Global Information Assurance Certification Paper

***** Name added by Northcutt, could expand history and severity, several chances for great research here. Format was very readable in the original, write ups are accurate and concise. This is a second submittal. 80 S. *****

Roger Bleess

All of the following logs are from our Cisco PIX Firewall. All IP information has been altered to protect all parties. I find that analysis is difficult with PIX logs. The amount of information contained in each entry is not as complete as logs from other products. This is currently my only source of information. I will utilize these analyses to strengthen our defenses.

Detect 1:

<130>Nov 06 1999 11:37:07: %PIX-2-106006: Deny inbound UDP from s.s.s.71/60000 to d.d.d.5/2140

<130>Nov 06 1999 11:37:07: %PIX-2-106006: Deny inbound UDP from s.s.s.71/60000 to d.d.d.4/2140

<130>Nov 06 1999 11:37:07: %PIX-2-106006: Deny inbound UDP from s.s.s.71/60000 to d.d.d.13/2140

<130>Nov 06 1999 11:37:07: %PIX-2-106006: Deny inbound UDP from s.s.s.71/60000 to d.d.d.10/2140

<130>Nov 06 1999 11:37:07: %PIX-2-106006: Deny inbound UDP from s.s.s.71/60000 to d.d.d.20/2140

<130>Nov 06 1999 11:37:07: %PIX-2-106006: Deny inbound UDP from s.s.s.71/60000 to d.d.d.96/2140

Analysis: This active scan is looking for hosts that are running the Deep Throat or The Invasor Trojans. It repeated the exact same sequence almost 3 hours later. This is definitely malicious in nature, but was successfully blocked.

Detect 2:

<130>Feb 29 2000 10:57:28: %PIX-2-106006: Deny inbound UDP from s.s.s.147/63209 to d.d.1.96/135

<130>Feb 29 2000 10:57:29: %PIX-2-106006: Deny inbound UDP from s.s.s.147/63209 to d.d.1.96/135

<130>Feb 29 2000 10:57:30: %PIX-2-106006: Deny inbound UDP from s.s.s.147/63209 to d.d.1.96/135

<130>Feb 29 2000 10:57:30: %PIX-2-106001: Inbound TCP connection denied from s.s.s.147/63365 to d.d.1.96/1028 flags SYN

<130>Feb 29 2000 10:57:31: %PIX-2-106006: Deny inbound UDP from s.s.s.147/63209 to d.d.1.96/135

Analysis: What caught my eye and ignited my curiosity was the single TCP attempt at a connection intermingled with the epmap program in the UDP traffic. There is no known exploit or vulnerability with port 1028 that I have been able to find. We could possibly have the makings of a new exploit, vulnerability, or Trojan.

Detect 3:

<130>Mar 05 1999 13:11:17: %PIX-2-106007: Deny inbound UDP from s1.s1.s1.22/1 to d.d.1.78/1597 due to DNS Response

<130>Mar 05 1999 13:11:19: %PIX-2-106001: Inbound TCP connection denied from s2.s2.s2.70/4473 to d.d.1.5/113 flags SYN

<130>Mar 05 1999 13:11:29: %PIX-2-106001: Inbound TCP connection denied from s1.s1.s1.70/4473 to d.d.1.5/113 flags SYN

<130>Mar 05 1999 13:19:47: %PIX-2-106007: Deny inbound UDP from s2.s2.s2.22/1 to d.d.1.78/1631 due to DNS Response

Analysis: Anomalous traffic from source port 1, possibly a slow port scan. It is intertwined but probably not related to an attempt by a second source on port 113 which is known for the Kazimas Trojan.

