*** Northcutt, fine job, Paul clearly demonstrates competency at analysis. Multiple sources, lessons learned along the way, research, good use of an analysis process. 89 *

SANS 2000 IDIC Practical

Paul Stillwell

April 24, 2000

Detect 1

Date: March 12, 2000
Detected using IPChains

At first I thought that this was the tail end of a slow UDP port scan. But the source address and consistent source port (below 1024) were bothering me. The domain is known and the source port was always 123 (xntp). After some research, I discovered that it was actually a misconfiguration of my IPChains rules (I had the source and dest ports reversed) for valid xntp traffic. What through me off initially is that the reverse lookup returns snort.someplace.net. A different name than what is in the xntp configuration file. The config file points to a server called clock.someplace.net which resolves to a.b.c.d, the reverse lookup on a.b.c.d returns snort.someplace.net.

This example illustrates well that caution and objectivity are required when analyzing any detect.

IPChains:

```
<...snip>
Mar 12 04:05:35 hostname kernel: Packet log: input - eth0 PROTO=17 snort.someplace.net:123
me.nowhere.com:61218 L=76 S=0x10 I=63671 F=0x4000 T=245

Mar 12 04:22:37 hostname kernel: Packet log: input - eth0 PROTO=17 snort.someplace.net:123
me.nowhere.com:61219 L=76 S=0x10 I=37095 F=0x4000 T=245

Mar 12 04:39:41 hostname kernel: Packet log: input - eth0 PROTO=17 snort.someplace.net:123
me.nowhere.com:61220 L=76 S=0x10 I=12549 F=0x4000 T=245

Mar 12 04:56:46 hostname kernel: Packet log: input - eth0 PROTO=17 snort.someplace.net:123
me.nowhere.com:61221 L=76 S=0x10 I=54469 F=0x4000 T=245

Mar 12 05:13:50 hostname kernel: Packet log: input - eth0 PROTO=17 snort.someplace.net:123
me.nowhere.com:61222 L=76 S=0x10 I=29903 F=0x4000 T=245
<snip...>
```

Detect 2

April 12, 2000
Detected by IPChains

Active Targeting

Yes, This trace is from my home machine on the @Home network. It occurred before I had Snort installed. IPChains is set to log anything that comes in that is not expected.

Intent

Scanning for the SubSeven Trojan.

Technique

The source port stays consistent throughout each scan, however, it changes from scan to scan. This could indicate the presence of a client that has the capability to scan large numbers of addresses for infected machines. Four packets are sent fairly quickly (sometimes 2/second, sometimes 1/second) which supports the hypothesis of a tool/client.

History

SubSeven seems to be the Trojan of the month. I am getting a lot of these. I chose these examples to show the wide range of sources I'm seeing and because these three scans all occurred in one day.

Identity

According to ARIN the sources are a super computing center, a cable user in Southern California, and a dialup ISP user.

