Interested in learning more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Defending Against Code Red II Using Symantec NetProwler and Intruder Alert, ddos

Today we are under attack from Code Red II. This worm has cost an estimated 2 billion dollars according to Computer Economics. Hotmail and FedEx have reported infections that cause shut down of some servers. Microsoft stated that at Hotmail no personal information was released, but how do they know? Did Microsoft use IDS, Intrusion Detection System, that tracked the activities that the worm performed? If they did use a IDS, why did they not catch the attack or the compromise of the WEB server? In this paper I will addr...

Copyright SANS Institute
Author Retains Full Rights

AD

Defending against Code Red II using Symantec NetProwler and Intruder Alert.

Kenneth Donze
August 15, 2001

Introduction

Today we are under attack from Code Red II. This worm has cost an estimated 2 billion dollars according to Computer Economics. Hotmail and FedEx have reported infections that cause shut down of some servers. Microsoft stated that at Hotmail no personal information was released, but how do they know? Did Microsoft use IDS, Intrusion Detection System, that tracked the activities that the worm performed? If they did use a IDS, why did they not catch the attack or the compromise of the WEB server? In this paper I will address the use of Symantec's NetProwler, network based IDS (NIDS), and Intruder Alert, host based IDS (HIDS), to detect and react to the Code Red II worm.

Details of Code Red II

Code Red II, also known as CodeRed.v3, CodeRed.C, CodeRed III, W32.Bady.C, is a variant of Code Red. Code Red is a Trojan that was designed to perform a Denial-of-Service attack on Whitehouse.gov. The means of entry into IIS is a buffer overflow exploit in Microsoft IIS Index Server, which is by default installed with every IIS installation. The exploit is with an Unchecked Buffer in Index Server ISAPI Extension in the idq.dll that allows the worm to execute code on the WEB server.

The buffer overflow attack has been in existence since 1988 with the first Internet worm. The basics of the attack are to overload a location in memory until it "spills out" into the application code memory. Then insert code into the application code to point to a place in memory that contains the hackers code. This code can perform functions from crashing the server to calling another function or program that allows remote access. In Nicole LaRock Decker's GSEC practical paper dated November 13, 2000 on **Buffer Overflows: Why, How and Prevention,** http://www.sans.org/infosecFAQ/threats/buffer_overflow.htm, she covers in detail on how a buffer overflow occurs and the steps to take in application development to prevent a buffer overflow.

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

The details of the buffer overflow with Microsoft's IIS Index server was published June 18, 2001 on Securityfocus.com. This is an important fact since Code Red, the first variant, was discovered on July 16 and Code Red II worm was discovered on August 4, 2001 that is 26 and 46 days respectively from the published date of the exploit. Since the exploit is known so is the signature of the attack and with this attack signature a NIDS is able to detect the attack. Once the NIDS detects the attack the IIS WEB server's defense is possible.

The Code Red II infection as reported by eEye.com, http://www.eeye.com/html/Research/Advisories/AL20010804.html, has three phases: Infection, Propagation, and Trojan insertion.

Phase 1: Infection

1. Checks local system language for Chinese (both Taiwanese and PRC)

2. Checks to see if this is the first execution; if not it proceeds to Propagation Phase

3. Uses the existence of an "atom" or flag inserted by Code Red II to determine if there is an infection; if the atom exists the worm sleeps forever, otherwise the atom is created

4. Sets the number of parallel propagation threads to 300 for non-Chinese systems and 600 for Chinese and then the Propagation Phase begins

5. Creates a new copy of its process which re-initiates the Infection Phase

6. Starts the Trojan Phase and the worm sleeps for 1 day for non-Chinese or 2 days for Chinese, before rebooting Windows

Phase 2: Propagation

1.Spreads until October 1, 2002; after this the system will reboot, effectively clearing the worm from memory. NOTE: A reboot is a function that a HIDS would detect.

2.Selects the next IP address to attempt to infect; address selection is designed to seek out nearby addresses, thereby speeding up the spread of the infection.

