Global Information Assurance Certification Paper

*** Northcutt, The maximum score I am supposed to give for this is a 90, however I feel this document contributes significantly to the state of practice for defensive information operations. Bravo and give my regards to clever.net! 92 *

GCIA Certification Practical

Timothy D. Trow
10 Detects with Analysis
April 24, 2000
I&W Methodology used.

Detect 1 Location: http://www.sans.org/y2k/032800-2000.htm

From an @home user… smattering of Netbus, a pinch of BackOrifice, a bit of SubSeven…

> Mar 27 00:09:52 cc1014244-a kernel: securityalert: tcp if=ef0 from 209.235.11.254:50998 to 24.3.21.199 on unserved port 512
> Mar 27 01:08:04 cc1014244-a kernel: securityalert: tcp if=ef0 from 24.40.35.215:2790 to 24.3.21.199 on unserved port 12345
> Mar 27 08:18:19 cc1014244-a kernel: securityalert: tcp if=ef0 from 38.27.95.44:2756 to 24.3.21.199 on unserved port 1080
>
> Mar 27 19:22:03 cc1014244-a kernel: securityalert: tcp if=ef0 from 38.26.9.97:4882 to 24.3.21.199 on unserved port 1080
> Mar 27 20:29:59 cc1014244-a kernel: securityalert: tcp if=ef0 from 151.198.141.96:2660 to 24.3.21.199 on unserved port 27374
>
> Mar 27 20:50:25 cc1014244-a kernel: securityalert: tcp if=ef0 from 151.198.141.96:2344 to 24.3.21.199 on unserved port 27374
>
> Mar 27 20:57:48 cc1014244-a kernel: securityalert: tcp if=ef0 from 207.50.63.40:3537 to 24.3.21.199 on unserved port 1243
>
> Mar 27 22:07:59 cc1014244-a kernel: securityalert: udp if=ef0 from 38.32.11.6:1044 to 24.3.21.199 on unserved port 31337

Active Targeting?

Yes. The traffic is being targeted towards the same address on various ports.

History:

No previous history was noted in the detect report.

Technique(s):

All activity was within one day, March 27. The times were very different. Times ranged from 10 minutes past midnight to later that evening. The attacker seemed to be very careful

about keeping the times at a distance. The source IP is multiple IP's, or someone is spoofing those IP's. The attacker is targetting the same destination address on every attempt, but targeting various destination ports. The various random source addresses really scare me. This is not a pretty picture. This could be some type of script running or a very careful and collective attack methodology!

Analysis/Intent:

There are many possible exploits being targeted here. Port 512/tcp is UNIX remote exec. This may be a way trying to gain access to a UNIX system by issuing remote commands. Rexecd allows redirection of stderr stream to an arbitrary port on the client machine. This stream is opened by rexecd before authentication of the user. Spoofing techniques could allow the client to direct the stderr stream towards an arbitrary host as well as an arbitrary port, possibly exploiting a given trust model. Another port of interest is port 12345/tcp. Netbus is similar to BackOrifice. It allows ANYONE running the client portion to connect and control ANYONE running the server portion of it, WITH THE SAME RIGHTS AND PRIVILEGES AS THE CURRENTLY LOGGED ON USER! It allows the remote user total access. The next port 1080/tcp is a SOCKS proxy port. This could be used as a potential spam relay point. Ports 27374/tcp are examples of sub-7 (or also known as subseven). This is a default port that appeared in v2.0. This port along with port 1243/tcp are very well known trojan ports. I found the following on this: Supports "port redirection", so that any attack can be funneled through a victim's machines. Contains extensive tricks to play with ICQ, AOL IM, MSN Messenger, and Yahoo messenger, including password sniffing, posting messages, and other features. Extensive UI tricks, such as flipping the screen, talking through the victim's speaker, and spying on the victim's screen. Sub7 is written by a hacker who calls himself "Mobman". The last trace show destination port 31337/tcp being targeted. This is the well known trojan horse port called BackOriffice. It is similar in action to the Netbus trojan horse, very dangerous and common among the hacker community. The targeted **port scanning** of these well-known ports is indicative of a need to exploit. I would be very concerned with these "attempts". What seems to be the saving grace is just that, they all seemed to be failed attempts. The **cc1014244-a kernel: securityalert:** seems to indicate that these attempts had failed. This seems to be a UNIX platform running some type of Firewall software.

Identify Hostile Individuals and Groups?

It may be hard to track these down. NOTE: I attempted an http to 209.235.11.254 (http://209.235.11.254/) and found that it brought me to the web page for "The Digital LandLords". Now it gets a little strange from here I have to confess. I clicked on the link named, The Digital LandLords and it brought me to the following URL; http://home.clever.net/. The web page described Clever Internet Services, A Division of Interliant. What is so strange about this is that I work for a company in Woburn. MA called Triumph Technologies, Inc. Interliant bought us up in November 1999. Interliant is in the ASP, Web hosting business...so I have a feeling that the would be attacker may be using their web servers as a launching pad for their attacks. Since Clever.net is an ISP located in Atlanta, this may be an inside job so to speak. An ISP/Web hosting facility would be able to gain access to multiple of servers to launch prospective attacks. The times also warrant this. They span the whole night!

Components:	**Score:**	**Comments:**
Criticality:	5	Attacks are against one machine.
Lethality:	5	These ports of attack are very lethal and some are well-known trojan horses
System Countermeasures:	4	The system seems to be blocking these ports
Network Countermeasures:	4	The network does a decent job of blocking these ports.

Severity Total:	2	**(Criticality + Lethality) – (System Countermeasures + Network countermeasures)**

