Global Information Assurance Certification Paper

*** Northcutt, good work, got his own detects and has an obvious "home field" advantage and it shows. Good use of an analysis process. Evidence of research. 86 ***

GIAC Practical for SANS 2000

Tony Gillespie

All of the following detects were taken from our Cisco syslogs. We have a very restrictive access list and are running the Cisco Firewall feature set. I have masked our Network IP addresses, but kept the host IP. All source IP addresses have been kept as the original. Unfortunately the only information I am able to supply is from our access list syslog. Due to internal constraints I am unable to capture the packets to examine them.

You will notice that all of my severity measures are negative numbers. I came up with this primarily because of the following information:

Our network uses NAT translation; therefore there are only a few hosts visible to the network.
We use Cisco access-lists to deny most traffic and use the Firewall feature set
The systems that are visible to the internet have the latest patches
We do not have a web server
Most of the detects were to hosts that do not exist on our network.
Since the host doesn't exist likelihood to succeed is minimal

DETECT # 1

Existence — Someone using IP addresses 206.251.19.80, 88, and 89 which are registered to Global Crossing, 1111 Karlstad Drive, Sunnyvale, CA 94089, has been targeting a single host on our network.

History — The history spans back to 3 Feb 2000. Starting on 3 Feb someone from one of these IP addresses started trying to do DNS zone transfers. This continues until 12 Mar, when all of a sudden they start mixing zone transfers with traceroutes. I checked with AFCERT and this IP was reported to them from multiple sites as attempting DNS zone transfers.

Techniques — The source IP addresses are always 80, 88 or 89 and the source ports are always in the 2000's but don't always increment.

Intent — Person is trying to receive a DNS zone transfer.

Targeting — There are absolutely no other denials from this network. This seems to be targeted specifically to our DNS server.

Severity **-4** = (Criticality **5** + Lethality **1**) **-** (Sys CtrMeasures **5** + Network Ctrmeasures **5**)