1/7 chance of selecting an IP address unrelated to local address

3/7 chance of selecting same class A range as local address

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

3/7 chance of selecting same class B range as local address

3. Attempts a speedy non-blocking connection to the address selected; if successful, it converts to blocking connection and attempts to infect

4. Repeats Propagation Phase

Phase 3: Trojan insertion

1. Copies cmd.exe into two directories.

2. Creates copies of explorer.exe on C; and D: of they exist

3. Imbeds Trojan code in these copies of explorer.exe; as long as one of these is running an attacker will be able to execute commands remotely. NOTE: A HIDS would detect the changing of a file. At this point an Antivirus scan would detect the Trojan, but the exploit could have already compromised the system by allowing the hacker free reign to create accounts and other backdoor trojans.

Now that we know the behavior of the worm, we are able to detect its presents. First, the worm uses an exploit in idq.dll using a string of characters that is detectable by a NIDS. Second, the worm performs two functions, system reboot and changing of explorer.exe, that will generate an alert in a HIDS.

Using NetProwler to detect Code Red II

Description of NetProwler

Symantec's NetProwler is a NIDS. This product acquired during the purchase of Axent in December 2000. NetProwler is a three-tiered product with an agent, manager, and console. The agent piece is placed on an un-switched network segment, the critical concept to NIDS is that they reside on the same un-switched network as the host you are monitoring, and analyzing the traffic for known attacks via a string of data. The analysis of a NDIS is comparable to the process of an antivirus scanner; they both look for a match via signatures in a data stream that signifies an attack or virus. The manager stores the attack signatures, attack reports. The console allows for configuration, reporting, and important alerting. With NetProwler, you are able to define the host by IP address, operating system, and applications that a host is running. This narrowing of the scope allows for more accurate reporting and alerting. This

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

allows the security administrators to focus on attacks related to their environment. For example in a network that only uses Microsoft NT and Windows 2000 will not get alerted to attacks specific for AIX or Solaris, they attack is useless and only creates overhead for the security administrators.

The installation of NetProwler, as with any IDS, requires that the critical host be defined and that there are incident handling policies in place. The first step is to determine what is important? Frederick the Great once commented that “to attempt to defend everything is to defend nothing.” With high levels of “script kitty’s” running random attacks at various systems it would be impossible to watch the entire network for all attacks. So tuning the IDS to the specifics of the host, OS and applications or services, will reduce the false alarms allowing time for the security group to focus on defending the key systems that support the company. The next step is applying the incident handling policy to the IDS. NetProwler can respond to an alert in multiple ways, from a sending a page to hardening a firewall. Each level of attack requires a plan of action from an alert to shutting down the connection. For the Code Red worm or other worms terminating the attack session or hardening the firewall, that will “black list the IP address the attacking host” could be sufficient to defend the host. In this engagement, the host continues to operate but the attack is stopped.

Code Red II detection NIDS style

In the pervious section, it determined that Securityfocus published the exploit June 18, 46 days before the outbreak of Code Red II. Symantec supplied NetProwler with the signature June 20 to the Index Server ISAPI buffer overflow exploit. This signature allows NetProwler to detect the Code Red attack and any other attack that uses this entry point into the server. Below are two types of known attack Index Server ISAPI buffer overflow signatures with the difference between the two signatures is character X replacing character N.

```
/default.ida?NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN%u9090%u6858%ucbd
3%u7801%u9090%u6858%ucbd3%u7801%u9090%u6858%ucbd3%u7801%u9
090%u9090%u8190%u00c3%u0003%u8b00%u531b%u53ff%u0078%u0000%u
00=a HTTP/1.0
```

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

/default.ida?XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXX%u9090%u6858%ucbd3%u7801%u9090%u6858%uc
bd3%u7801%u9090%u6858%ucbd3%u7801%u9090%u9090%u8190%u00c3%
u0003%u8b00%u531b%u53ff%u0078%u0000%u00=a HTTP/1.0

Since there are two versions of the signature with only minor differences between them there is a potential that a third or forth variant might surface that means that NetProwler potentially will need updated before a new signature package is released. In FIGURE 1 is the screen shot of the first page to create a new signature for NetProwler. In this page the signature is named, defined as simple packet or multiple packets, associated to OS and application, and prioritized.