Detect 2 Location: http://www.sans.org/y2k/032800.htm

```
Mar 27 12:33:28 myhost portsentry[178]: attackalert:
Connect from host: na-165-5.na.avantel.net.mx/148.245.165.5
to UDP port: 111
Mar 27 12:33:28 myhost portsentry[178]: attackalert:
Connect from host: na-165-5.na.avantel.net.mx/148.245.165.5
to UDP port: 111
Mar 27 12:33:33 myhost portsentry[178]: attackalert:
Connect from host: na-165-5.na.avantel.net.mx/148.245.165.5
to UDP port: 111
Mar 27 12:33:38 myhost portsentry[178]: attackalert:
Connect from host: na-165-5.na.avantel.net.mx/148.245.165.5
to UDP port: 111
Mar 27 12:33:43 myhost portsentry[178]: attackalert:
Connect from host: na-165-5.na.avantel.net.mx/148.245.165.5
to UDP port: 111
Mar 27 12:33:48 myhost portsentry[178]: attackalert:
Connect from host: na-165-5.na.avantel.net.mx/148.245.165.5
to UDP port: 111
Mar 27 12:33:53 myhost portsentry[178]: attackalert:
Connect from host: na-165-5.na.avantel.net.mx/148.245.165.5
to UDP port: 111
Mar 27 12:33:58 myhost portsentry[178]: attackalert:
Connect from host: na-165-5.na.avantel.net.mx/148.245.165.5
to UDP port: 111
Mar 27 12:34:03 myhost portsentry[178]: attackalert:
Connect from host: na-165-5.na.avantel.net.mx/148.245.165.5
to UDP port: 111
Mar 27 12:34:08 myhost portsentry[178]: attackalert:
Connect from host: na-165-5.na.avantel.net.mx/148.245.165.5
to UDP port: 111
Mar 27 12:34:13 myhost portsentry[178]: attackalert:
Connect from host: na-165-5.na.avantel.net.mx/148.245.165.5
to UDP port: 111
Mar 27 12:34:18 myhost portsentry[178]: attackalert:
Connect from host: na-165-5.na.avantel.net.mx/148.245.165.5
to UDP port: 111
Mar 27 12:34:23 myhost portsentry[178]: attackalert:
Connect from host: na-165-5.na.avantel.net.mx/148.245.165.5
to UDP port: 111
Mar 27 12:34:28 myhost portsentry[178]: attackalert:
Connect from host: na-165-5.na.avantel.net.mx/148.245.165.5
to UDP port: 111
Mar 27 12:34:33 myhost portsentry[178]: attackalert:
```

Connect from host: na-165-5.na.avantel.net.mx/148.245.165.5
to UDP port: 111
Mar 27 12:34:38 myhost portsentry[178]: attackalert:
Connect from host: na-165-5.na.avantel.net.mx/148.245.165.5
to UDP port: 111
Mar 27 12:34:43 myhost portsentry[178]: attackalert:
Connect from host: na-165-5.na.avantel.net.mx/148.245.165.5
to UDP port: 111
Mar 27 12:34:48 myhost portsentry[178]: attackalert:
Connect from host: na-165-5.na.avantel.net.mx/148.245.165.5
to UDP port: 111
Mar 27 12:34:53 myhost portsentry[178]: attackalert:
Connect from host: na-165-5.na.avantel.net.mx/148.245.165.5
to UDP port: 111
Mar 27 12:34:58 myhost portsentry[178]: attackalert:
Connect from host: na-165-5.na.avantel.net.mx/148.245.165.5
to UDP port: 111
Mar 27 12:35:03 myhost portsentry[178]: attackalert:
Connect from host: na-165-5.na.avantel.net.mx/148.245.165.5
to UDP port: 111
Mar 27 12:35:08 myhost portsentry[178]: attackalert:
Connect from host: na-165-5.na.avantel.net.mx/148.245.165.5
to UDP port: 111
Mar 27 12:35:13 myhost portsentry[178]: attackalert:
Connect from host: na-165-5.na.avantel.net.mx/148.245.165.5
to UDP port: 111
Mar 27 12:35:18 myhost portsentry[178]: attackalert:
Connect from host: na-165-5.na.avantel.net.mx/148.245.165.5
to UDP port: 111

Active Targeting?

Yes. The destinations interface seems to be a target of the source IP.

History:

No previous history was noted in the detect report.

Techniques:

It seems the destination port 111/udp is the target. Every few seconds, UDP packets are being set to the same destination IP and port. The time frame was only a couple of minutes. I also feel that the attacker has a very good idea of who he or she is targeting. The 'myhost' seems to be a mystery here. Not sure if this is a firewall or some host behind a firewall. The source address is an active Internet address. This seems to be a calculated and specific attack destined for one address and one specific port.

Analysis/Intent:

This detect seems to be an **attempt to connect to port 111 or sunrpc**. This port can also be seen with the tcp port service known as portmap. Port 111 is known for such services as

NFS and NIS or rpc-based services. This allows a would-be attacker the ability to learn what type of services may be running on the Unix server in question. This attack almost seems contrived, meaning that the attacker seems to know exactly where they want to go. Not having other information, you could say that this attacker knew exactly what machine to target and what service/ports to scan. There is no port or host scan attempts showing randomness. This is indeed strange.

Identify Hostile Individuals and Groups?

I checked Internic.net and found the following on the avantel.net

Server Name: IENLACES3.IENLACES.COM.MX
IP Address: 148.245.165.5
Registrar: NETWORK SOLUTIONS, INC.
Whois Server: whois.networksolutions.com
Referral URL: www.networksolutions.com

It seems to have originated in Mexico (the .mx), an ISP in Mexico. They should be notified of this activity for possible monitoring and notification. Other than that, no other groups of individuals known seem to have been responsible or known for this signature attack for port/111, sunrpc.

Components:	**Score:**	**Comments:**
Criticality:	3	This is probably a UNIX server and has some type of value
Lethality:	4	this could be a real problem if The unit is UNIX and the port is open
System Countermeasures:	3	I hoping that the system has been locked down with patches.
Network Countermeasures:	3	If the host is behind a Firewall, Then there is real problems. If ot, there is still problems.
Severity Total:	**1**	**(Criticality + Lethality) – (System Countermeasures + Network countermeasures)**

Detect 3 Location: http://www.sans.org/y2k/032600-2000.htm

A friend of mine sent me this. SN suggested I pass it to GIAC. (I've sanitized it, obviously.) Any ideas?

- A.

Do you know of any good exploitz that people are probing nntp for?