Detect 4:

<130>Mar 04 2000 18:22:52: %PIX-2-106001: Inbound TCP connection denied from s.s.s.18/1558 to d.d.1.5/8080 flags SYN

<130>Mar 04 2000 18:22:52: %PIX-2-106001: Inbound TCP connection denied from s.s.s.18/1559 to d.d.1.5/3128 flags SYN

<130>Mar 04 2000 18:22:53: %PIX-2-106001: Inbound TCP connection denied from s.s.s.18/1561 to d.d.1.13/3128 flags SYN

<130>Mar 04 2000 18:22:53: %PIX-2-106001: Inbound TCP connection denied from s.s.s.18/1560 to d.d.1.13/8080 flags SYN

<130>Mar 04 2000 18:22:53: %PIX-2-106001: Inbound TCP connection denied from s.s.s.18/1564 to d.d.1.4/8080 flags SYN

<130>Mar 04 2000 18:22:53: %PIX-2-106001: Inbound TCP connection denied from s.s.s.18/1565 to d.d.1.4/3128 flags SYN

<130>Mar 04 2000 18:22:53: %PIX-2-106001: Inbound TCP connection denied from s.s.s.18/1566 to d.d.1.96/8080 flags SYN

<130>Mar 04 2000 18:22:53: %PIX-2-106001: Inbound TCP connection denied from s.s.s.18/1568 to d.d.1.96/3128 flags SYN

<130>Mar 04 2000 18:22:53: %PIX-2-106001: Inbound TCP connection denied from s.s.s.18/1571 to d.d.1.7/8080 flags SYN

<130>Mar 04 2000 18:22:53: %PIX-2-106001: Inbound TCP connection denied from s.s.s.18/1572 to d.d.1.7/3128 flags SYN

<130>Mar 04 2000 18:22:53: %PIX-2-106001: Inbound TCP connection denied from s.s.s.18/1575 to d.d.1.82/8080 flags SYN

<130>Mar 04 2000 18:22:53: %PIX-2-106001: Inbound TCP connection denied from s.s.s.18/1576 to d.d.1.82/3128 flags SYN

<130>Mar 04 2000 18:22:53: %PIX-2-106001: Inbound TCP connection denied from s.s.s.18/1577 to d.d.1.10/8080 flags SYN

<130>Mar 04 2000 18:22:53: %PIX-2-106001: Inbound TCP connection denied from s.s.s.18/1578 to d.d.1.10/3128 flags SYN

<130>Mar 04 2000 18:22:54: %PIX-2-106001: Inbound TCP connection denied from s.s.s.18/1597 to d.d.10.20/8080 flags SYN

<130>Mar 04 2000 18:22:54: %PIX-2-106001: Inbound TCP connection denied from s.s.s.18/1598 to d.d.10.20/3128 flags SYN

<130>Mar 04 2000 18:22:54: %PIX-2-106001: Inbound TCP connection denied from s.s.s.18/1599 to d.d.10.21/8080 flags SYN

<130>Mar 04 2000 18:22:54: %PIX-2-106001: Inbound TCP connection denied from s.s.s.18/1600 to d.d.10.21/3128 flags SYN

<130>Mar 04 2000 18:22:55: %PIX-2-106001: Inbound TCP connection denied from s.s.s.18/1673 to d.d.1.250/8080 flags SYN

<130>Mar 04 2000 18:22:55: %PIX-2-106001: Inbound TCP connection denied from s.s.s.18/1674 to d.d.1.250/3128 flags SYN

Analysis: Here we have what looks to be the infamous Ring Zero Trojan. This is very automated as the time stamps and incrementing source ports indicate. It is interesting that the scan did not include hits on port 80 and that it hit multiple destinations in different subnets in a 2 second window. In the IDIC course we learned that Ring Zero appeared to be somewhat random in its scans and seldom hit more than one machine in a network. This appears to be more targeted.

Detect 5:

<130>Jan 07 2000 19:31:38: %PIX-2-106001: Inbound TCP connection denied from s.s.s.65/2779 to d.d.d.20/25 flags SYN

<130>Jan 07 2000 20:09:57: %PIX-2-106001: Inbound TCP connection denied from s.s.s.65/4196 to d.d.d.20/25 flags SYN

<130>Jan 07 2000 20:10:03: %PIX-2-106001: Inbound TCP connection denied from s.s.s.65/4196 to d.d.d.20/25 flags SYN

<130>Jan 07 2000 20:10:15: %PIX-2-106001: Inbound TCP connection denied from s.s.s.65/4196 to d.d.d.20/25 flags SYN

<130>Jan 07 2000 20:22:40: %PIX-2-106001: Inbound TCP connection denied from s.s.s.65/4661 to d.d.d.20/25 flags SYN