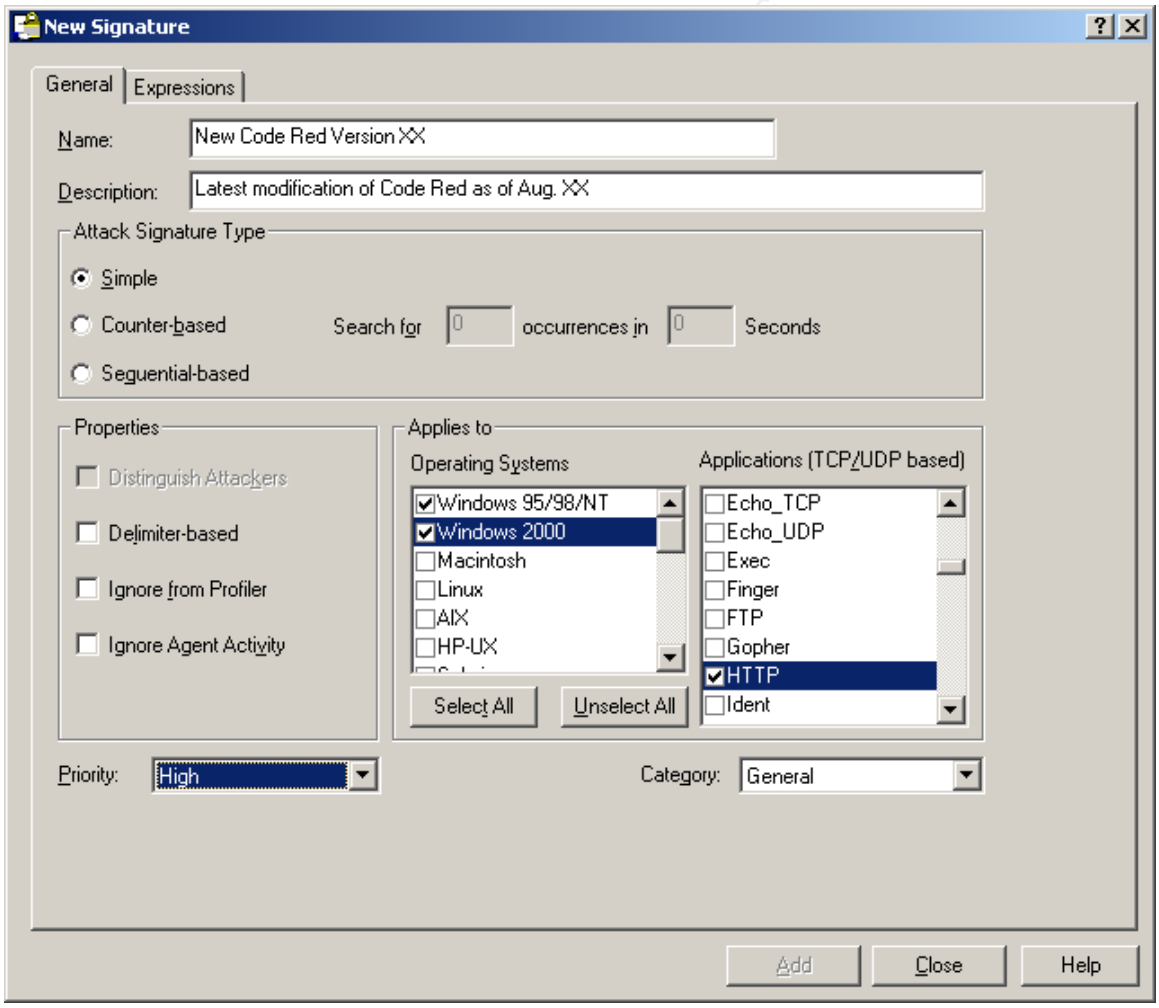

FIGURE 1

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

In FIGURE 2, the signature is defined. The information is that same information a network sniffer would gather from the network wire during the attack. Once the signature is created it is applied to all agents and is immediately used to detect the attack.