Mar 22 13:23:36 box.at.victim.com /ipmon[4872]: 13:23:36.638478 le0
@0:19
b 24.0.94.130,38945 -> IP.OF.VICTIM.COM,119 PR tcp len 20 44 -S
Mar 22 13:23:37 box.at.victim.com /ipmon[4872]: 13:23:37.315117 le0
@0:19
b 24.0.94.130,38945 -> IP.OF.VICTIM.COM,119 PR tcp len 20 40 -R
Mar 22 13:23:37 box.at.victim.com /ipmon[4872]: 13:23:37.326922 le0
@0:19
b 24.0.94.130,39317 -> IP.OF.VICTIM.COM,119 PR tcp len 20 44 -S
Mar 22 13:23:38 box.at.victim.com /ipmon[4872]: 13:23:38.312697 le0
@0:19
b 24.0.94.130,39317 -> IP.OF.VICTIM.COM,119 PR tcp len 20 40 -R
Mar 22 18:04:02 box.at.victim.com /ipmon[4872]: 18:04:01.661131 le0
@0:19
b 24.0.94.130,59273 -> IP.OF.VICTIM.COM,119 PR tcp len 20 44 -S
Mar 22 18:04:03 box.at.victim.com /ipmon[4872]: 18:04:03.188819 le0
@0:19
b 24.0.94.130,59273 -> IP.OF.VICTIM.COM,119 PR tcp len 20 40 -R
Mar 22 18:04:03 box.at.victim.com /ipmon[4872]: 18:04:03.210320 le0
@0:19
b 24.0.94.130,60187 -> IP.OF.VICTIM.COM,119 PR tcp len 20 44 -S
Mar 22 18:04:04 box.at.victim.com /ipmon[4872]: 18:04:03.811455 le0
@0:19
b 24.0.94.130,60187 -> IP.OF.VICTIM.COM,119 PR tcp len 20 40 -R
Mar 22 22:48:17 box.at.victim.com /ipmon[4872]: 22:48:16.835881 le0
@0:19
b 24.0.94.130,50230 -> IP.OF.VICTIM.COM,119 PR tcp len 20 44 -S
Mar 22 22:48:18 box.at.victim.com /ipmon[4872]: 22:48:18.161571 le0
@0:19
b 24.0.94.130,50230 -> IP.OF.VICTIM.COM,119 PR tcp len 20 40 -R
Mar 22 22:48:18 box.at.victim.com /ipmon[4872]: 22:48:18.173064 le0
@0:19
b 24.0.94.130,50678 -> IP.OF.VICTIM.COM,119 PR tcp len 20 44 -S
Mar 22 22:48:19 box.at.victim.com /ipmon[4872]: 22:48:18.986828 le0
@0:19
b 24.0.94.130,50678 -> IP.OF.VICTIM.COM,119 PR tcp len 20 40 -R
Mar 23 03:20:08 box.at.victim.com /ipmon[4872]: 03:20:07.585219 le0
@0:19
b 24.0.94.130,62610 -> IP.OF.VICTIM.COM,119 PR tcp len 20 44 -S
Mar 23 03:20:08 box.at.victim.com /ipmon[4872]: 03:20:08.045238 le0
@0:19
b 24.0.94.130,62610 -> IP.OF.VICTIM.COM,119 PR tcp len 20 40 -R
Mar 23 03:20:08 box.at.victim.com /ipmon[4872]: 03:20:08.056194 le0
@0:19
b 24.0.94.130,62931 -> IP.OF.VICTIM.COM,119 PR tcp len 20 44 -S
Mar 23 03:20:09 box.at.victim.com /ipmon[4872]: 03:20:08.858156 le0
@0:19
b 24.0.94.130,62931 -> IP.OF.VICTIM.COM,119 PR tcp len 20 40 -R
Mar 23 07:46:43 box.at.victim.com /ipmon[4872]: 07:46:42.379020 le0
@0:19
b 24.0.94.130,61302 -> IP.OF.VICTIM.COM,119 PR tcp len 20 44 -S

Mar 23 07:46:44 box.at.victim.com /ipmon[4872]: 07:46:43.418154 le0 @0:19
b 24.0.94.130,61302 -> IP.OF.VICTIM.COM,119 PR tcp len 20 40 -R
Mar 23 07:46:44 box.at.victim.com /ipmon[4872]: 07:46:43.442809 le0 @0:19
b 24.0.94.130,62218 -> IP.OF.VICTIM.COM,119 PR tcp len 20 44 -S
Mar 23 07:46:44 box.at.victim.com /ipmon[4872]: 07:46:44.091157 le0 @0:19
b 24.0.94.130,62218 -> IP.OF.VICTIM.COM,119 PR tcp len 20 40 -R

I've also been it up for a netbios scan -- big surprise here:

Mar 22 20:11:46 box.at.victim.com /ipmon[4872]: 20:11:45.638701 le0 @0:19 b 24.24.100.172,2066 -> IP.OF.VICTIM.COM,137 PR udp len 20 78

** Andy Johnston

Active Targeting?

Yes. The traffic has been targeted from the source IP to the destination port/interface.

History:

There was no other information available for this particular detect.

Techniques:

The 24.0.X.X seems to be a valid Internet IP and no real signs of any IP spoofing going on. The 'le0' seems to signify a UNIX based system, probably a Sun Solaris. The 'le0' is also probably the external interface of the host in question, the box.at.victim.com. The internal interfaces are usually defined as qe1 or qfe1 if fast ethernet. As the trace shows, the signs of SYN and RESET are clear. The target TCP port is 119, or USENET Network News Transport Protocol (nntp) seems to be the only target port on the victim server. We would probably see a SYN/ACK if the port was open and a RESET for closed port. The lack of a three-way handshake shows that active scan and access to port 119 of the victim.com host. Another thing I noticed is the times, they seem to be in blocks of different times.

Analysis/Intent:

The intent seems to be directed at port 119, a potentially dangerous port. Port 119 is used for nntp (network news transport protocol). What I found on port 119 is that it has been linked to a trojan horse called Happy99, ska trojan. I also found the following; Happy99 is a Win32 based Trojan program. When this program is executed it will display some fireworks. Apart from the fireworks display this program will do some other activity in the background without the user's permission. In the background this program will create two files SKA.EXE and SKA.DLL.It will alter WSOCK32.DLL to put its code into that file and keep the original file as WSOCK32.SKA. It can not modify the WSOCK32.DLL file if it is in use. In such a case this program will add an entry to the Windows Registry to run SKA.EXE the next time the computer is booted so that it can do

these modifications. The size of this trojan file is 10000 bytes. To play it safe, the system admin. should take a look into the targeting for the trojan on this particular server and also keep an eye out using various logging capabilities along with an IDS filtering set-up.

Identify Hostile Individuals and Groups?

From what I could find, it seems to be a user from @home in the west coast. It looks like they have been using this domain as a launching pad for the scan probing of port 119 for potential vulnerabilities. The ambiguity is enough to keep the red flags up. From the surface it's probably harmless, but I would take this port targeting as a real threat until I find otherwise or have proven otherwise. It is better to be safe then sorry!! Another avenue would be to contact @home and inform them.