Severity

Low

IPChains:

```
Apr 12 04:49:49 unbeliever kernel: Packet log: input - eth0 PROTO=6 a.supercomputer.place:3254
me.home.com:27374 L=48 S=0x00 I=57926 F=0x4000 T=111

Apr 12 04:49:50 unbeliever kernel: Packet log: input - eth0 PROTO=6 a.supercomputer.place:3254
me.home.com:27374 L=48 S=0x00 I=65094 F=0x4000 T=111

Apr 12 04:49:50 unbeliever kernel: Packet log: input - eth0 PROTO=6 a.supercomputer.place:3254
me.home.com:27374 L=48 S=0x00 I=5191 F=0x4000 T=111
```

```
Apr 12 04:49:51 unbeliever kernel: Packet log: input - eth0 PROTO=6 a.supercomputer.place:3254
me.home.com:27374 L=48 S=0x00 I=6727 F=0x4000 T=111


Apr 12 07:26:14 unbeliever kernel: Packet log: input - eth0 PROTO=6 cable.socal.com:22619
me.home.com:27374 L=48 S=0x00 I=15306 F=0x4000 T=106

Apr 12 07:26:14 unbeliever kernel: Packet log: input - eth0 PROTO=6 cable.socal.com:22619
me.home.com:27374 L=48 S=0x00 I=28362 F=0x4000 T=106

Apr 12 07:26:15 unbeliever kernel: Packet log: input - eth0 PROTO=6 cable.socal.com:22619
me.home.com:27374 L=48 S=0x00 I=30922 F=0x4000 T=106

Apr 12 07:26:16 unbeliever kernel: Packet log: input - eth0 PROTO=6 cable.socal.com:22619
me.home.com:27374 L=48 S=0x00 I=33482 F=0x4000 T=106


Apr 12 12:18:05 unbeliever kernel: Packet log: input - eth0 PROTO=6
someone.earthlink.place:4018 me.home.com:27374 L=48 S=0x00 I=56958 F=0x4000 T=112

Apr 12 12:18:06 unbeliever kernel: Packet log: input - eth0 PROTO=6
someone.earthlink.place:4018 me.home.com:27374 L=48 S=0x00 I=64126 F=0x4000 T=112

Apr 12 12:18:07 unbeliever kernel: Packet log: input - eth0 PROTO=6
someone.earthlink.place:4018 me.home.com:27374 L=48 S=0x00 I=4223 F=0x4000 T=112

Apr 12 12:18:07 unbeliever kernel: Packet log: input - eth0 PROTO=6
someone.earthlink.place:4018 me.home.com:27374 L=48 S=0x00 I=9343 F=0x4000 T=112
```

Detect 3

Date: April 4, 2000
Detected by browsing through SunScreen SPF-200 firewall logs

Active Targeting

Yes, the address targeted is the cluster address of some web servers.

Intent

Initially I thought this could be an attempted DDoS. However, as you will see in the Technique section, it is probably just an attempted DOS.

History

We have seen this pattern several times (04/05/2000, 04/06/2000, 04/10/2000 and 04/18/2000) since it's initial detect on April 4, 2000

Technique

"Valid" source address interleaved with non-routable sources. Although it is not evident from the trace below, it is suspected that the TTL value of all of these packets is the same (115). This particular firewall does not make it easy to examine the TTL value, therefore, a random sampling of packets were checked in (extremely) verbose mode and all had a TTL value of 115 indicating the true source of all of these packets was probably the same device. However, as there is currently no machine available outside of the firewall that can do a traceroute back to the one routable source address we cannot begin to speculate that it is the real IP address of the machine responsible for the scan.

Because at least two source addresses were spoofed and the large number of packets received we can speculate that the attacker does not expect a response from these queries. There were 2257 packets logged over the course of 48 minutes giving an average rate of 47.02 packets per minute. The number of packets received and the duration of the attack indicate an automated attack destined for the NetBIOS Name Service port used by Microsoft Operating systems

We can safely say that the attacker did not really know (or maybe didn't care) what O/S the targeted machine was running. If it were an attempt at a denial of service I would have expected a lot more packets. Looking at the timestamps there is a lot of inconsistency. It seems like the attacker is starting and stopping as if they were playing with some code they just acquired or created.

Severity

Low – Could have been much worse.

The targeted cluster is running Solaris so even if the packets had made it through the firewall the server would not have given up any information.

Comments

As a result of this detect, and the concern over DDoS attacks, which have a similar signature, we have re-issued a request to our ISP to implement ingress & egress filtering on their routers.