Analysis — This caught my eye initially because it has gone on over a long period of time (2 months now) and has only targeted a single system. Most of these detects were during non duty times for Eastern Standard Time, even taking into account that the accounts were from CA would indicate late night activity on the West coast. The source ports are always in the 2000's. The odds of this happening have got to be pretty slim, especially the same port numbers consistently showing up. This appears to be an attempt to get a DNS zone transfer. **Note that Eric Brock also detected some of this activity in his Detects. I noticed that Stephen Northcutt has suggested that this is probably load balancing. I wouldn't think that load balancing would go on for such a long period of time, but Stephen is the expert. I provided the full history of this since Eric stated his just showed up in late March.**

```
udp  206.251.19.89(2401) ->  ?.?.?.251(53),    Feb  3    08:59:39:  1  packet
tcp  206.251.19.89(2401) ->  ?.?.?.251(53),    Feb  3    09:00:09:  1  packet
udp  206.251.19.88(2200) ->  ?.?.?.251(53),    Feb  3    09:29:14:  1  packet
tcp  206.251.19.88(2200) ->  ?.?.?.251(53),    Feb  3    09:30:14:  1  packet
udp  206.251.19.89(2201) ->  ?.?.?.251(53),    Feb  11   19:13:14:  1  packet
tcp  206.251.19.89(2202) ->  ?.?.?.251(53),    Feb  11   19:14:04:  1  packet
udp  206.251.19.88(2100) ->  ?.?.?.251(53),    Feb  11   19:41:47:  1  packet
tcp  206.251.19.88(2100) ->  ?.?.?.251(53),    Feb  11   19:42:27:  1  packet
udp  206.251.19.89(2400) ->  ?.?.?.251(53),    Feb  11   20:39:16:  1  packet
tcp  206.251.19.89(2400) ->  ?.?.?.251(53),    Feb  11   20:40:06:  1  packet
udp  206.251.19.80(2100) ->  ?.?.?.251(53),    Feb  11   21:19:06:  1  packet
tcp  206.251.19.80(2100) ->  ?.?.?.251(53),    Feb  11   21:19:56:  1  packet
udp  206.251.19.88(2000) ->  ?.?.?.251(53),    Feb  16   02:07:49:  1  packet
tcp  206.251.19.88(2000) ->  ?.?.?.251(53),    Feb  16   02:07:59:  1  packet
udp  206.251.19.88(2000) ->  ?.?.?.251(53),    Feb  16   02:37:20:  1  packet
tcp  206.251.19.88(2000) ->  ?.?.?.251(53),    Feb  16   02:38:00:  1  packet
udp  206.251.19.88(2200) ->  ?.?.?.251(53),    Feb  16   02:44:13:  1  packet
tcp  206.251.19.88(2201) ->  ?.?.?.251(53),    Feb  16   02:44:53:  1  packet
udp  206.251.19.80(2100) ->  ?.?.?.251(53),    Feb  16   02:49:00:  1  packet
tcp  206.251.19.80(2100) ->  ?.?.?.251(53),    Feb  16   02:49:21:  1  packet
udp  206.251.19.88(2300) ->  ?.?.?.251(53),    Feb  16   03:04:27:  1  packet
```

```
tcp  206.251.19.88(2301) ->  ?.?.?.251(53),          Feb  16        03:05:07:  1  packet
udp  206.251.19.80(2201) ->  ?.?.?.251(53),          Feb  28        12:03:56:  1  packet
tcp  206.251.19.80(2200) ->  ?.?.?.251(53),          Feb  28        12:04:36:  1  packet
udp  206.251.19.80(2400) ->  ?.?.?.251(53),          Feb  28        12:46:55:  1  packet
tcp  206.251.19.80(2400) ->  ?.?.?.251(53),          Feb  28        12:47:15:  1  packet
udp  206.251.19.89(2101) ->  ?.?.?.251(53),          Feb  28        13:32:05:  1  packet
tcp  206.251.19.89(2100) ->  ?.?.?.251(53),          Feb  28        13:32:25:  1  packet
udp  206.251.19.88(2000) ->  ?.?.?.251(53),          Feb  29        08:36:18:  1  packet
tcp  206.251.19.88(2000) ->  ?.?.?.251(53),          Feb  29        08:36:38:  1  packet
udp  206.251.19.80(2200) ->  ?.?.?.251(53),          Feb  29        08:53:18:  1  packet
tcp  206.251.19.80(2202) ->  ?.?.?.251(53),          Feb  29        08:53:38:  1  packet
udp  206.251.19.89(2001) ->  ?.?.?.251(53),          Feb  29        10:15:32:  1  packet
tcp  206.251.19.89(2000) ->  ?.?.?.251(53),          Feb  29        10:16:22:  1  packet
udp  206.251.19.80(2000) ->  ?.?.?.251(53),          Mar  4         07:00:00:  1  packet
tcp  206.251.19.80(2000) ->  ?.?.?.251(53),          Mar  4         07:00:30:  1  packet
tcp  206.251.19.80(2200) ->  ?.?.?.251(53),          Mar  4         08:12:48:  1  packet
udp  206.251.19.80(2300) ->  ?.?.?.251(53),          Mar  4         11:20:17:  1  packet
tcp  206.251.19.80(2300) ->  ?.?.?.251(53),          Mar  4         11:20:38:  1  packet
udp  206.251.19.80(2000) ->  ?.?.?.251(53),          Mar  4         11:25:14:  1  packet
tcp  206.251.19.80(2000) ->  ?.?.?.251(53),          Mar  4         11:25:44:  1  packet
udp  206.251.19.89(2301) ->  ?.?.?.251(53),          Mar  9         14:59:08:  1  packet
tcp  206.251.19.89(2300) ->  ?.?.?.251(53),          Mar  9         14:59:48:  1  packet
udp  206.251.19.88(2102) ->  ?.?.?.251(53),          Mar  9         15:05:27:  1  packet
udp  206.251.19.89(2101) ->  ?.?.?.251(53),          Mar  9         15:14:36:  1  packet
tcp  206.251.19.89(2102) ->  ?.?.?.251(53),          Mar  9         15:16:06:  1  packet
udp  206.251.19.89(2301) ->  ?.?.?.251(53),          Mar  9         15:28:30:  1  packet
tcp  206.251.19.89(2301) ->  ?.?.?.251(53),          Mar  9         15:29:10:  1  packet
udp  206.251.19.88(2821) ->  ?.?.?.251(33434),       Mar  12        03:17:21:  1  packet
udp  206.251.19.88(2822) ->  ?.?.?.251(33434),       Mar  12        03:17:22:  1  packet
udp  206.251.19.80(2201) ->  ?.?.?.251(53),          Mar  12        03:18:30:  1  packet
udp  206.251.19.88(2821) ->  ?.?.?.251(33434),       Mar  12        03:18:36:  1  packet
tcp  206.251.19.80(2200) ->  ?.?.?.251(53),          Mar  12        03:18:50:  1  packet
udp  206.251.19.88(2819) ->  ?.?.?.251(33434),       Mar  12        03:19:42:  1  packet
udp  206.251.19.88(2822) ->  ?.?.?.251(33434),       Mar  12        03:19:44:  1  packet
udp  206.251.19.88(2821) ->  ?.?.?.251(33434),       Mar  12        03:19:55:  1  packet
udp  206.251.19.80(2719) ->  ?.?.?.251(33434),       Mar  12        03:20:51:  1  packet
udp  206.251.19.80(2720) ->  ?.?.?.251(33434),       Mar  12        03:20:52:  1  packet
udp  206.251.19.80(2721) ->  ?.?.?.251(33434),       Mar  12        03:20:53:  1  packet
udp  206.251.19.80(2722) ->  ?.?.?.251(33434),       Mar  12        03:20:54:  1  packet
udp  206.251.19.80(2723) ->  ?.?.?.251(33434),       Mar  12        03:20:55:  1  packet
udp  206.251.19.88(2819) ->  ?.?.?.251(33434),       Mar  12        03:22:32:  1  packet
udp  206.251.19.88(2820) ->  ?.?.?.251(33434),       Mar  12        03:22:34:  1  packet
udp  206.251.19.88(2821) ->  ?.?.?.251(33434),       Mar  12        03:22:35:  1  packet
udp  206.251.19.88(2822) ->  ?.?.?.251(33434),       Mar  12        03:22:37:  1  packet
udp  206.251.19.89(2819) ->  ?.?.?.251(33434),       Mar  12        03:24:59:  1  packet
udp  206.251.19.89(2820) ->  ?.?.?.251(33434),       Mar  12        03:25:00:  1  packet
udp  206.251.19.89(2821) ->  ?.?.?.251(33434),       Mar  12        03:25:01:  1  packet
udp  206.251.19.89(2822) ->  ?.?.?.251(33434),       Mar  12        03:25:02:  1  packet
udp  206.251.19.89(2823) ->  ?.?.?.251(33434),       Mar  12        03:27:17:  1  packet
udp  206.251.19.88(2819) ->  ?.?.?.251(33434),       Mar  12        03:27:20:  1  packet
udp  206.251.19.88(2821) ->  ?.?.?.251(33434),       Mar  12        03:27:50:  1  packet
```

```
udp  206.251.19.89(2820) ->  ?.?.?.251(33434),     Mar  12        03:30:07:  4  packets
udp  206.251.19.89(2820) ->  ?.?.?.251(33434),     Mar  12        03:32:34:  1  packet
udp  206.251.19.89(2819) ->  ?.?.?.251(33434),     Mar  12        03:33:16:  1  packet
udp  206.251.19.89(2820) ->  ?.?.?.251(33434),     Mar  12        03:33:17:  1  packet
udp  206.251.19.89(2821) ->  ?.?.?.251(33434),     Mar  12        03:33:18:  1  packet
udp  206.251.19.89(2822) ->  ?.?.?.251(33434),     Mar  12        03:33:19:  1  packet
udp  206.251.19.88(2819) ->  ?.?.?.251(33434),     Mar  12        03:36:35:  1  packet
udp  206.251.19.88(2820) ->  ?.?.?.251(33434),     Mar  12        03:36:36:  1  packet
udp  206.251.19.88(2821) ->  ?.?.?.251(33434),     Mar  12        03:36:38:  1  packet
udp  206.251.19.88(2822) ->  ?.?.?.251(33434),     Mar  12        03:36:40:  1  packet
udp  206.251.19.88(2819) ->  ?.?.?.251(33434),     Mar  12        03:37:14:  1  packet