Components:	**Score:**	**Comments:**
Criticality:	3	Not sure the value behind the server.
Lethality:	1	Look harmless from the surface, the potential is there.
System Countermeasures:	4	Hopefully the OS is patched
Network Countermeasures:	4	Hopefully the have other avenues to dial/connect out.
Severity Total:	-4	**(Criticality + Lethality) – (System Countermeasures + Network countermeasures)**

Detect 4 Location: http://www.sans.org/y2k/032500.htm

Mar 24 01:54:58 cc1014244-a kernel:
securityalert: tcp if=ef0 from
24.3.57.38:11111 to 24.3.21.199 on unserved port 12345
Mar 24 03:14:13 cc1014244-a kernel:
securityalert: tcp if=ef0 from
171.214.113.228:2766 to 24.3.21.199 on unserved port 1243
Mar 24 04:45:01 cc1014244-a kernel:
securityalert: tcp if=ef0 from
208.61.109.243:3578 to 24.3.21.199 on unserved port 1243
Mar 24 04:45:06 cc1014244-a kernel:
securityalert: tcp if=ef0 from
208.61.109.243:3832 to 24.3.21.199 on unserved port 27347
Mar 24 05:40:42 cc1014244-a kernel:
securityalert: udp if=ef0 from
24.24.100.172:2147 to 24.3.21.199 on unserved port 137

Mar 24 14:56:08 cc1014244-a kernel:
securityalert: udp if=ef0 from
63.17.79.40:4294 to 24.3.21.199 on unserved port 137
Mar 24 17:20:44 cc1014244-a kernel:
securityalert: tcp if=ef0 from
62.6.100.45:1828 to 24.3.21.199 on unserved port 27374

Mar 24 20:50:47 cc1014244-a kernel:
securityalert: tcp if=ef0 from
194.27.62.179:4857 to 24.3.21.199 on unserved port 27374

Active Targeting?

Yes. The traffic seems to be targeted at the host's interface from a source IP.

History:

There did not seem to be any other information supporting/denying this detect.

Techniques:

The detect seems to be targeting some very nasty UDP and TCP ports. These packets seems to be focused on one destination IP. The times vary as do the different IP's. The UDP traffic was foucsed on port 137. The TCP traffic was targeted at port 12345, 1243, 27347 and 27374. The IP's seem to be valid Internet IP's and not spoofed. I have a feeling that this was also a UNIX (?) based system and or Firewall.

Analysis/Intent:

As mentioned above, these ports are not very nice by nature. Port 12345 is a Netbus trojan. Port 1243 is Subseven and Backdoor-G trojans, port 137 is Netbios, port 27374 is Subseven 2.0 (an older version). These will need to be checked very carefully on the system in question for possible trojans placed and other exploits that netbios may have been exposed. Netbios can be a very dangerous tool in determining name resolution and other pertinent information concerning system names and functions.

Identify Hostile Individuals and Groups?

Traffic seems to have originated from various locations/IP's. These are potentially dangerous ports and should be looked at very carefully. Detailed logs and tracking system should be put together in order to keep a running history of the destination IP's and the port and services targeted. These ports seem to be random in nature or not very random at all.

Components:	Score:	Comments:
Criticality:	3	Whether or not this is a critical Server or not, the ports speak for themselves.
Lethality:	5	I consider these ports very important and dangerous.
System Countermeasures:	5	The system should be patched down and up to par.
Network Countermeasures:	3	I have a feeling this may be a Firewall or a very important Server.

Severity Total:	0	**(Criticality + Lethality) – (System Countermeasures + Network countermeasures)**

Detect 5 Location: http://www.sans.org/y2k/032800-2000.htm

I noticed this in my logs from yesterday...

-Kathleen

Hello,

I am writing because I noticed that your www7.clever.net server scanned a few of my servers yesterday for
exec (TCP port 512) and BO Facil (TCP port 5556). Your host may have been compromised or originated
from one of your customers, etc. I would appreciate it if you could investigate that matter and let me know the
outcome.

I have sanitized the information below. Please let me know if you need more information to investigate.

Thank you,
Kathleen

Mar 27 17:01:03.516 host kernel: 226 IP packet dropped (www7.clever.net[209.235.11.254]->host1[x.x.x.x1]: Protocol=TCP[SYN] Port 53050->5556): Restricted Port: Protocol=TCP[SYN] Port 53050->5556 (received on interface x.x.x.x)
Mar 27 17:01:03.516 host kernel: 226 IP packet dropped (www7.clever.net[209.235.11.254]->host1[x.x.x.x1]: Protocol=TCP[SYN] Port 53051->512): Restricted Port: Protocol=TCP[SYN] Port 53051->512 (received on interface x.x.x.x)
Mar 27 17:01:03.521 host kernel: 226 IP packet dropped (www7.clever.net[209.235.11.254]->host2[x.x.x.x2]: Protocol=TCP[SYN] Port 53052->5556): Restricted Port: Protocol=TCP[SYN] Port 53052->5556 (received on interface x.x.x.x)
Mar 27 17:01:03.522 host kernel: 226 IP packet dropped (www7.clever.net[209.235.11.254]->host2[x.x.x.x2]: Protocol=TCP[SYN] Port 53053->512): Restricted Port: Protocol=TCP[SYN] Port 53053->512 (received on interface x.x.x.x)
Mar 27 17:01:03.528 host kernel: 226 IP packet dropped (www7.clever.net[209.235.11.254]->x.x.x.x3: Protocol=TCP[SYN] Port 53054->5556): Restricted Port: Protocol=TCP[SYN] Port 53054->5556 (received on interface x.x.x.x)
Mar 27 17:01:03.528 host kernel: 226 IP packet dropped (www7.clever.net[209.235.11.254]->x.x.x.x3: Protocol=TCP[SYN] Port 53055->512): Restricted Port: Protocol=TCP[SYN] Port 53055->512 (received on interface x.x.x.x)

Active Targeting?

Yes. The traffic seems to be detected at the particular host, possibly a Firewall.

History:

As far as I can tell, there is no other information other than contacting Kathleen herself.

Techniques:

The TCP SYN packets where sent but without the SYN-ACK return. These ports were not open to begin with. I'm assuming the destination host is the same. Another thing to look at is the time. It seems to be at a consist time frame. No gaps to look at. The 2 ports being targeted are 5556/TCP and 512/TCP. From what I can tell this attack seems to be targeted at a Firewall and the networks behind it. The IP's seem to be valid and there are no signs of wrong doing at the IP level.

Analysis/Intent:

This detect seems to be a straightforward **host scan for 2 potentially dangerous ports, 5556/TCP and 512/TCP.** Port 512/TCP is a remote exec. Like I stated in a earlier detect, it is defined using the following terminology; . Rexecd allows redirection of stderr stream to an arbitrary port on the client machine. This stream is opened by rexecd before authentication of the user. Spoofing techniques could allow the client to direct the stderr stream towards an arbitrary host as well as an arbitrary port, possibly exploiting a given trust model. Another factor to consider is that remote exec is "intended for Intranet use" and not for someone on the internet trying to gain access to an internal server!! The other port in question, port 5556/TCP I found was tied to mtb backup that I believe is system specific. Maybe some type of scan was sent in order to determine the machine in question.. Like Kathleen stated, port 5556/TCP is used by would be attackers for facilitating BackOrifice at the front-end level. Both of ports have vulnerabilities that could be used by hackers to infiltrate your system

Identify Hostile Individuals and Groups?