<130>Jan 07 2000 20:22:43: %PIX-2-106001: Inbound TCP connection denied from s.s.s.65/4661 to d.d.d.20/25 flags SYN

<130>Jan 07 2000 20:22:49: %PIX-2-106001: Inbound TCP connection denied from s.s.s.65/4661 to d.d.d.20/25 flags SYN

<130>Jan 07 2000 20:23:01: %PIX-2-106001: Inbound TCP connection denied from s.s.s.65/4661 to d.d.d.20/25 flags SYN

<130>Jan 07 2000 20:35:21: %PIX-2-106001: Inbound TCP connection denied from s.s.s.65/1169 to d.d.d.20/25 flags SYN

<130>Jan 07 2000 20:35:23: %PIX-2-106001: Inbound TCP connection denied from s.s.s.65/1169 to d.d.d.20/25 flags SYN

<130>Jan 07 2000 20:35:29: %PIX-2-106001: Inbound TCP connection denied from s.s.s.65/1169 to d.d.d.20/25 flags SYN

<130>Jan 07 2000 20:35:41: %PIX-2-106001: Inbound TCP connection denied from s.s.s.65/1169 to d.d.d.20/25 flags SYN

Analysis: Multiple attempts by an outside Mail server to make an SMTP connection to a web server. This looks suspicious so additional capturing and filtering on this type of connection is required before this can be ruled Hostile or Friendly. There is just not enough information at this point to make a proper analysis.

Detect 6:

<130>Jan 07 2000 20:36:39: %PIX-2-106007: Deny inbound UDP from s.s.s.13/0 to d.d.d.5/53 due to DNS Query

<130>Jan 07 2000 20:36:39: %PIX-2-106007: Deny inbound UDP from s.s.s.13/256 to d.d.d.5/53 due to DNS Query

<130>Jan 07 2000 20:36:39: %PIX-2-106007: Deny inbound UDP from s.s.s.13/512 to d.d.d.5/53 due to DNS Query

<130>Jan 07 2000 20:36:54: %PIX-2-106001: Inbound TCP connection denied from s.s.s.13/2900 to d.d.d.5/53 flags SYN

<130>Jan 07 2000 20:36:54: %PIX-2-106001: Inbound TCP connection denied from s.s.s.13/2901 to d.d.d.5/53 flags SYN

<130>Jan 07 2000 20:36:54: %PIX-2-106001: Inbound TCP connection denied from s.s.s.13/2902 to d.d.d.5/53 flags SYN

Analysis: DNS port probe from different source ports. Use of a reserved UDP port (0) in itself is anomalous and (512) is the biff program, which should not be visible on the Internet because it should be bound to 127.0.0.1. Looks to be two automated process. One concentrates on UDP while the other is utilizing TCP. Source address is of a Name Server that could quite possibly be compromised.

Detect 7:

<130>Jan 21 2000 05:07:57: %PIX-2-106006: Deny inbound UDP from s.s.s.104/1043 to d.d.d.33/161

<130>Jan 21 2000 05:08:04: %PIX-2-106006: Deny inbound UDP from s.s.s.104/1043 to d.d.d.20/161

<130>Jan 21 2000 05:08:04: %PIX-2-106006: Deny inbound UDP from s.s.s.104/1043 to d.d.d.5/161

<130>Jan 21 2000 05:08:04: %PIX-2-106006: Deny inbound UDP from s.s.s.104/1043 to d.d.d.10/161

<130>Jan 21 2000 05:08:04: %PIX-2-106006: Deny inbound UDP from s.s.s.104/1043 to d.d.d.13/161

<130>Jan 21 2000 05:08:04: %PIX-2-106006: Deny inbound UDP from s.s.s.104/1043 to d.d.d.21/161

<130>Jan 21 2000 05:08:04: %PIX-2-106006: Deny inbound UDP from s.s.s.104/1043 to d.d.d.96/161

<130>Jan 21 2000 05:08:04: %PIX-2-106006: Deny inbound UDP from s.s.s.104/1043 to d.d.d.4/161

Analysis: Port 161 UDP is the default encapsulation for SMTP. This appears to be host scanning to see if a host running this protocol is available. It also looks like this scan may be part of a much broader Class B scan. It is definitely automated and malicious in intent.