udp  206.251.19.88(2820) ->  ?.?.?.251(33434),     Mar  12        03:37:16:  1  packet
udp  206.251.19.88(2400) ->  ?.?.?.251(53),        Mar  12        03:37:36:  1  packet
tcp  206.251.19.88(2400) ->  ?.?.?.251(53),        Mar  12        03:37:56:  1  packet
udp  206.251.19.89(2101) ->  ?.?.?.251(53),        Mar  12        03:41:36:  1  packet
tcp  206.251.19.89(2100) ->  ?.?.?.251(53),        Mar  12        03:42:06:  1  packet
udp  206.251.19.88(2300) ->  ?.?.?.251(53),        Mar  12        03:52:17:  1  packet
udp  206.251.19.89(2300) ->  ?.?.?.251(53),        Mar  12        03:52:36:  1  packet
tcp  206.251.19.89(2301) ->  ?.?.?.251(53),        Mar  12        03:52:46:  1  packet
udp  206.251.19.88(2819) ->  ?.?.?.251(33434),     Mar  12        23:23:22:  1  packet
udp  206.251.19.88(2820) ->  ?.?.?.251(33434),     Mar  12        23:23:23:  1  packet
udp  206.251.19.88(2821) ->  ?.?.?.251(33434),     Mar  12        23:23:24:  1  packet
udp  206.251.19.88(2822) ->  ?.?.?.251(33434),     Mar  12        23:23:25:  1  packet
udp  206.251.19.89(2823) ->  ?.?.?.251(33434),     Mar  12        23:24:06:  1  packet
udp  206.251.19.89(2819) ->  ?.?.?.251(33434),     Mar  12        23:25:19:  1  packet
udp  206.251.19.89(2820) ->  ?.?.?.251(33434),     Mar  12        23:25:20:  1  packet
udp  206.251.19.80(2719) ->  ?.?.?.251(33434),     Mar  12        23:29:19:  1  packet
udp  206.251.19.80(2720) ->  ?.?.?.251(33434),     Mar  12        23:29:20:  1  packet
udp  206.251.19.89(2819) ->  ?.?.?.251(33434),     Mar  12        23:29:21:  2  packets
udp  206.251.19.89(2820) ->  ?.?.?.251(33434),     Mar  12        23:29:23:  2  packets
udp  206.251.19.89(2821) ->  ?.?.?.251(33434),     Mar  12        23:29:27:  3  packets
udp  206.251.19.89(2822) ->  ?.?.?.251(33434),     Mar  12        23:29:28:  3  packets
udp  206.251.19.89(2100) ->  ?.?.?.251(53),        Mar  12        23:31:53:  1  packet
tcp  206.251.19.89(2101) ->  ?.?.?.251(53),        Mar  12        23:32:23:  1  packet
udp  206.251.19.80(2719) ->  ?.?.?.251(33434),     Mar  12        23:33:21:  1  packet
udp  206.251.19.80(2720) ->  ?.?.?.251(33434),     Mar  12        23:33:22:  1  packet
udp  206.251.19.80(2721) ->  ?.?.?.251(33434),     Mar  12        23:33:24:  1  packet
udp  206.251.19.80(2722) ->  ?.?.?.251(33434),     Mar  12        23:33:25:  1  packet
udp  206.251.19.80(2719) ->  ?.?.?.251(33434),     Mar  12        23:50:12:  1  packet
udp  206.251.19.80(2720) ->  ?.?.?.251(33434),     Mar  12        23:50:13:  1  packet
udp  206.251.19.80(2721) ->  ?.?.?.251(33434),     Mar  12        23:50:14:  1  packet
udp  206.251.19.80(2722) ->  ?.?.?.251(33434),     Mar  12        23:50:15:  1  packet
udp  206.251.19.88(2821) ->  ?.?.?.251(33434),     Mar  12        23:50:17:  1  packet
udp  206.251.19.88(2822) ->  ?.?.?.251(33434),     Mar  12        23:50:18:  1  packet
udp  206.251.19.80(2400) ->  ?.?.?.251(53),        Mar  12        23:53:09:  1  packet
tcp  206.251.19.80(2400) ->  ?.?.?.251(53),        Mar  12        23:53:29:  1  packet
udp  206.251.19.88(2401) ->  ?.?.?.251(53),        Mar  13        00:16:36:  1  packet
tcp  206.251.19.88(2400) ->  ?.?.?.251(53),        Mar  13        00:16:56:  1  packet
udp  206.251.19.89(2300) ->  ?.?.?.251(53),        Mar  13        00:26:02:  1  packet
tcp  206.251.19.89(2300) ->  ?.?.?.251(53),        Mar  13        00:26:32:  1  packet
tcp  206.251.19.89(2002) ->  ?.?.?.251(53),        Mar  13        12:00:47:  1  packet
```

```
udp  206.251.19.89(2100) ->  ?.?.?.251(53),          Mar  14        09:25:58:  1  packet
tcp  206.251.19.89(2101) ->  ?.?.?.251(53),          Mar  14        09:26:49:  1  packet
udp  206.251.19.88(2000) ->  ?.?.?.251(53),          Mar  15        03:19:41:  1  packet
tcp  206.251.19.88(2001) ->  ?.?.?.251(53),          Mar  15        03:20:11:  1  packet
udp  206.251.19.88(2000) ->  ?.?.?.251(53),          Mar  15        03:50:34:  1  packet
tcp  206.251.19.88(2000) ->  ?.?.?.251(53),          Mar  15        03:50:53:  1  packet
udp  206.251.19.80(2100) ->  ?.?.?.251(53),          Mar  15        04:36:15:  1  packet
tcp  206.251.19.80(2100) ->  ?.?.?.251(53),          Mar  15        04:36:25:  1  packet
udp  206.251.19.80(2300) ->  ?.?.?.251(53),          Mar  16        03:24:13:  1  packet
tcp  206.251.19.80(2300) ->  ?.?.?.251(53),          Mar  16        03:24:43:  1  packet
udp  206.251.19.88(2000) ->  ?.?.?.251(53),          Mar  16        03:55:07:  1  packet
tcp  206.251.19.88(2000) ->  ?.?.?.251(53),          Mar  16        03:55:27:  1  packet
udp  206.251.19.88(2001) ->  ?.?.?.251(53),          Mar  16        04:07:09:  1  packet
tcp  206.251.19.88(2000) ->  ?.?.?.251(53),          Mar  16        04:07:39:  1  packet
tcp  206.251.19.89(2400) ->  ?.?.?.251(53),          Mar  16        04:09:39:  1  packet
udp  206.251.19.89(2201) ->  ?.?.?.251(53),          Mar  16        04:44:11:  1  packet
tcp  206.251.19.89(2200) ->  ?.?.?.251(53),          Mar  16        04:44:51:  1  packet
udp  206.251.19.80(2101) ->  ?.?.?.251(53),          Mar  16        06:53:38:  1  packet
tcp  206.251.19.80(2100) ->  ?.?.?.251(53),          Mar  16        06:54:29:  1  packet
udp  206.251.19.80(2002) ->  ?.?.?.251(53),          Mar  16        23:49:02:  1  packet
tcp  206.251.19.80(2001) ->  ?.?.?.251(53),          Mar  16        23:49:12:  1  packet
udp  206.251.19.89(2000) ->  ?.?.?.251(53),          Mar  17        00:30:23:  1  packet
tcp  206.251.19.89(2001) ->  ?.?.?.251(53),          Mar  17        00:30:43:  1  packet
udp  206.251.19.80(2001) ->  ?.?.?.251(53),          Mar  17        00:41:46:  1  packet
tcp  206.251.19.80(2000) ->  ?.?.?.251(53),          Mar  17        00:42:06:  1  packet
udp  206.251.19.88(2814) ->  ?.?.?.251(33434),       Mar  20        05:21:09:  1  packet
udp  206.251.19.88(2815) ->  ?.?.?.251(33434),       Mar  20        05:21:11:  1  packet
udp  206.251.19.88(2816) ->  ?.?.?.251(33434),       Mar  20        05:21:13:  1  packet
udp  206.251.19.88(2817) ->  ?.?.?.251(33434),       Mar  20        05:22:23:  1  packet
udp  206.251.19.88(2814) ->  ?.?.?.251(33434),       Mar  20        05:22:54:  1  packet
udp  206.251.19.88(2816) ->  ?.?.?.251(33434),       Mar  20        05:22:56:  1  packet
udp  206.251.19.88(2814) ->  ?.?.?.251(33434),       Mar  20        05:24:04:  1  packet
udp  206.251.19.88(2816) ->  ?.?.?.251(33434),       Mar  20        05:24:05:  1  packet
udp  206.251.19.88(2815) ->  ?.?.?.251(33434),       Mar  20        05:25:11:  1  packet
udp  206.251.19.88(2816) ->  ?.?.?.251(33434),       Mar  20        05:25:13:  1  packet
udp  206.251.19.88(2817) ->  ?.?.?.251(33434),       Mar  20        05:25:14:  1  packet
udp  206.251.19.88(2814) ->  ?.?.?.251(33434),       Mar  20        05:26:14:  1  packet
udp  206.251.19.88(2816) ->  ?.?.?.251(33434),       Mar  20        05:26:16:  1  packet
udp  206.251.19.88(2817) ->  ?.?.?.251(33434),       Mar  20        05:26:20:  1  packet
udp  206.251.19.88(2814) ->  ?.?.?.251(33434),       Mar  20        05:27:25:  1  packet
udp  206.251.19.88(2817) ->  ?.?.?.251(33434),       Mar  20        05:27:31:  1  packet
udp  206.251.19.88(2400) ->  ?.?.?.251(53),          Mar  20        05:29:17:  1  packet
udp  206.251.19.88(2814) ->  ?.?.?.251(33434),       Mar  20        05:29:35:  1  packet
udp  206.251.19.88(2815) ->  ?.?.?.251(33434),       Mar  20        05:29:36:  1  packet
tcp  206.251.19.88(2401) ->  ?.?.?.251(53),          Mar  20        05:29:37:  1  packet
udp  206.251.19.89(2814) ->  ?.?.?.251(33434),       Mar  20        05:30:39:  1  packet
udp  206.251.19.89(2815) ->  ?.?.?.251(33434),       Mar  20        05:30:40:  1  packet
udp  206.251.19.89(2816) ->  ?.?.?.251(33434),       Mar  20        05:30:41:  1  packet
udp  206.251.19.89(2817) ->  ?.?.?.251(33434),       Mar  20        05:30:42:  1  packet
udp  206.251.19.89(2815) ->  ?.?.?.251(33434),       Mar  20        05:32:21:  1  packet
udp  206.251.19.89(2815) ->  ?.?.?.251(33434),       Mar  20        05:32:56:  1  packet
```