What I found from Internic and from typing in www7.clver.net is that it brings you to a Web site called "The Digital Landlords". Click on a link there and it brings you to Clever.net. This is an ISP located in the southeast. This could be a great launching area for an attacker or attackers. As Kathleen seems to have done already, she is taking action to find out the origins and the logic/tact behind these attacks.

Components:	**Score:**	**Comments:**
Criticality:	5	This seems to be a critical server and or Firewall in front

		of it.
Lethality:	3	Though this seems to be stopping the attacks
System Countermeasures:	4	I'm assuming the system has The latest patches on the OS.
Network Countermeasures:	4	The compnay probably has Some type of backup communications in place
Severity Total:	0	**(Criticality + Lethality) – (System Countermeasures + Network countermeasures)**

Detect 6 Location: http://www.sans.org/y2k/032900-2030.htm

Hello, would you mind making sure that I am subscribed to each of these lists.

Also, do you happen to know what could be behind these detects?

192.168.111.101.1027 > SVRLOC.MCAST.NET.427: udp 138
192.168.111.101.1027 > SVRLOC.MCAST.NET.427: udp 90
192.168.111.102.1028 > SVRLOC.MCAST.NET.427: udp 138
192.168.111.102.1028 > SVRLOC.MCAST.NET.427: udp 90
192.168.111.111.1027 > SVRLOC.MCAST.NET.427: udp 138
192.168.111.111.1027 > SVRLOC.MCAST.NET.427: udp 90
192.168.111.114.1026 > SVRLOC.MCAST.NET.427: udp 138
192.168.111.114.1026 > SVRLOC.MCAST.NET.427: udp 90
192.168.111.164.1027 > SVRLOC.MCAST.NET.427: udp 138
192.168.111.164.1027 > SVRLOC.MCAST.NET.427: udp 90
192.168.139.19.1027 > SVRLOC.MCAST.NET.427: udp 138
192.168.139.19.1027 > SVRLOC.MCAST.NET.427: udp 90
192.168.139.38.1027 > SVRLOC.MCAST.NET.427: udp 138
192.168.139.38.1027 > SVRLOC.MCAST.NET.427: udp 90
192.168.139.82.1026 > SVRLOC.MCAST.NET.427: udp 138
192.168.139.82.1026 > SVRLOC.MCAST.NET.427: udp 90
192.168.40.112.1025 > SVRLOC.MCAST.NET.427: udp 138
192.168.40.112.1025 > SVRLOC.MCAST.NET.427: udp 90
192.168.40.58.1026 > SVRLOC.MCAST.NET.427: udp 138
192.168.40.58.1026 > SVRLOC.MCAST.NET.427: udp 90
192.168.46.23.427 > SVRLOC.MCAST.NET.427: udp 49

I have multiple instances of these being sent out in fairly short order. I ran it through uniq after cutting off the time stamp and I have found close to 30 machines on our network that is doing this same thing. Since we aren't doing MultiCast traffic yet on our network, I found this to be interesting at best. Each time (except the last one in that listabove) was using a src port of 102x and pointed at port 427. Kinda intriguing. Kinda curious if this is normal traffic due to some Netbios discovery, or if I am seeing a trojan in action. In any

case, here is a few listings with time stamps that you can see how close together the udp packets really are. I
will probably run it through tcpdump -x sometime later tonight.

13:25:21.182824 192.168.111.164.1027 > SVRLOC.MCAST.NET.427: udp 138
13:25:21.306509 192.168.111.164.1027 > SVRLOC.MCAST.NET.427: udp 90
13:25:21.479862 192.168.111.111.1027 > SVRLOC.MCAST.NET.427: udp 90
13:25:21.795723 192.168.111.101.1027 > SVRLOC.MCAST.NET.427: udp 138
13:25:21.989945 192.168.111.101.1027 > SVRLOC.MCAST.NET.427: udp 90
13:25:22.183933 192.168.111.164.1027 > SVRLOC.MCAST.NET.427: udp 90
13:25:22.345969 192.168.139.38.1027 > SVRLOC.MCAST.NET.427: udp 90

Thanks.
Scott

Active Targeting?

Yes. The outgoing traffic is seen to the destination address and port.

History:

No other evidence of information relating to this detect mentioned.

Techniques:

No sign of flag sets, or anomalous flag sets. As Scott mentioned above, these Packets/traces seem to have been originated from his internal network. The 192.168 in non-routable per the RFC and the destination address of svrloc.mcast.net.427. Port 427 is interesting. I'm presuming that port 427 is a udp port. If so, I found some interesting information on this; SCO OpenServer 5.0.5 'userOsa' symlink Vulnerability:

bugtraq id	701
object	/etc/sysadm.d/bin/userOsa (exec)
class	Origin Validation Error
cve	GENERIC-MAP-NOMATCH
remote	No
local	Yes
published	October 11, 1999
updated	April 11, 2000
vulnerable	SCO Open Server 5.0.5
	SCO Open Server 5.0.4
	SCO Open Server 5.0.3
	SCO Open Server 5.0.2
	SCO Open Server 5.0.1
	SCO Open Server 5.0
not vulnerable	

I also found some interesting data on 427/TCP; Specifically, the vulnerable service in the Intranetware client is the SLP Request service on TCP port 427. The command "nmap -sS -p427 target.com", which scans only port 427 on the target system with a TCP half-open sequence, causes an immediate Blue Screen condition. This condition is

recoverable; however subsequently the affected system loses all TCP network connectivity. Similarly, any "nmap -sS" scan which includes port 427 in the range of scanned ports causes the same fault (on most systems this includes the default scan with no ports specified). Some of then times stated in the later half of the detect seem The source IP's (internal) tend to be random hosts with various high ports. It also seems to cross various subnets and hosts.

Analysis/Intent:

My gut seems to point at some type of discovery versus one end trying to initiate a three-way handshake and exploit some type of vulnerability such as a trojan horse. The lack of a tcp communication session seems to shun the idea of a spoofed ip. I feel that 427/UDP is based on the data I found above, that GENERIC-MAP-NOMATCH is a SCO OpenServer 5.0.5 'userOsa' symlink Vulnerability and is the probable cause of this. The netBIOS port, 138 is another concern. Some information I found on that; Used by Windows (and services on UNIX like SAMBA). The main danger on the Internet is that by crafting special messages sent to this port, a hacker can convince Windows that their machine is "local", and can therefore bypass some of Microsoft's security settings that differentiate between "local" and "internet" zones. NetBIOS datagram service. This is primarily used for broadcasting information. It is primarily used by the SMB browser service that fills the information within the "Network Neighborhood" icon.