Detect 8:

<130>Mar 03 2000 05:52:50: %PIX-2-106001: Inbound TCP connection denied from s.s.s.141/1025 to d.d.1.4/111 flags SYN

<130>Mar 03 2000 05:52:51: %PIX-2-106001: Inbound TCP connection denied from s.s.s.141/1026 to d.d.1.96/111 flags SYN

<130>Mar 03 2000 05:52:51: %PIX-2-106001: Inbound TCP connection denied from s.s.s.141/1030 to d.d.1.82/111 flags SYN

<130>Mar 03 2000 05:52:51: %PIX-2-106001: Inbound TCP connection denied from s.s.s.141/1042 to d.d.10.21/111 flags SYN

<130>Mar 03 2000 05:52:52: %PIX-2-106001: Inbound TCP connection denied from s.s.s.141/1079 to d.d.1.250/111 flags SYN

<130>Mar 03 2000 05:52:53: %PIX-2-106001: Inbound TCP connection denied from s.s.s.141/4998 to d.d.1.5/111 flags SYN

<130>Mar 03 2000 05:52:53: %PIX-2-106001: Inbound TCP connection denied from s.s.s.141/4999 to d.d.1.13/111 flags SYN

<130>Mar 03 2000 05:52:53: %PIX-2-106001: Inbound TCP connection denied from s.s.s.141/1025 to d.d.1.4/111 flags SYN

<130>Mar 03 2000 05:52:54: %PIX-2-106001: Inbound TCP connection denied from s.s.s.141/1026 to d.d.1.96/111 flags SYN

<130>Mar 03 2000 05:52:54: %PIX-2-106001: Inbound TCP connection denied from s.s.s.141/1030 to d.d.1.82/111 flags SYN

<130>Mar 03 2000 05:52:54: %PIX-2-106001: Inbound TCP connection denied from s.s.s.141/1041 to d.d.10.20/111 flags SYN

<130>Mar 03 2000 05:52:54: %PIX-2-106001: Inbound TCP connection denied from s.s.s.141/1042 to d.d.10.21/111 flags SYN

<130>Mar 03 2000 05:52:54: %PIX-2-106001: Inbound TCP connection denied from s.s.s.141/1028 to d.d.1.7/111 flags SYN

<130>Mar 03 2000 05:52:54: %PIX-2-106001: Inbound TCP connection denied from s.s.s.141/1031 to d.d.1.10/111 flags SYN

Analysis: A quick, automated, and direct sunrpc scan on our subnet. Interesting twist in the source ports in that primarily the 1000 series is used but there is also the use of 4998 and 4999. This appears to be a scan for active unix hosts running this very dangerous rpc service.

Detect 9:

<130>Feb 27 1999 20:23:43: %PIX-2-106001: Inbound TCP connection denied from s.s.s.20/5 to d.d.d.5/53 flags SYN

<130>Feb 27 1999 20:23:43: %PIX-2-106001: Inbound TCP connection denied from s.s.s.20/7 to d.d.d.5/53 flags SYN

<130>Feb 27 1999 20:23:43: %PIX-2-106001: Inbound TCP connection denied from s.s.s.20/6 to d.d.d.5/53 flags SYN

Analysis: This attempted connection to our DNS service came from very low source ports in sequence in a short period of time. The use of the echo port (7) is to elicit an echo reply. Source port 5 was once intended for fingerprinting but really is not used in practice. This is definitely a targeted attack to perform reconnaissance.

Detect 10:

<130>Mar 06 1999 20:37:14: %PIX-2-106001: Inbound TCP connection denied from s.s.s.6/20 to d.d.d.103/1230 flags SYN

<130>Mar 06 1999 20:37:26: %PIX-2-106001: Inbound TCP connection denied from s.s.s.6/20 to d.d.d.103/1230 flags SYN

Analysis: This trace shows an attempted ftp data transfer into our network. Amazingly there was no trace of a port 21 request going out. This occurred at 8:30 PM which does not rule out someone being in the office trying to open an ftp session. Fortunately, our PIX is setup to block this inbound traffic. Follow up to ensure outgoing logging is operating properly is required.