SunScreen SPF-200:

```
148312     qfe0 (deny rule or no pass rule)2000/4/4 14:29:11.667852     10.0.0.1 ->
server.cluster UDP D=137 S=137 LEN=58

148323     qfe0 (deny rule or no pass rule)2000/4/4 14:29:13.159727     10.0.0.1 ->
server.cluster UDP D=137 S=137 LEN=58

148330     qfe0 (deny rule or no pass rule)2000/4/4 14:29:14.201428     10.0.0.1 ->
server.cluster UDP D=137 S=137 LEN=58

148336     qfe0 (deny rule or no pass rule)2000/4/4 14:29:14.653467     10.0.0.1 ->
server.cluster UDP D=137 S=137 LEN=58

148345     qfe0 (deny rule or no pass rule)2000/4/4 14:29:15.701321     10.0.0.1 ->
server.cluster UDP D=137 S=137 LEN=58

148351     qfe0 (deny rule or no pass rule)2000/4/4 14:29:17.200075     10.0.0.1 ->
server.cluster UDP D=137 S=137 LEN=58

154004     qfe0 (deny rule or no pass rule)2000/4/4 15:05:24.672919    10.0.0.11 ->
server.cluster UDP D=137 S=137 LEN=58

154012     qfe0 (deny rule or no pass rule)2000/4/4 15:05:26.176217    10.0.0.11 ->
server.cluster UDP D=137 S=137 LEN=58

154018     qfe0 (deny rule or no pass rule)2000/4/4 15:05:27.669124    10.0.0.11 ->
server.cluster UDP D=137 S=137 LEN=58

156866     qfe0 (deny rule or no pass rule)2000/4/4 15:21:16.328143 205.250.106.45 ->
server.cluster UDP D=137 S=137 LEN=58

156867     qfe0 (deny rule or no pass rule)2000/4/4 15:21:16.390505     10.0.0.1 ->
server.cluster UDP D=137 S=137 LEN=58

156872     qfe0 (deny rule or no pass rule)2000/4/4 15:21:17.830198 205.250.106.45 ->
server.cluster UDP D=137 S=137 LEN=58

156873     qfe0 (deny rule or no pass rule)2000/4/4 15:21:17.884252     10.0.0.1 ->
server.cluster UDP D=137 S=137 LEN=58

156875     qfe0 (deny rule or no pass rule)2000/4/4 15:21:19.324201 205.250.106.45 ->
server.cluster UDP D=137 S=137 LEN=58

156876     qfe0 (deny rule or no pass rule)2000/4/4 15:21:19.438643     10.0.0.1 ->
server.cluster UDP D=137 S=137 LEN=58

156886     qfe0 (deny rule or no pass rule)2000/4/4 15:21:23.275270 205.250.106.45 ->
server.cluster UDP D=137 S=137 LEN=58

156887     qfe0 (deny rule or no pass rule)2000/4/4 15:21:23.356962     10.0.0.1 ->
server.cluster UDP D=137 S=137 LEN=58

156890     qfe0 (deny rule or no pass rule)2000/4/4 15:21:24.781950 205.250.106.45 ->
server.cluster UDP D=137 S=137 LEN=58
```

```
156891     qfe0 (deny rule or no pass rule)2000/4/4 15:21:24.852243     10.0.0.1 ->
server.cluster UDP D=137 S=137 LEN=58
<snip...>
```

Detect 4

Date April 21, 2000
Detected By: Snort & IPChains

Active Targeting

Yes. This detect is from my home machine on the @Home network. Snort is configured not to go into promiscuous mode, therefore everything it reports was actually sent to me. I have IPChains set to log anything that comes in that is not expected.

Intent

Probably scanning the @home network for machines infected with a Trojan called "Deep Throat, The Invasor".

Technique

Surprisingly I only received one packet. I would have expected to see two or three. The scanner could be trying to elude common intrusion detection techniques that would require 3 or more packets before an alert was raised.

Identity

After a nslookup, and querying the ARIN Whois database, the source address points to a DSL provider in Massachusetts

Severity

Low

Comments

I have been seeing a lot of scans for well-known Trojans.

Snort:

```
[**] Deep Throat/Invasor [**]
04/21-17:04:13.198326 user.dsl.ma:60000 -> me.at.home:2140
UDP TTL:50 TOS:0x0 ID:2320
Len: 10
```

IPChains:

```
Apr 21 17:04:13 unbeliever kernel: Packet log: input - eth0 PROTO=17
user.dsl.ma:60000 me.at.home:2140 L=30 S=0x00 I=2320 F=0x0000 T=50
```

Detect 5

Date: April 21, 2000
Detected by Snort & IPChains

Active Targeting

Yes. This detect is from my home machine on the @Home network. Snort is configured not to go into promiscuous mode, therefore everything it reports was actually sent to me. I have IPChains set to log anything that comes in that is not expected.