udp 206.251.19.89(2815) -> ?.?.?.251(33434), Mar 20 05:35:46: 1 packet
udp 206.251.19.89(2817) -> ?.?.?.251(33434), Mar 20 05:35:53: 1 packet
udp 206.251.19.89(2814) -> ?.?.?.251(33434), Mar 20 05:36:51: 1 packet
udp 206.251.19.89(2815) -> ?.?.?.251(33434), Mar 20 05:36:55: 1 packet
udp 206.251.19.80(2714) -> ?.?.?.251(33434), Mar 20 05:38:28: 1 packet
udp 206.251.19.80(2715) -> ?.?.?.251(33434), Mar 20 05:38:29: 1 packet
udp 206.251.19.80(2716) -> ?.?.?.251(33434), Mar 20 05:38:31: 1 packet
udp 206.251.19.80(2717) -> ?.?.?.251(33434), Mar 20 05:38:32: 1 packet
udp 206.251.19.80(2714) -> ?.?.?.251(33434), Mar 20 05:40:16: 1 packet
udp 206.251.19.80(2715) -> ?.?.?.251(33434), Mar 20 05:40:17: 1 packet
udp 206.251.19.80(2716) -> ?.?.?.251(33434), Mar 20 05:40:18: 1 packet
udp 206.251.19.80(2717) -> ?.?.?.251(33434), Mar 20 05:40:19: 1 packet
udp 206.251.19.88(2100) -> ?.?.?.251(53), Mar 20 05:40:40: 1 packet
tcp 206.251.19.88(2100) -> ?.?.?.251(53), Mar 20 05:40:50: 1 packet
udp 206.251.19.88(2814) -> ?.?.?.251(33434), Mar 20 06:01:37: 1 packet
udp 206.251.19.88(2815) -> ?.?.?.251(33434), Mar 20 06:01:38: 1 packet
udp 206.251.19.88(2816) -> ?.?.?.251(33434), Mar 20 06:01:39: 1 packet
udp 206.251.19.88(2818) -> ?.?.?.251(33434), Mar 20 06:01:42: 1 packet
udp 206.251.19.88(2814) -> ?.?.?.251(33434), Mar 20 06:02:47: 1 packet
tcp 206.251.19.88(2100) -> ?.?.?.251(53), Mar 20 06:03:18: 1 packet
udp 206.251.19.89(2814) -> ?.?.?.251(33434), Mar 20 06:08:11: 1 packet
udp 206.251.19.89(2815) -> ?.?.?.251(33434), Mar 20 06:08:13: 1 packet
udp 206.251.19.89(2816) -> ?.?.?.251(33434), Mar 20 06:08:14: 1 packet
udp 206.251.19.89(2817) -> ?.?.?.251(33434), Mar 20 06:08:15: 1 packet
udp 206.251.19.80(2200) -> ?.?.?.251(53), Mar 20 06:09:39: 1 packet
tcp 206.251.19.80(2200) -> ?.?.?.251(53), Mar 20 06:09:49: 1 packet
udp 206.251.19.80(2715) -> ?.?.?.251(33434), Mar 20 06:12:39: 1 packet
udp 206.251.19.80(2716) -> ?.?.?.251(33434), Mar 20 06:12:40: 1 packet
udp 206.251.19.80(2717) -> ?.?.?.251(33434), Mar 20 06:12:41: 1 packet
udp 206.251.19.80(2718) -> ?.?.?.251(33434), Mar 20 06:12:42: 1 packet
udp 206.251.19.80(2100) -> ?.?.?.251(53), Mar 20 06:29:25: 1 packet
tcp 206.251.19.80(2100) -> ?.?.?.251(53), Mar 20 06:29:55: 1 packet
udp 206.251.19.88(2814) -> ?.?.?.251(33434), Mar 20 11:56:46: 1 packet
udp 206.251.19.88(2815) -> ?.?.?.251(33434), Mar 20 11:56:47: 1 packet
udp 206.251.19.88(2816) -> ?.?.?.251(33434), Mar 20 11:56:48: 1 packet
udp 206.251.19.88(2817) -> ?.?.?.251(33434), Mar 20 11:56:49: 1 packet
udp 206.251.19.88(2818) -> ?.?.?.251(33434), Mar 20 11:56:50: 1 packet
udp 206.251.19.88(2301) -> ?.?.?.251(53), Mar 20 16:37:29: 1 packet
tcp 206.251.19.88(2302) -> ?.?.?.251(53), Mar 20 16:38:19: 1 packet
udp 206.251.19.88(2814) -> ?.?.?.251(33434), Mar 20 16:39:10: 1 packet
udp 206.251.19.88(2815) -> ?.?.?.251(33434), Mar 20 16:39:11: 1 packet
udp 206.251.19.88(2816) -> ?.?.?.251(33434), Mar 20 16:39:12: 1 packet
udp 206.251.19.88(2817) -> ?.?.?.251(33434), Mar 20 16:39:13: 1 packet
udp 206.251.19.89(2400) -> ?.?.?.251(53), Mar 21 06:01:56: 1 packet
tcp 206.251.19.89(2400) -> ?.?.?.251(53), Mar 21 06:02:16: 1 packet
udp 206.251.19.88(2815) -> ?.?.?.251(33434), Mar 21 06:03:35: 1 packet
udp 206.251.19.88(2816) -> ?.?.?.251(33434), Mar 21 06:03:36: 1 packet
udp 206.251.19.88(2817) -> ?.?.?.251(33434), Mar 21 06:03:37: 1 packet
udp 206.251.19.88(2816) -> ?.?.?.251(33434), Mar 21 17:06:17: 1 packet
udp 206.251.19.88(2817) -> ?.?.?.251(33434), Mar 21 17:06:19: 1 packet
udp 206.251.19.88(2818) -> ?.?.?.251(33434), Mar 21 17:06:20: 1 packet

```
udp  206.251.19.88(2819) ->  ?.?.?.251(33434),     Mar  21        17:06:21:  1  packet
udp  206.251.19.88(2820) ->  ?.?.?.251(33434),     Mar  21        17:06:22:  1  packet
udp  206.251.19.89(2816) ->  ?.?.?.251(33434),     Mar  21        17:07:17:  1  packet
udp  206.251.19.89(2817) ->  ?.?.?.251(33434),     Mar  21        17:07:18:  1  packet
udp  206.251.19.89(2818) ->  ?.?.?.251(33434),     Mar  21        17:07:20:  1  packet
udp  206.251.19.89(2819) ->  ?.?.?.251(33434),     Mar  21        17:07:21:  1  packet
udp  206.251.19.89(2820) ->  ?.?.?.251(33434),     Mar  21        17:07:22:  1  packet
udp  206.251.19.89(2817) ->  ?.?.?.251(33434),     Mar  21        17:08:35:  1  packet
udp  206.251.19.89(2818) ->  ?.?.?.251(33434),     Mar  21        17:08:36:  1  packet
udp  206.251.19.89(2819) ->  ?.?.?.251(33434),     Mar  21        17:08:37:  1  packet
udp  206.251.19.89(2820) ->  ?.?.?.251(33434),     Mar  21        17:08:38:  1  packet
udp  206.251.19.89(2301) ->  ?.?.?.251(53),        Mar  21        17:33:26:  1  packet
tcp  206.251.19.89(2300) ->  ?.?.?.251(53),        Mar  21        17:33:46:  1  packet
udp  206.251.19.88(2818) ->  ?.?.?.251(33434),     Mar  21        17:54:06:  1  packet
udp  206.251.19.88(2816) ->  ?.?.?.251(33434),     Mar  21        17:55:14:  1  packet
udp  206.251.19.88(2817) ->  ?.?.?.251(33434),     Mar  21        17:55:16:  1  packet
udp  206.251.19.88(2820) ->  ?.?.?.251(33434),     Mar  21        17:55:19:  1  packet
udp  206.251.19.89(2816) ->  ?.?.?.251(33434),     Mar  21        17:56:15:  1  packet
udp  206.251.19.89(2817) ->  ?.?.?.251(33434),     Mar  21        17:56:16:  1  packet
udp  206.251.19.89(2818) ->  ?.?.?.251(33434),     Mar  21        17:56:17:  1  packet
udp  206.251.19.89(2819) ->  ?.?.?.251(33434),     Mar  21        17:56:19:  1  packet
udp  206.251.19.89(2816) ->  ?.?.?.251(33434),     Mar  21        17:59:23:  1  packet
udp  206.251.19.89(2819) ->  ?.?.?.251(33434),     Mar  21        17:59:27:  1  packet
udp  206.251.19.80(2716) ->  ?.?.?.251(33434),     Mar  21        18:00:57:  1  packet
udp  206.251.19.80(2717) ->  ?.?.?.251(33434),     Mar  21        18:00:58:  1  packet
udp  206.251.19.80(2718) ->  ?.?.?.251(33434),     Mar  21        18:01:00:  1  packet
udp  206.251.19.80(2719) ->  ?.?.?.251(33434),     Mar  21        18:01:01:  1  packet
udp  206.251.19.89(2402) ->  ?.?.?.251(53),        Mar  22        12:09:44:  1  packet
tcp  206.251.19.89(2400) ->  ?.?.?.251(53),        Mar  22        12:10:44:  1  packet
udp  206.251.19.88(2000) ->  ?.?.?.251(53),        Mar  25        22:57:40:  1  packet
tcp  206.251.19.88(2001) ->  ?.?.?.251(53),        Mar  25        22:57:50:  1  packet
udp  206.251.19.89(2817) ->  ?.?.?.251(33434),     Mar  25        23:16:33:  1  packet
udp  206.251.19.89(2818) ->  ?.?.?.251(33434),     Mar  25        23:16:34:  1  packet
udp  206.251.19.89(2819) ->  ?.?.?.251(33434),     Mar  25        23:16:36:  1  packet
