans for the worm and removes the Trojan.VirtualRoot and Root.exe files from all Windows environments. The tool will actually access the Microsoft page that contains the patches if it finds a problem. All activity is logged to a log file called FixCRed.log.

FixCodeRed Assessment Tool

Symantec has come up with its own tool to determine if your equipment is at risk. It is called the FixCodeRed Assessment Tool and it can be found at http://security2.norton.com/us/crdetect.asp?venid=sym&langid=us&plfid=00&pkj=PLYIGMKIIPLBMRSJRFS. The executable file is called CRDetect.exe and it can be used for the

home or office.

The Cost of Code Red

The cost of the Code Red worm has totaled over $1 billion so far. Stephen Northcutt, a director of the SANS institute, points out several things about the future of our technology in Computer World magazine. Mr. Northcutt stated ".. The original Code Red worm was not that big of a deal. But a slightly smarter attack code will be capable of doing significant harm, to the point where we could lose connectivity in parts of the Internet. It could be a day or two before we recover, and that's a whole lot of downtime if you're Amazon.com". When asked about prosecuting attackers, he stated" I think we'd better start right now, because the cost of hacking in nearly 100% free, It's a criminal act. If they succeed and do harm, then you've lost a lot of money, prestige, and revenue."

Conclusion

Security Maintenance is essential to your organization. With all of the patches and tools available for Code Red, there is no reason to be infected by the variants that are currently out there on the Internet. We need to understand that there will always be vulnerabilities and we need to do the best that we can to try and eliminate as many as possible. Our industry needs to always look for weaknesses, fix the problems, cure the infections, and try to prevent them. For Code Red, add all of your patches and your security tools, but don't get a false sense of security from it. There will be a bigger worm out their next to create more destruction. Code Red is just a good example of attackers taking advantage of vulnerabilities.

REFERENCES

USA Today, www.usatoday.com/life/cyber/tech/2001-08-01-code-red-costs.htm

Computing and Technology, www.antivirus.about.com/library/weekly/aa072001a.htm

Cert Coordination Center, www.cert.org/advisories/CA-2001-19.html

Digital Island, www.digitalisland.net/codered/

ZDNet, www.zdnet.com/zdhelp/stories/main/0,5594,2799820,00.html

ZDNet, www.zdnet.com/zdnn/stories/comment/0,5859,2800509,00.html

EEye Digital Security, www.eeye.com/html/research/advisories/AL20010804.html

Computer World, www.computerworld.com/cwi/story/0,1199,nav47_sto63434,00.html

Cisco, www.cisco.com/warp/public/707/cisco-code-red-worm-pub.shtml

MacInTouch, www.macintouch.com/codered.html

Cert Coordination Center, www.cert.org/advisories/CA-2001-23.html

Cert Coordination Center, www.cert.org/incident_notes/IN-2001-10.html

Computer World, www.computerworld.com/cwi/story/0,1199,nav65-663_sto63310,00.html

ZDNet.com, www.zdnet.com/eweek/stories/general/0,11011,2801821.,00.html

Symantec, www.symantec.com/avcenter/venc/data/codered.removal.tool.html

Symantec, www.symantec.com/avcenter/venc/data/trojan.virtualroot.html

CAIDA, www.caida.org/analysis/security/code-red

Symantec, www.Symantec.com/avcenter/venc/data/codered.worm.html