Intent

Searching for machines with unprotected shares or machines running Windows.

Technique

Likely an automated scan of machines on the @Home network. The timestamps show a approximately 1 packet per second, the source and destination ports of 137, and a length of 58 bytes. This is consistent with the ArachNIDS database (IDS177 netbios-name-query) with the exception of the source port of 137. The ArachNIDS example uses a source port above 1024.

History / Identity

This probe originated from within same network in Southern California as detect #2 above.

Severity

Low

Snort:

```
[**] SMB Name Wildcard [**]
04/21-13:21:41.856720 some.cableuser.socal:137 -> me.athome.com:137
UDP TTL:110 TOS:0x0 ID:10946
Len: 58

[**] SMB Name Wildcard [**]
04/21-13:21:43.410188 some.cableuser.socal:137 -> me.athome.com:137
UDP TTL:110 TOS:0x0 ID:11202
Len: 58

[**] SMB Name Wildcard [**]
04/21-13:21:44.920499 some.cableuser.socal:137 -> me.athome.com:137
UDP TTL:110 TOS:0x0 ID:11458
Len: 58
```

IPChains:

```
Apr 21 13:21:41 unbeliever kernel: Packet log: input - eth0 PROTO=17 some.cableuser.socal:137
me.athome.com:137 L=78 S=0x00 I=10946 F=0x0000 T=110

Apr 21 13:21:43 unbeliever kernel: Packet log: input - eth0 PROTO=17 some.cableuser.socal:137
me.athome.com:137 L=78 S=0x00 I=11202 F=0x0000 T=110
```

```
Apr 21 13:21:44 unbeliever kernel: Packet log: input - eth0 PROTO=17 some.cableuser.socal:137
me.athome.com:137 L=78 S=0x00 I=11458 F=0x0000 T=110
```

Detect 6

Date April 22, 2000
Detected by Snort & IPChains

Active Targeting

Yes. This detect is from my home machine on the @Home network. Snort is configured not to go into promiscuous mode, therefore everything it reports was actually sent to me. I have IPChains set to log anything that comes in that is not expected.

Intent

Looking for machines running WinGate (or another proxy server) possibly to exploit one of the many vulnerabilities that have existed in this product or to find a proxy server that will allow anonymous redirection of their connections.

Technique

Based on the port being scanned this is likely an automated scan of many machines on the @Home network.

Identity

In order to actually get feedback from their scan, the attacker would not be able to spoof the source address. A combination of an ARIN Whois query and a reverse nslookup shows that this one originated from address space owned by UU-Net that is probably used for dialup accounts.

Severity

Low

Comments

Both Snort and IPChains logged connection attempts to port 8080, commonly used by WinGate (and other proxy servers). @Home users sometimes use WinGate in order to connect more than one machine to the @Home network and only use one IP Address.

Snort:

```
[**] WinGate 8080 Attempt [**]
04/22-03:20:05.164500 dial.uu.net:4615 -> me.at.home:8080
TCP TTL:54 TOS:0x0 ID:36113  DF
**S***** Seq: 0x91ED9D   Ack: 0x0   Win: 0x860
TCP Options => MSS: 536 NOP NOP SackOK

[**] WinGate 8080 Attempt [**]
04/22-03:20:05.950088 dial.uu.net:4615 -> me.at.home:8080
TCP TTL:54 TOS:0x0 ID:49169  DF
**S***** Seq: 0x91ED9D   Ack: 0x0   Win: 0x860
```

```
TCP Options => MSS: 536 NOP NOP SackOK

[**] WinGate 8080 Attempt [**]
04/22-03:20:06.691105 dial.uu.net:4615 -> me.at.home:8080
TCP TTL:54 TOS:0x0 ID:56337  DF
**S***** Seq: 0x91ED9D   Ack: 0x0   Win: 0x860
TCP Options => MSS: 536 NOP NOP SackOK
```