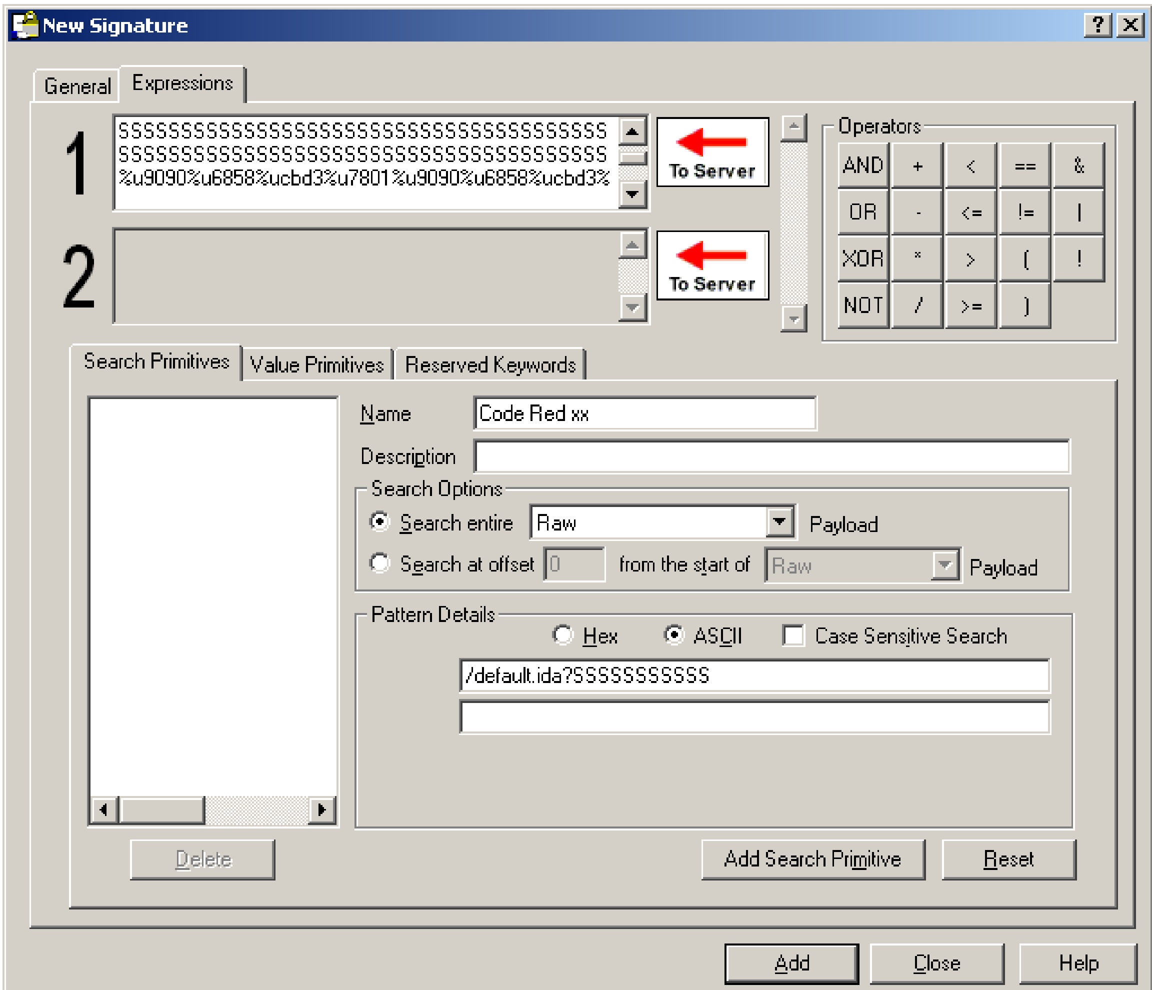

FIGURE 2

The issue with applying a new self created signature knowing when there is a new missed attack. That is the reasoning for having a HIDS, to catch attacks missed by the NIDS and affecting the host.