Identify Hostile Indivuals and Groups?

The internal IP is the 192.168.X.X. I was unable to really trace the origins of the svrloc.mcast.net network/location. I feel this is an internal matter, but that these servers should be checked for the above mentioned issues and vulnerabilities/exploits. Obiously, Scott is taking the appropriate steps in trying determine the reason behind the

Components:	**Score:**	**Comments:**
Criticality:	3	Not sure exactly the cause of this. Gave it a neutral status.
Lethality:	2	This seems to be internal and Thus not as lethal.
System Countermeasures:	3	Really hard to say at this point. I believe there server(s) may Need to be looked at for vulnerabilities.
Network Countermeasures:	3	Not sure the status of this Internally.
Severity Total:	-1	**(Criticality + Lethality) – (System Countermeasures + Network countermeasures)**

Detect 7 Location: http://www.sans.org/y2k/033100.htm

(Guy Bruneau from Canada writes in with this interesting report. I do not normally post long traces except

as the last entry in the file, but this is intriguing! Great research opportunity, what are these new ports, clues?
)

I detected the following Ring Zero scan today (ports 80, 3128, 8080) but it also contained a couple extra
ports (8002, 8050) I haven't seen yet associated with this activity. Any idea?

Guy Bruneau

Site: @home Host lookup: Date: 20000330 Pattern:
src host 63.11.117.219 /usr/local/logger/one_day_pat.pl
-S -d 20000330 -l @home -p 'src host 63.11.117.219 '
/Shadow/@home/Mar30
16:55:35.440651 1Cust219.tnt1.bryan.oh.da.uu.net.1865 > @.home.com.8080:
S 12492586:12492586(0) win 8192 (DF)
16:55:35.465692 1Cust219.tnt1.bryan.oh.da.uu.net.1866 > @.home.com.www:
S 12492589:12492589(0) win 8192 (DF)
16:55:35.484070 1Cust219.tnt1.bryan.oh.da.uu.net.1868 > @.home.com.3128:
S 12492595:12492595(0) win 8192 (DF)
16:55:35.484222 1Cust219.tnt1.bryan.oh.da.uu.net.1870 > @.home.com.8050:
S 12492601:12492601(0) win 8192 (DF)
16:55:35.484367 1Cust219.tnt1.bryan.oh.da.uu.net.1869 > @.home.com.8002:
S 12492598:12492598(0) win 8192 (DF)
16:55:36.664311 1Cust219.tnt1.bryan.oh.da.uu.net.1865 > @.home.com.8080:
S 12492586:12492586(0) win 8192 (DF)
16:55:36.666792 1Cust219.tnt1.bryan.oh.da.uu.net.1868 > @.home.com.3128:
S 12492595:12492595(0) win 8192 (DF)
16:55:36.706460 1Cust219.tnt1.bryan.oh.da.uu.net.1869 > @.home.com.8002:
S 12492598:12492598(0) win 8192 (DF)
16:55:36.758762 1Cust219.tnt1.bryan.oh.da.uu.net.1870 > @.home.com.8050:
S 12492601:12492601(0) win 8192 (DF)
16:55:37.625224 1Cust219.tnt1.bryan.oh.da.uu.net.1865 > @.home.com.8080:
S 12492586:12492586(0) win 8192 (DF)
16:55:37.939332 1Cust219.tnt1.bryan.oh.da.uu.net.1868 > @.home.com.3128:
S 12492595:12492595(0) win 8192 (DF)
16:55:37.949391 1Cust219.tnt1.bryan.oh.da.uu.net.1869 > @.home.com.8002:
S 12492598:12492598(0) win 8192 (DF)
16:55:37.985345 1Cust219.tnt1.bryan.oh.da.uu.net.1870 > @.home.com.8050:
S 12492601:12492601(0) win 8192 (DF)
16:55:38.396403 1Cust219.tnt1.bryan.oh.da.uu.net.1866 > @.home.com.www:
S 12492589:12492589(0) win 8192 (DF)
16:55:38.786750 1Cust219.tnt1.bryan.oh.da.uu.net.1865 > @.home.com.8080:
S 12492586:12492586(0) win 8192 (DF

Active Targeting?

Yes. There is evidence of targeting the @home.com user with various ports.

History:

There does not seem to be any other supporting evidence for this detect.

Techniques:

The times demonstrated where all within a couple of minutes. The source port was roughly the same..all are high ports in the 1865 to 170. The source IP is 63.11.117.219 from what Guy had mentioned. Another thing I noticed was that the SYN flag was set, but no other SYN-ACK or RES. The DF (defrag bit) was set, but then again there does not seem to be any data in the transfer, we find (0). The win 8192 seems valid. I also find that the same sequence numbers exist for each targeted port, such as in the first trace port 8080. And we find the same sequence number towards the end of the detect with the same port and seq. Numbers. The destination ip seems to be the same, but different ports are the targets.

Analysis/Intent:

This detect seems to be a **port scan for potential exploits** on various ports of interest. Port 80 as we all know is http. Port 8080 is sometimes used as an alternative to port 80 and is known as a proxy port (on a proxy server). Port 3128 is used as a proxy "squid" port. Some oh the information I found on the Internet support this; This is the default port for the "squid" HTTP proxy. An attacker scanning for this port is likely searching for a proxy server they can use to surf the Internet anonymously. You may see scans for other proxies at the same time, such as at port 8000/8001/8080/8888. Another cause of scans at this port, for a similar reason, is when users enter chatrooms.
Now, the real question is what does these other ports have in common with the "ring zero" scan Guy had found in regards to port 8002 and 8050. What I found out about port 8002 is that it; (TCP) 'rcgi' or "PERL.NLM' allows running of PERL scripts on a Novell 4.1 webserver. This could show that the port scan was to try to determine the server in question, exploration of the destination port/server. I was unable to find anything on port 8050. This could have been a diversion or a mistake from the source IP. This may have a comparison to port 8080. From what I can remember, the proxy port could be opened to any type of port, the default is 8080. There are settings that will allow you to open other ports for this service, via the browser. This may be a port scan within a port scan so too speak. Looking for other ports for manipulation. I would be very concerned that a possible known exploit is being searched for.

Identify Hostile Individuals and Groups?