udp  206.251.19.89(2820) ->  ?.?.?.251(33434),     Mar  25        23:16:37:  1  packet
udp  206.251.19.88(2817) ->  ?.?.?.251(33434),     Mar  25        23:16:38:  1  packet
udp  206.251.19.88(2818) ->  ?.?.?.251(33434),     Mar  25        23:16:39:  1  packet
udp  206.251.19.88(2819) ->  ?.?.?.251(33434),     Mar  25        23:16:40:  1  packet
udp  206.251.19.88(2820) ->  ?.?.?.251(33434),     Mar  25        23:16:41:  1  packet
udp  206.251.19.88(2821) ->  ?.?.?.251(33434),     Mar  25        23:16:42:  1  packet
udp  206.251.19.89(2817) ->  ?.?.?.251(33434),     Mar  25        23:17:56:  1  packet
udp  206.251.19.89(2820) ->  ?.?.?.251(33434),     Mar  25        23:17:59:  1  packet
udp  206.251.19.89(2817) ->  ?.?.?.251(33434),     Mar  25        23:18:28:  1  packet
udp  206.251.19.89(2821) ->  ?.?.?.251(33434),     Mar  25        23:18:30:  1  packet
udp  206.251.19.80(2717) ->  ?.?.?.251(33434),     Mar  25        23:20:38:  1  packet
udp  206.251.19.80(2718) ->  ?.?.?.251(33434),     Mar  25        23:20:39:  1  packet
udp  206.251.19.80(2719) ->  ?.?.?.251(33434),     Mar  25        23:20:40:  1  packet
udp  206.251.19.80(2720) ->  ?.?.?.251(33434),     Mar  25        23:20:42:  1  packet
udp  206.251.19.80(2200) ->  ?.?.?.251(53),        Mar  25        23:49:49:  1  packet
tcp  206.251.19.80(2200) ->  ?.?.?.251(53),        Mar  25        23:49:59:  1  packet
udp  206.251.19.80(2200) ->  ?.?.?.251(53),        Mar  26        00:09:55:  1  packet
```

```
tcp  206.251.19.80(2201) ->  ?.?.?.251(53),          Mar  26        00:10:05:  1  packet
udp  206.251.19.80(2200) ->  ?.?.?.251(53),          Mar  26        00:20:10:  1  packet
tcp  206.251.19.80(2201) ->  ?.?.?.251(53),          Mar  26        00:20:39:  1  packet
udp  206.251.19.88(2818) ->  ?.?.?.251(33434),       Mar  27        09:16:48:  1  packet
udp  206.251.19.88(2819) ->  ?.?.?.251(33434),       Mar  27        09:16:49:  1  packet
udp  206.251.19.88(2820) ->  ?.?.?.251(33434),       Mar  27        09:16:50:  1  packet
udp  206.251.19.88(2821) ->  ?.?.?.251(33434),       Mar  27        09:16:51:  1  packet
udp  206.251.19.88(2819) ->  ?.?.?.251(33434),       Mar  27        09:18:02:  1  packet
udp  206.251.19.88(2820) ->  ?.?.?.251(33434),       Mar  27        09:18:04:  1  packet
udp  206.251.19.88(2821) ->  ?.?.?.251(33434),       Mar  27        09:18:05:  1  packet
udp  206.251.19.89(2819) ->  ?.?.?.251(33434),       Mar  27        09:18:53:  1  packet
udp  206.251.19.89(2820) ->  ?.?.?.251(33434),       Mar  27        09:18:54:  1  packet
udp  206.251.19.89(2821) ->  ?.?.?.251(33434),       Mar  27        09:18:55:  1  packet
udp  206.251.19.89(2818) ->  ?.?.?.251(33434),       Mar  27        09:20:15:  1  packet
udp  206.251.19.89(2819) ->  ?.?.?.251(33434),       Mar  27        09:20:16:  1  packet
udp  206.251.19.89(2820) ->  ?.?.?.251(33434),       Mar  27        09:20:18:  1  packet
udp  206.251.19.89(2821) ->  ?.?.?.251(33434),       Mar  27        09:20:19:  1  packet
udp  206.251.19.80(2718) ->  ?.?.?.251(33434),       Mar  27        09:23:30:  1  packet
udp  206.251.19.80(2719) ->  ?.?.?.251(33434),       Mar  27        09:23:32:  1  packet
udp  206.251.19.80(2720) ->  ?.?.?.251(33434),       Mar  27        09:23:33:  1  packet
udp  206.251.19.80(2721) ->  ?.?.?.251(33434),       Mar  27        09:23:34:  1  packet
udp  206.251.19.88(2300) ->  ?.?.?.251(53),          Mar  27        09:39:14:  1  packet
tcp  206.251.19.88(2300) ->  ?.?.?.251(53),          Mar  27        09:39:54:  1  packet
udp  206.251.19.80(2000) ->  ?.?.?.251(53),          Mar  27        10:27:23:  1  packet
tcp  206.251.19.80(2000) ->  ?.?.?.251(53),          Mar  27        10:27:43:  1  packet
udp  206.251.19.89(2818) ->  ?.?.?.251(33434),       Mar  27        10:47:29:  1  packet
udp  206.251.19.89(2819) ->  ?.?.?.251(33434),       Mar  27        10:47:30:  1  packet
udp  206.251.19.89(2820) ->  ?.?.?.251(33434),       Mar  27        10:47:31:  1  packet
udp  206.251.19.80(2720) ->  ?.?.?.251(33434),       Mar  27        10:50:51:  1  packet
udp  206.251.19.88(2822) ->  ?.?.?.251(33434),       Mar  28        08:19:18:  1  packet
udp  206.251.19.88(2823) ->  ?.?.?.251(33434),       Mar  28        08:19:19:  1  packet
udp  206.251.19.89(2823) ->  ?.?.?.251(33434),       Mar  28        08:21:32:  1  packet
udp  206.251.19.89(2824) ->  ?.?.?.251(33434),       Mar  28        08:21:33:  1  packet
udp  206.251.19.89(2823) ->  ?.?.?.251(33434),       Mar  28        08:23:03:  1  packet
udp  206.251.19.89(2400) ->  ?.?.?.251(53),          Mar  28        22:50:06:  1  packet
tcp  206.251.19.89(2400) ->  ?.?.?.251(53),          Mar  28        22:50:47:  1  packet
udp  206.251.19.88(2822) ->  ?.?.?.251(33434),       Mar  28        23:08:24:  1  packet
udp  206.251.19.88(2823) ->  ?.?.?.251(33434),       Mar  28        23:08:25:  1  packet
udp  206.251.19.88(2824) ->  ?.?.?.251(33434),       Mar  28        23:08:26:  1  packet
udp  206.251.19.88(2825) ->  ?.?.?.251(33434),       Mar  28        23:08:27:  1  packet
udp  206.251.19.89(2822) ->  ?.?.?.251(33434),       Mar  28        23:11:37:  1  packet
udp  206.251.19.89(2823) ->  ?.?.?.251(33434),       Mar  28        23:11:38:  1  packet
udp  206.251.19.89(2824) ->  ?.?.?.251(33434),       Mar  28        23:11:39:  1  packet
udp  206.251.19.89(2825) ->  ?.?.?.251(33434),       Mar  28        23:11:41:  1  packet
udp  206.251.19.88(2822) ->  ?.?.?.251(33434),       Mar  28        23:14:08:  1  packet
udp  206.251.19.89(2823) ->  ?.?.?.251(33434),       Mar  28        23:14:43:  1  packet
udp  206.251.19.89(2823) ->  ?.?.?.251(33434),       Mar  28        23:17:17:  2  packets
udp  206.251.19.88(2300) ->  ?.?.?.251(53),          Mar  28        23:17:47:  1  packet
tcp  206.251.19.88(2300) ->  ?.?.?.251(53),          Mar  28        23:18:28:  1  packet
udp  206.251.19.80(2722) ->  ?.?.?.251(33434),       Mar  28        23:19:36:  1  packet
udp  206.251.19.80(2723) ->  ?.?.?.251(33434),       Mar  28        23:19:37:  1  packet
```

```
udp  206.251.19.80(2724) ->  ?.?.?.251(33434),     Mar  28      23:19:38:  1  packet
udp  206.251.19.80(2725) ->  ?.?.?.251(33434),     Mar  28      23:19:39:  1  packet
udp  206.251.19.80(2722) ->  ?.?.?.251(33434),     Mar  28      23:23:07:  2  packets
udp  206.251.19.80(2722) ->  ?.?.?.251(33434),     Mar  28      23:25:18:  1  packet
udp  206.251.19.89(2100) ->  ?.?.?.251(53),        Mar  28      23:26:49:  1  packet
tcp  206.251.19.89(2100) ->  ?.?.?.251(53),        Mar  28      23:27:09:  1  packet
```