Using Intruder Alert to detect Code Red II

Description of Intruder Alert

Symantec Intruder Alert is a HIDS. It also was a product acquired from Axent during the merger. Intruder Alert is a three-tiered product agent, manager, and console. The agent piece is placed on a critical host like WEB servers, file servers, database servers, etc. The agent is tied into the host OS allowing the

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

agent to read log files, notice file changes, user changes, and access to running services. The manager is the central repository for policies and alerts plus it correlates events to determine if it is an attack. The console in includes two components the first is the ITA Administrator and the second is the Event Viewer. In addition, Intruder Alert can also receive events generated by NetProwler and then apply an action to the event like show to event viewer.

Intruder Alert configuration uses a set of policies to control the what, when, how of an attack and then apply a response to that attack. Inside each policy, FIGURE 3, includes the rules and the domain; inside the domain are the watched agents. A rule is an event or a series of events that are considered an attack. In Figure 3 the good_file_watch rule is reading the system log file for the message "c:\ita_demo\watch_files\good.txt File Change." When this message is found the rule's Action is to Execute Command, replace.bat, that replaces the modified file good.txt with a known good version and then it sends a alert to the Event Viewer.

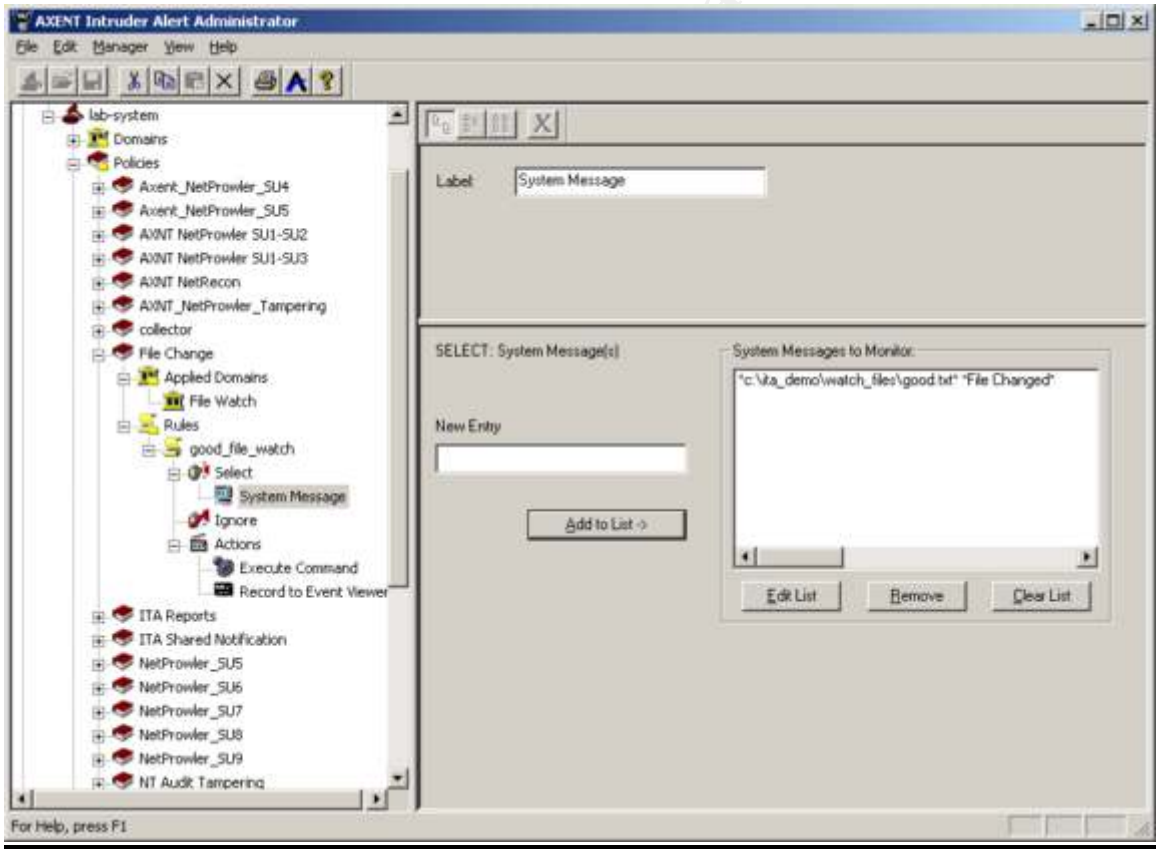

FIGURE 3

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

With Intruder Alert, an event is decided from one of the Select functions listed below:

- System Message - Selects or ignores specific text in event messages generated by an application or operating system.
- ITA Status - Selects or ignores specific text in Intruder Alert status messages.
- ITA Error - Selects or ignores specific text in Intruder Alert error messages.
- ITA Command - Selects or ignores ITA commands sent to the Agent from Intruder Alert Event Viewer.
- Flag - Selects or ignores flags raised by other rules.
- Timer - Selects timers started by another rule's action.
- Date - Selects or ignores events occurring within a range of time.
- ITA Rule -Selects or ignores a specified rule.
- System - Selects or ignores events generated on specific Agent systems

When an event happens it calls an Action or Actions listed below:

- Record to Event Viewer - Records the event in an event database on the Manager system for Intruder Alert Event Viewer reporting.
- Raise Flag - Raises a flag for a specified period of time.
- Lower Flag - Cancels a raised flag.
- Send Email - E-mails the event message to a specified recipient.
- Send Page - Notifies an administrator via pager that the event occurred.