The source IP was determined by Guy as 63.11.117.219 from a UU.net account, a major ISP that is known around the world as an MCI Worldcom company.

Components:	**Score:**	**Comments:**
Criticality:	3	This seems to be server and not a major production server/Firewall.
Lethality:	4	This seems to be a potentially dangerous exploit being targeted.
System Countermeasures:	3	I'm assuming that the system has been locked down.
Network Countermeasures:	4	I'm assuming that he has other avenues of getting out. (dialup/ISDN?)

Severity Total:	**0**	**(Criticality + Lethality) – (System Countermeasures + Network countermeasures)**

Detect 8 Location: http://www.sans.org/y2k/033000-2300.htm

Mar 28 00:16:09.225 firewall kernel: 226 IP packet dropped
(24.66.81.36->firewall.mydomain.edu[10.0.0.1]: Protocol=TCP[SYN]
Port 2357->27374): Restricted Port: Protocol=TCP[SYN] Port 2357->27374
(received on interface 10.0.0.1)
Mar 28 00:16:09.226 firewall kernel: 226 IP packet dropped
(24.66.81.36->firewall.mydomain.edu[10.0.0.1]: Protocol=TCP[SYN]
Port 2357->27374): Restricted Port: Protocol=TCP[SYN] Port 2357->27374
(received on interface 10.0.0.1) [1 duplicates suppressed]

Active Targeting?

Yes. The traffic from the source to the host interface of the Firewall.

History:

There was no other informations to support this detect.

Techniques:

The Firewall seems to be the main target. A SYN-TCP packet was sent to it. The time frame show that this was done at nighttime and over a relatively short period of time. The destination port of 27374/TCP was the target from an identical port of 2357/TCP!! This is very interesting in itself. The same source port brings some type of automation script that runs at the wee hours of the morning. The second trace, the "{ 1 duplicates was surpressed}" shows that this was the second attempt at the same destination port trying to exploit the same destination address.

Analysis/Intent:

This detect/trace seems to be an attempt to connect to a known exploit port, port 27374/UDP. This is a known vulnerability called Sub-7, or a very dangerous trojan horse. Though the log shows that the TCP port 27374 was the target, the 'known' sub-7 trojan horse actually uses UDP port 27374 and not TCP 27374?!?! This could have been a basic automated scan for the generic port and not realizing that the protocol is the key to the trojan horse. The exploit could have also been manipulated to work with TCP versus UDP. Though the potential exploit is extremely harmful, I wonder about the intent seeing this trace.

Identify Hostile Individuals and Groups?

This is another @home user. As the other detects I've analyzed, many detects have

been seen from multiple @home user accounts. The times would seem to justify this and I would take this potential scan seriously. I would take this to the next level!!

Components:	**Score:**	**Comments:**
Criticality:	4.5	The Firewall was the target here!!
Lethality:	2	Although the Firewall seems to have batten down this Attempt, I still worry!!
System Countermeasures:	4.5	I'm assuming that this system has been patched and hardended as much as possible.
Network Countermeasures:	4	Assuming backup is in place
Severity Total:	**-2**	**(Criticality + Lethality) – (System Countermeasures + Network countermeasures)**

Detect 9 Location: http://www.sans.org/y2k/032300.htm

Hi,

Some more proxy (ring zero?) scanning, this time out of china

Mar 23 02:50:58 beer kernel: Packet log: input DENY ppp0
PROTO=6 202.102.129.59:1719 139.130.12.177:3128
L=48 S=0x00 I=50768 F=0x4000 T=112 SYN (#18)
Mar 23 02:51:07 beer kernel: Packet log: input DENY ppp0
PROTO=6 202.102.129.59:1719 139.130.12.177:3128
L=48 S=0x00 I=12114 F=0x4000 T=112 SYN (#18)

Adam

Active Targeting?

Yes. We see traffic to the destination port of 3128 with the same destination address being targeted.

History:

There was no other information available with this detect.

Techniques:

The times are from early morning. Apart from that, this seems to be a Linux server being scanned. The ppp0 is an interface, such as running the ifconfig command and finding the ppp0 and le0 interfaces. The accept and deny are the way he has configured

the server to block or accept traffic. This does not seem to be a firewall per say. The SYN TCP (from the PROTO=6) packet has been targeted at the destination host of 139.130.12.177 and the same destination port of 3128. The source port was the same, 1719 as well as the source IP. As stated above, there was only the SYN and no other signs of a legitimate three-way communication session. This source IP was not a valid IP that was allowed to talk to the destination IP address and port. It was not internal communications between a DMZ and their internal network.

Analysis/Intent:

This detect was an active attempt to connect to a potentially dangerous port, port 3128/TCP. This port is known as a squid port and is defined in proxy ports. **Side note: I currently have a proxy port defined within my Netscape browser that communicates with the proxy server I have using standard proxy software. Though very quick and effective for allowing multiple users access over one pipe (I have cable modem), it is not the most secure set-up in the world. Beyond that, I should leave the details to the unknown. My point is that this could be a 'ring 0' attempt or the start of one. I would check out the system in question and do a through investigation of the server.

Identify Hostile Individuals and Groups?

Adam mentioned that this was from China. This alone should put up a red flag.
I would keep a close eye on the logs and try to filter the port 3128 and the source IP.
I would also keep in the back of my mind that the other ports that may be used to try to exploit the 'ring zero' phenomena are ports 80 and 8080. As I talked about in a earlier detect, port 8002 should be construed as another possible port with harmful intent.

Components:	**Score:**	**Comments:**
Criticality:	3	It does not seem to be a Firewall but a server of some sorts.
Lethality:	3	Potentially damaging port exploit\vulnerability.
System Countermeasures:	4	The server seems to have the latest Patches on OS.
Network Countermeasures:	4	Making an assumption that some type of backup is in place.
Severity Total:	-2	**(Criticality + Lethality) – (System Countermeasures + Network countermeasures)**

Detect 10 Location:

** Important: NDA is an Interliant Company just as my company is, Triumph Technologies, Inc. NDA is a Consulting company focusing on UNIX administration and support. All of Interliant's subsidiaries are on one mailing list. I received this e-mail shortly after the SANS conference in

Orlando. Although I find this interesting, the information is limited and was unable to acquire more to date. If interested in posting on the SANS site, please inform me so that I can make the e-mail as anonymous as possible for security reasons. I would appreciate some feedback on this for personal and professional reasons. Thanks!!

Ragu Nandan <ragu@nda.com> on 04/04/2000 01:30:58 PM

To: tech@nda.com
cc:
Subject: mail spoofing (contd)?