IPChains

```
Apr 22 03:20:05 unbeliever kernel: Packet log: input - eth0 PROTO=6 dial.uu.net:4615
me.at.home:8080 L=48 S=0x00 I=36113 F=0x4000 T=54
Apr 22 03:20:05 unbeliever kernel: Packet log: input - eth0 PROTO=6 dial.uu.net:4615
me.at.home:8080 L=48 S=0x00 I=49169 F=0x4000 T=54
Apr 22 03:20:06 unbeliever kernel: Packet log: input - eth0 PROTO=6 dial.uu.net:4615
me.at.home:8080 L=48 S=0x00 I=56337 F=0x4000 T=54
```

Detect 7

Date March 12, 2000
Detected By IPChains

Active Targeting

Yes, This trace is from my home machine on the @Home network. It occurred before I had Snort installed. IPChains is set to log anything that comes in that is not expected.

Intent

The target port is one that I had not seen before, but after consulting the Trojan list at http://www.simovits.com/nyheter9902.html it could be a scan looking for a Trojan called "Hack`a`Tack". The source port on both packets is the same indicating that a tool was probably used to run the scan.

Technique

The source port on both packets is the same indicating that a tool was probably used to run the scan.

Identity

At first, due to the time difference on the packet headers I thought that this was two separate scans, then looking at the networks that these packets came from and after a little research I decided that it may have been the same person both times. The sources appear to be from a dialup pool of addresses at netcom.ca (now owned by AT&T).

Severity

Low

IPChains:

```
Mar 12 13:07:16 unbeliever kernel: Packet log: input - eth0 PROTO=17 dial1.netcom:31790
me.at.home:31789 L=29 S=0x00 I=16164 F=0x0000 T=122

Mar 12 20:09:33 unbeliever kernel: Packet log: input - eth0 PROTO=17 dial2.netcom:31790
me.at.home:31789 L=29 S=0x00 I=30904 F=0x0000 T=122
```

Detect 8

Date April 4, 2000
Detected by SunScreen SPF-200 Firewall

Active Targeting

Yes, this activity targets the cluster address of some web servers.

Intent

Possible Denial of Service attempt.

Technique

I examined several of the packets in verbose mode and determined that source IP address was actually 10.0.0.0 and that the TTL seemed consistent at 117. The timestamps show a very consistent pattern of 2 packets in one second repeated at two second intervals, the source and destination ports of 137, and a length of 58 bytes. This is consistent with the ArachNIDS database (IDS177 netbios-name-query) with the exception of the source port of 137. The ArachNIDS example uses a source port above 1024.

This is also different from Detect #5 above in that the apparent intent here is a DoS rather than scanning for unprotected shares.

Identity

Unknown. A verbose decode of some of the packets revealed that the source address was actually 10.0.0.0.

Severity

Low.

Comments

This particular cluster seems to attract a disproportionately large amount of NetBIOS Name Service (UDP Port 137) attention for a cluster of Solaris servers. Of interest is the source address of "arpanet" (this time the source has not been changed). The reason this is interesting is that the firewall is not configured to use any kind of name service. I examined several of the packets in verbose mode and determined that source IP address was actually 10.0.0.0.

SunScreen SPF-200:

```
100867     qfe0 (deny rule or no pass rule)2000/4/4 9:29:34.654960      arpanet ->
server.cluster UDP D=137 S=137 LEN=58

100870     qfe0 (deny rule or no pass rule)2000/4/4 9:29:34.659208      arpanet ->
server.cluster UDP D=137 S=137 LEN=58
```

```
100876     qfe0 (deny rule or no pass rule)2000/4/4 9:29:36.154095      arpanet ->
server.cluster UDP D=137 S=137 LEN=58

100879     qfe0 (deny rule or no pass rule)2000/4/4 9:29:36.157710      arpanet ->
server.cluster UDP D=137 S=137 LEN=58
<snip… 42 Packets total>
```

Detect 9

Date April 23, 2000
Detected with IPChains

Active Targeting

This detect is from my home machine on the @Home network. Snort is configured not to go into promiscuous mode, therefore everything it reports was actually sent to me. I also have IPChains set to log anything that comes in that is not expected.