- Append to File - Writes the event to the end of a specified log file.
- Notify - Sends the event message
- Start Timer - Initiates a timer to count down to a specified date or for a specified amount of time.
- Execute Command - Executes a system command, batch file, executable file, NetWare Loadable Module, or shell script
- Run Shared Actions - Executes an action defined in another policy rule residing on the Agent system.
- Cancel Timer - Terminates a timer.
- Kill process - Stops a process referenced in the event.
- Disconnect session - disconnects the user's session
- Disable Account - Disables a user's account

How the rules are applied depends on the Incident Handling procedures that are in place. Knowing how Code Red II works via a system reboot and file modification, Intruder Alert has multiple ways to detect the attack and limit the damage it will cause.

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

Code Red II detection HIDS style

In the eEye report, reviewed in Code Red details, Code Red II performed two actions that a general WEB server generally does not perform in a common environment. The first action, a system restart, is an action would write an entry into the system log and the second, the changing and moving of explorer.exe, is a file that could be monitored by Intruder Alert. Since Code Red II performs both events, a good Intruder Alert Policy would look for both events then take an action to reduce the damage.

The next step is to determine the Action needed to stop the damage caused by Code Red II. The first Action is to send an alert to the Event Viewer notifing the security administrators of the infection. After sending an alert to the security administrators, the next step is to contain the worm and to prevent unauthorized access caused by the worm. There are multiple paths to take to contain or remove the worm. One method is to use one of the tools that Both Symantec and Microsoft provide to remove the worm from memory and the file system or there are antivirus signatures provided by all antivirus vendors to remove the Trojan from the file system. Either method uses a command or script that could be executed from an Action rule. The next step to containment of the Trojan is to turn off the network interface using the Kill Process Action; this will stop the unauthorized access and stop the worm from spreading. In addition, the last step would send a Page notifying the WEB admin that the WEB server is inactive and infected with Code Red II. And lastly, an e-mail is sent to the WEB Admin that a hotfix, located at http://www.microsoft.com/windows2000/downloads/critical/q300972/default.asp?FinishURL=%2Fdownloads%2Frelease%2Easp%3FReleaseID%3D30800%26redirect%3Dno , is available to prevent the idq.dll buffer overflow and since the WEB server is down that they may want to apply it before restarting the WEB server.