DETECT # 2

Existence — Single IP addresse attempting to send traffic to port 25 on a non Mail system continuously over a period of 3 days. This site was registered to another military installation.

History — I have never recorded any other instances of denials from this site.

Techniques — Send multiple packets to the smtp port continuously in intervals from 15 to 25 minutes

Intent — To deliver mail

Targeting — This was not a targeted host, but a wrong email address.

Severity **-7** = (Criticality **2** + Lethality **1**) **-** (Sys CtrMeasures **5** + Network Ctrmeasures **5**)

Analysis — This received immediate attention because it was a single host attempting to send multiple packets to a host that doesn't have the SMTP port active. The continuous attempts suggested that it was automated. ARIN revealed that the site was another military site that did frequent business with us. Concluded that this was probably an email server attempting to send email to a wrong address.

```
tcp  ?.?.?.65(1446)      ->  ?.?.?.201(25),     Mar  31  18:42:01:  1  packet
tcp  ?.?.?.65(1446)      ->  ?.?.?.201(25),     Mar  31  18:42:06:  1  packet
tcp  ?.?.?.65(1446)      ->  ?.?.?.201(25),     Mar  31  18:42:15:  2  packets
tcp  ?.?.?.65(1446)      ->  ?.?.?.201(25),     Mar  31  18:42:35:  1  packet
tcp  ?.?.?.65(1446)      ->  ?.?.?.201(25),     Mar  31  18:43:12:  1  packet
tcp  ?.?.?.65(1551)      ->  ?.?.?.201(25),     Mar  31  19:05:43:  1  packet
tcp  ?.?.?.65(1551)      ->  ?.?.?.201(25),     Mar  31  19:05:47:  1  packet
tcp  ?.?.?.65(1551)      ->  ?.?.?.201(25),     Mar  31  19:05:55:  1  packet
tcp  ?.?.?.65(1551)      ->  ?.?.?.201(25),     Mar  31  19:05:58:  1  packet
tcp  ?.?.?.65(1551)      ->  ?.?.?.201(25),     Mar  31  19:06:15:  1  packet
tcp  ?.?.?.65(1551)      ->  ?.?.?.201(25),     Mar  31  19:06:51:  1  packet
tcp  ?.?.?.65(1710)      ->  ?.?.?.201(25),     Mar  31  20:07:57:  1  packet
tcp  ?.?.?.65(1710)      ->  ?.?.?.201(25),     Mar  31  20:08:02:  1  packet
```

This repeats several times over a 3 day period.

```
tcp  ?.?.?.65(6236)      ->  ?.?.?.201(25),     Apr   2  23:59:11:  1  packet
tcp  ?.?.?.65(6236)      ->  ?.?.?.201(25),     Apr   2  23:59:38:  1  packet
```

DETECT # 3

Existence	Same IP address sends packets a few times each month. 204.178.16.36, which is registered to Bell Laboratories/Lucent Technologies, 700 Mountain Ave, Murray Hill, NJ 07974
History	This site has been sending a series of 3 udp packets multiple times a month since Jan
Techniques	The interesting part about this detect is that all of the detects occur between 0700 and 0715. The destination port is always above 33434. The detects always come in a series of 3 packets. Always has the same destination host.
Intent	Gateway mapping
Targeting	Only a single host machine is targeted, but this destination host doesn't exist.
Severity	**-9** = (Criticality **0** + Lethality **1**) **-** (Sys CtrMeasures **5** + Network Ctrmeasures **5**)
Analysis	These detects were always consistent at approximately the same time of day. I was interested as to why Bell Laboratories were interested in us. Just for research I attempted to go to the source site's port 80. Sure enough there was a web page. This is part of the Internet Mapping Project. They use UDP traceroute-style path probes to build a tree showing paths that internet traffic takes. Since these are UDP traceroutes it is likely that the system is not a windows based system. They produce the fractal pictures seen in different magazines depicting internet bandwidth in varying colors. You can be asked to be removed from such traces. I would think that over time this site could have a great database that shows bottleneck vulnerabilities to sites.

```
udp  204.178.16.36(33128)   -> ?.?.?.1(33783),     Jan  10 07:06:51:  1   packet
udp  204.178.16.36(33128)   -> ?.?.?.1(34123),     Jan  10 07:06:57:  1   packet
udp  204.178.16.36(33128)   -> ?.?.?.1(35264),     Jan  10 07:07:12:  1   packet
udp  204.178.16.36(39702)   -> ?.?.?.1(33819),     Feb  5  07:10:18:  1   packet
udp  204.178.16.36(39702)   -> ?.?.?.1(35643),     Feb  5  07:09:57:  1   packet
udp  204.178.16.36(39702)   -> ?.?.?.1(37318),     Feb  5  07:10:02:  1   packet
udp  204.178.16.36(41497)   -> ?.?.?.1(34664),     Jan  13 07:04:59:  1   packet
udp  204.178.16.36(41497)   -> ?.?.?.1(35038),     Jan  13 07:05:05:  1   packet
udp  204.178.16.36(41497)   -> ?.?.?.1(35894),     Jan  13 07:05:21:  1   packet
udp  204.178.16.36(44782)   -> ?.?.?.1(33933),     Feb  12 07:11:20:  1   packet
udp  204.178.16.36(44782)   -> ?.?.?.1(35964),     Feb  12 07:10:59:  1   packet
udp  204.178.16.36(44782)   -> ?.?.?.1(36279),     Feb  12 07:11:04:  1   packet
udp  204.178.16.36(47968)   -> ?.?.?.1(33568),     Mar  30 07:07:29:  1   packet
udp  204.178.16.36(47968)   -> ?.?.?.1(33681),     Mar  30 07:07:35:  1   packet
udp  204.178.16.36(47968)   -> ?.?.?.1(33989),     Mar  30 07:07:50:  1   packet
udp  204.178.16.36(50459)   -> ?.?.?.1(33986),     Mar  4  07:14:26:  1   packet
udp  204.178.16.36(50459)   -> ?.?.?.1(34705),     Mar  4  07:14:42:  1   packet
udp  204.178.16.36(50459)   -> ?.?.?.1(36519),     Mar  4  07:14:20:  1   packet
udp  204.178.16.36(52324)   -> ?.?.?.1(33468),     Feb  22 07:13:34:  1   packet
udp  204.178.16.36(52324)   -> ?.?.?.1(33883),     Feb  22 07:13:50:  1   packet
udp  204.178.16.36(52324)   -> ?.?.?.1(35595),     Feb  22 07:13:28:  1   packet
udp  204.178.16.36(53092)   -> ?.?.?.1(35210),     Jan  24 07:08:19:  1   packet
udp  204.178.16.36(53092)   -> ?.?.?.1(35565),     Jan  24 07:08:24:  1   packet
udp  204.178.16.36(53092)   -> ?.?.?.1(37289),     Jan  24 07:08:40:  1   packet
udp  204.178.16.36(57045)   -> ?.?.?.1(33441),     Mar  1  07:14:56:  1   packet
```

```
udp  204.178.16.36(57045)   -> ?.?.?.1(34671),      Mar 1  07:14:34:  1  packet
udp  204.178.16.36(57045)   -> ?.?.?.1(34983),      Mar 1  07:14:40:  1  packet
udp  204.178.16.36(58286)   -> ?.?.?.1(34483),      Mar 21 07:04:38:  1  packet
udp  204.178.16.36(58286)   -> ?.?.?.1(36509),      Mar 21 07:04:16:  1  packet
udp  204.178.16.36(58286)   -> ?.?.?.1(36723),      Mar 21 07:04:22:  1  packet
```

DETECT # 4

Existence	An individual supposedly at IP address 209.166.41.8, which is registered to Tricetel, Inc, 205 Browertown Road, West Paterson, NJ 07424.
History	There isn't evidence of this IP attempting anything on our network before
Techniques	This was a very slow attempt at scanning hosts. The time between these is over 4 hours. Probably monitored, because the scanning stops after 3 attempts and the long time span. These were probably crafted packets due to the source port being 53.
Intent	The individual wanted to know which hosts on our network might have port 111 listening. More than likely this was only a reconnaissance sweep.
Targeting	While targeting our network the person was not individually targeting a specific machine

Severity **-9** = (Criticality **0** + Lethality **1**) **-** (Sys CtrMeasures **5** + Network Ctrmeasures **5**)

Analysis This was an attempt to find Sun RPC ports that were listening on our network. Due to the fact that these hosts do not exist the intent was malicious. The fact that the scans were 1 packet at 4 hour intervals I think the person was definitely trying to not get noticed. After receiving nothing in 3 host attempts individual stopped. Since I feel the packets were crafted, the source IP is probably spoofed as well.

```
tcp 209.166.41.8(53)    -> ?.?.?.1(111),    Mar 14 01:15:04:  1   packet
tcp 209.166.41.8(53)    -> ?.?.?.2(111),    Mar 14 05:34:19:  1   packet
tcp 209.166.41.8(53)    -> ?.?.?.3(111),    Mar 14 09:53:45:  1   packet
```

DETECT # 5

Existence — Individual at IP address 161.58.239.94, registered to an ISP JvNCnet in Princeton NJ

History — While I have detected activity from the 161.58 IP range before I have never received anything from the 239 subnet. With the exception of the 5th and 18th of Mar 00.