Intent

Possibly looking for a news server that is vulnerable to any of a number of well-known security problems.

Technique

It looks like they are automated as I consistently log two connection attempts within a minute.

History

I see connection attempts to my news service port on a regular (daily) basis from this source.

Identity

A reverse lookup reveals that the machine scanning me is (according to the DNS) an authorized @Home scanning server

Severity

Low

Comments

Snort did not report this one as it is not configured to report Syn requests to generally valid service ports (I haven't had time to customize it too much yet). However, IPChains is configured to report anything that is not expected, and I am not running a news server, so connection attempts to the news port are of interest but benign.

IPChains:

```
Apr 23 15:04:00 unbeliever kernel: Packet log: input - eth0 PROTO=6 auth.scanner.home:54923
me.at.home:119 L=44 S=0x00 I=343 F=0x0000 T=242

Apr 23 15:04:18 unbeliever kernel: Packet log: input - eth0 PROTO=6 auth.scanner.home:64602
me.at.home:119 L=44 S=0x00 I=344 F=0x0000 T=242
```

```
Apr 23 18:59:31 unbeliever kernel: Packet log: input - eth0 PROTO=6 auth.scanner.home:48149
me.at.home:119 L=44 S=0x00 I=40383 F=0x0000 T=242

Apr 23 18:59:55 unbeliever kernel: Packet log: input - eth0 PROTO=6 auth.scanner.home:59653
me.at.home:119 L=44 S=0x00 I=40384 F=0x0000 T=242
```

Detect 10

Date April 4, 2000
Detected by SunScreen SPF-200

Active Targeting

Yes, each one of these packets were sent to addresses within our DMZ network

Intent

Recon, it appears to be a host scan.

Technique

At first it would appear that the scanner knows something about our network as the first packet goes to our DNS server and the next to the cluster address of our web server, but then continues to cover almost the rest of the class C range. They might have a tool which seeks out DNS servers, then queries them for a www.whatever, and then proceeds to scan from there.

This is an automated technique sending many packets per second. The firewall is configured to drop packets silently, and according to the nmap documentation a Half-Open" scan will only send a RST if it receives a Syn-ACK (this assumes that the scanner is using nmap). According to this trace (and the fact that no machines have services running on port 81) no Syn-ACK should have been sent, and yet we see a corresponding RST for each of the SYNs. Watching the source ports we can see that the source is not too busy (other than scanning us).

History

Checking through our logs, we haven't seen this source before.

Identity

A reverse lookup revealed nothing. According to ARIN, this is a European source, so I went to RIPE and found that the source belongs to an ISP in the UK.