Conclusion

The correct use of both NetProwler and Intruder Alert or other NIDS or HIDS can stop the spread and damage cause by Code Red II. At last count, there are over 9000 reported infections. Granted, most are small shops or home users there are infections report by large multi-national companies with a final cost, as reported by Ziff Davis http://www.zdnet.com/zdnn/stories/news/0,4586,2802447,00.html, at over $8.7 billion. With NetProwler a means of detecting and stopping the buffer overflow exploit was available about 40 days before the published date of Code Red II the spread of the worm could have been limited. On the host side, an HIDS would have detected the anomaly the worm caused with a server restart and the changing of explorer.exe. With the use of NIDS and HIDS, the total damage and news cause by Code Red II would have been a little blip on the Internet radar screen.

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

References:

http://www.sans.org/infosecFAQ/threats/buffer_overflow.htm

http://www.eeye.com/html/Research/Advisories/AL20010804.html

http://www.cert.org/advisories/CA-2001-19.html

http://www.sarc.com/avcenter/venc/data/codered.ii.html

http://www.sarc.com/avcenter/venc/data/codered.worm.html

http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS01-033.asp

Running Snort on IIS Web Servers Part 2: Advanced Techniques
by Mark Burnett

Symantec Documentation for NetProwler 3.51 and Intruder Alert 3.51

http://www.zdnet.com/zdnn/stories/news/0,4586,2802447,00.html

© SANS Institute 2001, Author retains full rights

Last Updated: May 19th, 2013

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Malaysia @ MCMC 2013	**Cyberjaya, MY**	**Jun 03, 2013 - Jun 08, 2013**	**Live Event**
SANS Pen Test Berlin 2013	**Berlin, DE**	**Jun 03, 2013 - Jun 08, 2013**	**Live Event**
Industial Control Systems Security Training - Houston	**Houston, TXUS**	**Jun 10, 2013 - Jun 15, 2013**	**Live Event**
Security Impact of IPv6 Summit 2013	**Washington, DCUS**	**Jun 14, 2013 - Jun 16, 2013**	**Live Event**
SANSFIRE 2013	**Washington, DCUS**	**Jun 14, 2013 - Jun 22, 2013**	**Live Event**
SANS Canberra 2013	**Canberra, AU**	**Jul 01, 2013 - Jul 13, 2013**	**Live Event**
SANS London Summer 2013	**London, GB**	**Jul 09, 2013 - Jul 16, 2013**	**Live Event**
Digital Forensics & Incident Response Summit 2013	**Austin, TXUS**	**Jul 09, 2013 - Jul 16, 2013**	**Live Event**
SANS Rocky Mountain 2013	**Denver, COUS**	**Jul 14, 2013 - Jul 20, 2013**	**Live Event**
SANS Mumbai 2013	**Mumbai, IN**	**Jul 22, 2013 - Jul 27, 2013**	**Live Event**
SEC528 SANS Training Program for the CompTIA® New Advanced Security Practitioner (CASP) Certification	**Washington, DCUS**	**Jul 22, 2013 - Jul 26, 2013**	**Live Event**
SANS San Francisco 2013	**San Francisco, CAUS**	**Jul 29, 2013 - Aug 03, 2013**	**Live Event**
SANS SEC 560: Network Penetration Testing @ Bangalore 2013	**Bangalore, IN**	**Aug 05, 2013 - Aug 10, 2013**	**Live Event**
SANS Boston 2013	**Boston, MAUS**	**Aug 05, 2013 - Aug 10, 2013**	**Live Event**
Critical Security Controls Summit	**Washington, DCUS**	**Aug 12, 2013 - Aug 18, 2013**	**Live Event**
Industrial Control Systems Security Training - DC	**Washington, DCUS**	**Aug 12, 2013 - Aug 16, 2013**	**Live Event**
Mobile Device Security Summit 2013	**OnlineCAUS**	**May 30, 2013 - Jun 06, 2013**	**Live Event**
SANS OnDemand	**Books & MP3s OnlyUS**	**Anytime**	**Self Paced**