Techniques — On the 5th only interested in one machine, but due to how quickly initiated probably automated. Tries same 2 ports on all hosts, but particularly interested in port 1665.

Intent — Malicious since host Ips don't exist, unsure of significance of dest ports. Just random selection so host mapping.

Targeting — Appears random selection of hosts on our network

Severity **-4** = (Criticality **0** + Lethality **1**) **-** (Sys CtrMeasures **5** + Network Ctrmeasures **5**)

Analysis — The source ports are all common ports which indicates to me that the packets were crafted. The person is specifically interested in 2 ports, 1665, and 1520. I searched through several sites looking for vulnerabilities to these ports or possible trojans that are listening at these ports and have found nothing. The ports are listed at IANA as being assigned to 1520-atm zip post office and 1665- netview-aix-5. It would be interesting to look at the individual packets. There must be an application vulnerability that uses these ports.

tcp 161.58.239.94(21)	-> ?.?.?.35(1665),	Mar 5 09:21:56: 1 packet
tcp 161.58.239.94(21)	-> ?.?.?.35(1665),	Mar 5 09:21:58: 1 packet
tcp 161.58.239.94(21)	-> ?.?.?.14(1665),	Mar 18 19:51:51: 1 packet
tcp 161.58.239.94(21)	-> ?.?.?.14(1665),	Mar 18 19:52:02: 1 packet
tcp 161.58.239.94(21)	-> ?.?.?.25(1520),	Mar 18 20:19:52: 1 packet
tcp 161.58.239.94(21)	-> ?.?.?.25(1520),	Mar 18 20:19:54: 1 packet
tcp 161.58.239.94(21)	-> ?.?.?.46(1520),	Mar 18 02:04:01: 1 packet
tcp 161.58.239.94(21)	-> ?.?.?.61(1665),	Mar 18 23:31:40: 1 packet
tcp 161.58.239.94(21)	-> ?.?.?.61(1665),	Mar 18 23:31:52: 1 packet
tcp 161.58.239.94(21)	-> ?.?.?.82(1665),	Mar 18 05:15:22: 1 packet
tcp 161.58.239.94(21)	-> ?.?.?.108(1665),	Mar 19 03:12:07: 1 packet
tcp 161.58.239.94(22)	-> ?.?.?.35(1665),	Mar 5 09:21:47: 1 packet
tcp 161.58.239.94(23)	-> ?.?.?.35(1665),	Mar 5 09:22:07: 1 packet
tcp 161.58.239.94(23)	-> ?.?.?.14(1665),	Mar 18 19:48:14: 1 packet
tcp 161.58.239.94(23)	-> ?.?.?.61(1665),	Mar 18 23:28:03: 1 packet
tcp 161.58.239.94(23)	-> ?.?.?.61(1665),	Mar 18 23:28:06: 1 packet
tcp 161.58.239.94(23)	-> ?.?.?.95(1665),	Mar 18 16:09:18: 1 packet
tcp 161.58.239.94(53)	-> ?.?.?.46(1520),	Mar 18 02:04:25: 1 packet
tcp 161.58.239.94(53)	-> ?.?.?.46(1520),	Mar 18 02:04:33: 1 packet
tcp 161.58.239.94(53)	-> ?.?.?.61(1665),	Mar 18 23:28:04: 1 packet
tcp 161.58.239.94(80)	-> ?.?.?.35(1665),	Mar 5 09:22:19: 1 packet
tcp 161.58.239.94(80)	-> ?.?.?.35(1665),	Mar 5 09:22:30: 1 packet

DETECT # 6

Existence — Individual is using IP address 195.159.0.90, which is registered to an ISP in Oslo, Norway

History — No activity other than this.

Techniques — Slow host scanning, spread out over different days. Source ports are from ports that are known to be associated with Trojans.

Intent — Search for systems on our network listening to particular ports, again 1520 and 1665

Targeting — The target ports are specific, but hosts are again random.

Severity **-9** = (Criticality **0** + Lethality **1**) **-** (Sys CtrMeasures **5** + Network Ctrmeasures **5**)

Analysis — This scan showed up on 2 separate syslog dates but is from a single session spanning over 10 hours. The person was scanning for any host listening on ports 1520 and 1665. Because the source ports were all from ports known for being used with Trojans, 113-Kazimas, 666-Attack FTP, Back Construction, Satanz Backdoor, ServU, 6667-SchedulAgent. I think that they were possibly specifically picked as a signature in their crafted packets. Again, there must be an undocumented vulnerability to applications using these destination ports.

```
tcp 195.159.0.90(113)      -> ?.?.?.1(1665),      Jan 27 18:09:07:  1  packet
tcp 195.159.0.90(113)      -> ?.?.?.12(1520),     Jan 27 18:33:44:  1  packet
tcp 195.159.0.90(113)      -> ?.?.?.48(1665),     Jan 27 21:14:42:  1  packet
tcp 195.159.0.90(113)      -> ?.?.?.106(1520),    Jan 28 01:15:16:  1  packet
tcp 195.159.0.90(113)      -> ?.?.?.14(1665),     Jan 28 04:08:15:  1  packet
tcp 195.159.0.90(113)      -> ?.?.?.25(1520),     Jan 28 04:35:25:  1  packet
tcp 195.159.0.90(666)      -> ?.?.?.12(1520),     Jan 27 18:48:09:  1  packet
tcp 195.159.0.90(666)      -> ?.?.?.48(1665),     Jan 27 21:29:54:  1  packet
tcp 195.159.0.90(666)      -> ?.?.?.59(1520),     Jan 27 21:52:58:  1  packet
tcp 195.159.0.90(666)      -> ?.?.?.82(1665),     Jan 27 15:26:08:  1  packet
tcp 195.159.0.90(666)      -> ?.?.?.106(1520),    Jan 28 01:39:04:  1  packet
tcp 195.159.0.90(666)      -> ?.?.?.25(1520),     Jan 28 05:01:00:  1  packet
tcp 195.159.0.90(6667)     -> ?.?.?.12(1520),     Jan 27 18:34:03:  1  packet
tcp 195.159.0.90(6667)     -> ?.?.?.48(1665),     Jan 27 21:15:35:  1  packet
tcp 195.159.0.90(6667)     -> ?.?.?.48(1665),     Jan 27 21:15:37:  1  packet
```

DETECT # 7

Existence — This individual was using IP address 193.220.68.84, which is registered to the Open Society Foundation for Albania and is an Open Internet Center in Albania.

History — no previous activity

Techniques — manual scan, probably not crafted

Intent — Individual was looking for a web server or proxy server

Targeting — Specifically targeting web servers or proxy servers, possibly targeting this site as a military site, but host destination machine not a viable target

Severity **-9** = (Criticality **5** + Lethality **1**) **-** (Sys CtrMeasures **5** + Network Ctrmeasures **5**)

Analysis — This was probably not a crafted packet based strictly on the source ports. The time difference was only 49 seconds. The machine could be fairly active indicated by the difference in the source ports. The person was obviously just randomly picking hosts, because host 65 does not exist on network. Particular interest since the originating host is from Albania and destination host is a US military site.

```
tcp 193.220.68.84(63485)    -> ?.?.?.65(80),      Mar 27 10:38:02: 1  packet
tcp 193.220.68.84(63533)    -> ?.?.?.65(8080),    Mar 27 10:38:51: 1  packet
```

DETECT # 8

Existence	Individual was using IP address 200.188.80.21, which is registered to a Brazilian Research Network, RNP, Rua Pio XI, 1500, Sao Paulo, 05468
History	No previous activity
Techniques	Crafted packets, slow spread out over 12 hours
Intent	Identify any listening ports on target system
Targeting	Targeted a particular system but looking for any unassigned ports that are listening on the system.