Hi,
I wan't to trace the origin of a mail spoofing attack. Based on the mail headers, I could see it is coming from a 38.29 net,
Is there a way to find out? Below are the
2 headers extracted from 2 such mails sent to the same person. Jabba is the external dns and mail relay.

1st header

Received: from edify.com (jabba.edify.com [209.220.16.10]) by eagle.edify.com with SMTP (Microsoft Exchange Internet Mail Service Version
5.5.2650.21)
id GYLQV9TH; Sun, 2 Apr 2000 12:26:07 -0700
Received: from neptune. (neptune-16.edify.com [209.220.16.2] (may be forged))
by edify.com (8.8.6/8.8.7) with SMTP id MAA06469;
Sun, 2 Apr 2000 12:14:26 -0700 (PDT)
From: cindy4@edify.com
Received: from servernt2.mulino.it ([38.29.117.70]) by servernt2.mulino.it
(Lotus SMTP MTA v4.6.3 (778.2 1-4-1999)) with SMTP id C12568B5.0062F874;
Sun, 2 Apr 2000 20:01:03 +0200
To: judd@AllThePlanet.com
Message-ID: <199903230437.EAA00485@alltheplanet.com>
Date: Sun, 02 Apr 00 10:05:25 EST
Subject:

2nd header

Received: from edify.com (jabba.edify.com [209.220.16.10]) by eagle.edify.com with SMTP (Microsoft Exchange Internet Mail Service

```
Version
5.5.2650.21)
        id GYLQVPNT; Wed, 29 Mar 2000 22:51:56 -0800
Received: from post.tcrz.net (post.tcrz.net [195.37.232.164])
        by edify.com (8.8.6/8.8.7) with ESMTP id WAA02848;
        Wed, 29 Mar 2000 22:40:03 -0800 (PST)
Message-Id: <200003300640.WAA02848@edify.com>
Received: from post.tcrz.net ([38.29.114.97]) by post.tcrz.net
         (Post.Office MTA v3.5.3 release 223 ID#
127-60884U4000L300S0V35)
         with SMTP id net; Thu, 30 Mar 2000 05:27:52 +0200
To: AllPlanet.de@edify.com
Date: Wed, 29 Mar 00 19:11:01 EST
From: hv@edify.com
Subject: hi
```

Active Targeting?

Yes. There is clear evidence of two-way communications between the source and destination servers.

History:

As far as I know, this is the first potential mail spoofing problems our companies have been exposed to. No other information to support this particular detects.

Techniques:

The source of the mail seems to be from 2 separate IP's, but both from the same network—a 38.29 network but from different hosts. The network is a class B network. Jabba.edify.com is the external dns and mail relay server. The neptune-16.edify.com, with an IP address of 209.220.16.2 is different from the valid jabba.edify.com dns server. The 2 headers seem to have the same process or tactic in place, but from different launching pads (servers).

Analysis/Intent:

My guess is that the 2 source IP's, 38.29.117.70 and 38.29.114.97 are from separate incidents. Not sure, but the same IP networks, but from different web servers from different parts of the world?! The first header shows that the source was from servernt2.mulino.net that connected to neptune-16.edify.com (ip of 209.220.16.2) which may not exist, but be a spoofed ip. The jabba.edify.com ip is really 209.220.16.10!!! I may have this completely wrong, but that is my guess. The second header as another picture. I find that the source is from 38.29.114.97is from post.tcrz.net. If you go to this web page, you will find that it is a page for the user to authenticate to view their local mail account. So my thought is that someone has to authenticate before logging on to use his or her particular e-mail account. Once in, they would be able to use this virtual e-mail server as a launching pad for some type of dubious activity. The IP of 195.37.232.164 which may be tzcr's external dns/e-mail server and the 38.29.114.97 is their internal e-mail server. The second header seems plausible. The first header seems like the scary one. The source IP is the 38.29.117.70 and the next hop seems directed

at the 'fake' server called neptune-16.edify.com with an IP of 209.220.16.2, which is on the same subnet of the 209.220.16.10 (the valid external mail and dns server).

Identify Hostile Individuals and Groups?

Note sure if this is a coordinated effort, but the separate ip's have used multiple Web servers to sent or spoof IP's to certain destination IP's. The servernt2.mulino.it is from Italy. They are a publishing company. Tcrz.net is, I believe, is a German site! It is some type of hosting and e-mail site. Whois showed me the following:
WHOIS information for tcrz.net:

Registrar:
NETWORK SOLUTIONS, INC.
Organization:
TeleConsult Dienstleistungs-GmbH
address: Roetzer Str. 12
, DE

Admin contact:
Hruby, Thomas
email:
thruba@HERRMANN.DE
phone:
+49 9971 880110
fax:
+49 9971 32381

Tech contact:
ruebezahl, hans
email:
teleconsult@SOFTHOME.NET
phone:
+49 9466 94060
fax:
+49 9466 940625

I find this startling and would have a hint of suspicion as to why this traffic has been targeted at jabba.edify.com's external mail and dns server. I would keep a close eye on the server and the traffic that traverses it.

Components:	**Score:**	**Comments:**
Criticality:	5	E-mail server and DNS servers are prized possessions.
Lethality:	4	I feel this may be a spoofed attempt and thus very dangerous.
System Countermeasures:	3	Not sure if they have anything in place to prevent IP spoofing.

		The ISP can put filters in place.
Network Countermeasures:	4	There is backup resolutions in place for down situations.
Severity Total:	**2**	**(Criticality + Lethality) – (System Countermeasures + Network countermeasures)**

****Sources of Information used throughout the analysis of the 10 detects:**

http://www.nttoolbox.com/
http://www.yahoo.com/ >> search engines
http://www.mygale.org/cdc/trojanh.htm
http://www.robertgraham.com/pubs/firewall-seen.html#subseven
http://linux-firewall-tools.com/linux/ports.html
http://vil.mcafee.com/dispVirus.asp?virus_k=10171
http://vil.mcafee.com/dispVirus.asp?virus_k=10171
http://www.progenic.com/t100/
http://www.hildrum.com/ports.htm
http://www.pspl.com/trojan_info/win32/happy99.htm
http://www.ltsw.se/knbase/tcp/tcp1.htp
http://www2.merton.ox.ac.uk/~security/bugtraq-199812/0229.html
http://www.securityfocus.com/bid/701.html
http://advice.networkice.com/advice/Exploits/Ports/ >> A great resource!!
http://advice.networkice.com/advice/Exploits/Ports/138/default.htm
http://www.mulino.it/frame6.htm
http://www.mulino.it/index2.htm
www.tcrz.net/
http://post.tcrz.net:81/