Severity **-9** = (Criticality **0** + Lethality **1**) **-** (Sys CtrMeasures **5** + Network Ctrmeasures **5**)

Analysis The individual was performing a portmapping scan against a particular host looking for listening ports. All of these ports are not currently assigned to an application according to IANA. The packets were obviously crafted since the source port number was the same over a 12 hour period.

```
tcp 200.188.80.21(24322)   -> ?.?.?.48(10219),   Mar 12 13:33:52:  1   packet
tcp 200.188.80.21(24322)   -> ?.?.?.48(11755),   Mar 12 14:13:30:  1   packet
tcp 200.188.80.21(24322)   -> ?.?.?.48(26091),   Mar 12 13:49:04:  1   packet
tcp 200.188.80.21(24322)   -> ?.?.?.48(26091),   Mar 12 14:08:01:  1   packet
tcp 200.188.80.21(24322)   -> ?.?.?.48(36843),   Mar 12 19:47:15:  1   packet
tcp 200.188.80.21(24322)   -> ?.?.?.48(38891),   Mar 12 13:59:08:  1   packet
tcp 200.188.80.21(24322)   -> ?.?.?.48(45035),   Mar 12 17:37:04:  1   packet
tcp 200.188.80.21(24322)   -> ?.?.?.48(9707),    Mar 12 19:23:27:  1   packet
tcp 200.188.80.21(24322)   -> ?.?.?.48(40427),   Mar 13 08:36:51:  1   packet
tcp 200.188.80.21(24322)   -> ?.?.?.48(52203),   Mar 13 02:23:56:  1   packet
tcp 200.188.80.21(24322)   -> ?.?.?.48(65003),   Mar 13 02:16:00:  1   packet
```

DETECT # 9

Existence Individual using IP address, 206.204.112.44, which is registered to ConXion Corporation, 4201 Burton Drive, Santa Clara, CA 95054

History no previous activity

Techniques crafted packet, slow probably manual entry

Intent discover trojans

Targeting specifically targeted ports known to be used by Trojans

Severity **-9** = (Criticality **0** + Lethality **1**) **-** (Sys CtrMeasures **5** + Network Ctrmeasures **5**)

Analysis This individual was probably crafting their packets since the source port was identical over a 2 hour period. The destination ports targeted are well known trojan ports. 1999-BackDoor, Transcout; 2000-Der Spaeher 3, Insane Network, Transcout; 2140-Deep Throat, The Invasor. More than likely simply looking for these trojans.

```
tcp 206.204.112.44(18145)   -> ?.?.?.7(1999),    Mar 10 08:17:19:  1   packet
tcp 206.204.112.44(18145)   -> ?.?.?.7(2000),    Mar 10 08:01:07:  1   packet
tcp 206.204.112.44(18145)   -> ?.?.?.7(2140),    Mar 10 06:15:11:  1   packet
```

DETECT # 10

Existence Individual was using IP address 207.44.231.3, which is registered to Sirius Solutions, Inc, 2 Connecticut St, Ste 200, San Francisco, CA 94107

History While this IP address wasn't used before, it's neighbor host 2 has been seen before

Techniques crafting packets, slow

Intent Port mapping

Targeting any ports listening,

Severity **-9** = (Criticality **0** + Lethality **1**) **-** (Sys CtrMeasures **5** + Network Ctrmeasures **5**)

Analysis The source port is the same for all packets, which is very unlikely due to the time span. Since the packet is crafted possibly the IP address is spoofed also. Individual is searching for any available TCP ports.

tcp	207.44.231.3(18145)	-> ?.?.?.7(1064),	Mar	3	09:57:46:	1 packet
tcp	207.44.231.3(18145)	-> ?.?.?.7(1064),	Mar	3	09:57:54:	1 packet
tcp	207.44.231.3(18145)	-> ?.?.?.7(1124),	Mar	3	09:29:54:	1 packet
tcp	207.44.231.3(18145)	-> ?.?.?.7(1132),	Mar	3	06:42:47:	1 packet
tcp	207.44.231.3(18145)	-> ?.?.?.7(1312),	Mar	3	08:13:19:	1 packet
tcp	207.44.231.3(18145)	-> ?.?.?.7(1320),	Mar	3	05:26:10:	1 packet
tcp	207.44.231.3(18145)	-> ?.?.?.7(1320),	Mar	3	05:26:11:	1 packet
tcp	207.44.231.3(18145)	-> ?.?.?.7(1484),	Mar	3	09:36:51:	1 packet
tcp	207.44.231.3(18145)	-> ?.?.?.7(1484),	Mar	3	09:36:53:	1 packet
tcp	207.44.231.3(18145)	-> ?.?.?.7(1612),	Mar	3	05:54:01:	1 packet
tcp	207.44.231.3(18145)	-> ?.?.?.7(1680),	Mar	3	05:33:08:	1 packet
tcp	207.44.231.3(18145)	-> ?.?.?.7(1680),	Mar	3	05:33:12:	1 packet
tcp	207.44.231.3(18145)	-> ?.?.?.7(1732),	Mar	3	07:52:25:	1 packet
tcp	207.44.231.3(18145)	-> ?.?.?.7(1732),	Mar	3	07:52:35:	1 packet
tcp	207.44.231.3(18145)	-> ?.?.?.7(1844),	Mar	3	09:43:49:	1 packet
tcp	207.44.231.3(18145)	-> ?.?.?.7(1844),	Mar	3	09:43:51:	1 packet
tcp	207.44.231.3(18145)	-> ?.?.?.7(2032),	Mar	3	08:27:15:	1 packet
tcp	207.44.231.3(18145)	-> ?.?.?.7(2032),	Mar	3	08:27:18:	1 packet
tcp	207.44.231.3(18145)	-> ?.?.?.7(2092),	Mar	3	07:59:23:	1 packet
tcp	207.44.231.3(18145)	-> ?.?.?.7(2092),	Mar	3	07:59:25:	1 packet
tcp	207.44.231.3(18145)	-> ?.?.?.7(2212),	Mar	3	07:03:40:	1 packet
tcp	207.44.231.3(18145)	-> ?.?.?.7(2332),	Mar	3	06:07:57:	1 packet
tcp	207.44.231.3(18145)	-> ?.?.?.7(2332),	Mar	3	06:07:59:	1 packet
tcp	207.44.231.3(18145)	-> ?.?.?.7(2392),	Mar	3	08:34:12:	1 packet
tcp	207.44.231.3(18145)	-> ?.?.?.7(2392),	Mar	3	08:34:16:	1 packet

Last Updated: October 18th, 2017

Upcoming Training

SANS Berlin 2017	Berlin, Germany	Oct 23, 2017 - Oct 28, 2017	Live Event
SANS Seattle 2017	Seattle, WA	Oct 30, 2017 - Nov 04, 2017	Live Event
San Diego Fall 2017 - SEC503: Intrusion Detection In-Depth	San Diego, CA	Oct 30, 2017 - Nov 04, 2017	vLive
SANS San Diego 2017	San Diego, CA	Oct 30, 2017 - Nov 04, 2017	Live Event
SANS Paris November 2017	Paris, France	Nov 13, 2017 - Nov 18, 2017	Live Event
Community SANS Pensacola SEC503	Pensacola, FL	Nov 27, 2017 - Dec 02, 2017	Community SANS
SIEM & Tactical Analytics Summit & Training	Scottsdale, AZ	Nov 28, 2017 - Dec 05, 2017	Live Event
SANS Munich December 2017	Munich, Germany	Dec 04, 2017 - Dec 09, 2017	Live Event
SANS Cyber Defense Initiative 2017	Washington, DC	Dec 12, 2017 - Dec 19, 2017	Live Event
Community SANS Nashville SEC401^	Nashville, TN	Jan 08, 2018 - Jan 13, 2018	Community SANS
SANS Security East 2018	New Orleans, LA	Jan 08, 2018 - Jan 13, 2018	Live Event
Las Vegas 2018 - SEC503: Intrusion Detection In-Depth	Las Vegas, NV	Jan 28, 2018 - Feb 02, 2018	vLive
SANS Las Vegas 2018	Las Vegas, NV	Jan 28, 2018 - Feb 02, 2018	Live Event
SANS London February 2018	London, United Kingdom	Feb 05, 2018 - Feb 10, 2018	Live Event
SANS Dallas 2018	Dallas, TX	Feb 19, 2018 - Feb 24, 2018	Live Event
SANS Northern VA Spring - Tysons 2018	McLean, VA	Mar 17, 2018 - Mar 24, 2018	Live Event
SANS Secure Canberra 2018	Canberra, Australia	Mar 19, 2018 - Mar 24, 2018	Live Event
SANS 2018	Orlando, FL	Apr 03, 2018 - Apr 10, 2018	Live Event
SANS Baltimore Spring 2018	Baltimore, MD	Apr 21, 2018 - Apr 28, 2018	Live Event
SANS Security West 2018	San Diego, CA	May 11, 2018 - May 18, 2018	Live Event
Community SANS Columbia SEC503	Columbia, MD	Aug 13, 2018 - Aug 18, 2018	Community SANS
SANS OnDemand	Online	Anytime	Self Paced
SANS SelfStudy	Books & MP3s Only	Anytime	Self Paced