Severity

Low

SunScreen SPF-200:

```
197118     qfe0 (deny rule or no pass rule)2000/4/23 23:40:41.799467  somewhere.uk ->
www.xxx.yyy.65 TCP D=81 S=35039 Syn Seq=1630776701 Len=0 Win=8760

197119     qfe0 (deny rule or no pass rule)2000/4/23 23:40:41.815759  somewhere.uk ->
www.xxx.yyy.110 TCP D=81 S=35084 Syn Seq=1633711439 Len=0 Win=8760
```

```
197120     qfe0 (deny rule or no pass rule)2000/4/23 23:40:41.821791  somewhere.uk ->
www.xxx.yyy.122 TCP D=81 S=35096 Syn Seq=1634569286 Len=0 Win=8760

197121     qfe0 (deny rule or no pass rule)2000/4/23 23:40:41.881175  somewhere.uk ->
www.xxx.yyy.111 TCP D=81 S=35085 Syn Seq=1633717717 Len=0 Win=8760

197122     qfe0 (deny rule or no pass rule)2000/4/23 23:40:41.881790  somewhere.uk ->
www.xxx.yyy.116 TCP D=81 S=35090 Syn Seq=1634129000 Len=0 Win=8760

197123     qfe0 (deny rule or no pass rule)2000/4/23 23:40:41.882470  somewhere.uk ->
www.xxx.yyy.120 TCP D=81 S=35094 Syn Seq=1634455097 Len=0 Win=8760

197124     qfe0 (deny rule or no pass rule)2000/4/23 23:40:41.883093  somewhere.uk ->
www.xxx.yyy.117 TCP D=81 S=35091 Syn Seq=1634163889 Len=0 Win=8760

197125     qfe0 (deny rule or no pass rule)2000/4/23 23:40:41.883867  somewhere.uk ->
www.xxx.yyy.126 TCP D=81 S=35100 Syn Seq=1634778972 Len=0 Win=8760

197132     qfe0 (deny rule or no pass rule)2000/4/23 23:40:43.692429  somewhere.uk ->
www.xxx.yyy.110 TCP D=81 S=35084 Rst Seq=1633711440 Len=0 Win=8760

197133     qfe0 (deny rule or no pass rule)2000/4/23 23:40:43.692654  somewhere.uk ->
www.xxx.yyy.111 TCP D=81 S=35085 Rst Seq=1633717718 Len=0 Win=8760

197134     qfe0 (deny rule or no pass rule)2000/4/23 23:40:43.693859  somewhere.uk ->
www.xxx.yyy.117 TCP D=81 S=35091 Rst Seq=1634163890 Len=0 Win=8760

197135     qfe0 (deny rule or no pass rule)2000/4/23 23:40:43.694124  somewhere.uk ->
www.xxx.yyy.116 TCP D=81 S=35090 Rst Seq=1634129001 Len=0 Win=8760

197136     qfe0 (deny rule or no pass rule)2000/4/23 23:40:43.694891  somewhere.uk ->
www.xxx.yyy.120 TCP D=81 S=35094 Rst Seq=1634455098 Len=0 Win=8760

197137     qfe0 (deny rule or no pass rule)2000/4/23 23:40:43.695713  somewhere.uk ->
www.xxx.yyy.122 TCP D=81 S=35096 Rst Seq=1634569287 Len=0 Win=8760

197138     qfe0 (deny rule or no pass rule)2000/4/23 23:40:43.696641  somewhere.uk ->
www.xxx.yyy.126 TCP D=81 S=35100 Rst Seq=1634778973 Len=0 Win=8760

197139     qfe0 (deny rule or no pass rule)2000/4/23 23:40:43.703563  somewhere.uk ->
www.xxx.yyy.112 TCP D=81 S=35086 Rst Seq=1633797176 Len=0 Win=8760

197140     qfe0 (deny rule or no pass rule)2000/4/23 23:40:43.714323  somewhere.uk ->
www.xxx.yyy.113 TCP D=81 S=35087 Rst Seq=1633826658 Len=0 Win=8760

197141     qfe0 (deny rule or no pass rule)2000/4/23 23:40:43.715872  somewhere.uk ->
www.xxx.yyy.114 TCP D=81 S=35088 Rst Seq=1633899295 Len=0 Win=8760

197142     qfe0 (deny rule or no pass rule)2000/4/23 23:40:43.716515  somewhere.uk ->
www.xxx.yyy.65 TCP D=81 S=35039 Rst Seq=1630776702 Len=0 Win=8760

197143     qfe0 (deny rule or no pass rule)2000/4/23 23:40:43.717734  somewhere.uk ->
www.xxx.yyy.115 TCP D=81 S=35089 Rst Seq=1634024027 Len=0 Win=8760

197144     qfe0 (deny rule or no pass rule)2000/4/23 23:40:43.719304  somewhere.uk ->
www.xxx.yyy.118 TCP D=81 S=35092 Rst Seq=1634231379 Len=0 Win=8760

197145     qfe0 (deny rule or no pass rule)2000/4/23 23:40:43.720612  somewhere.uk ->
www.xxx.yyy.123 TCP D=81 S=35097 Rst Seq=1634628732 Len=0 Win=8760

197146     qfe0 (deny rule or no pass rule)2000/4/23 23:40:43.722091  somewhere.uk ->
www.xxx.yyy.121 TCP D=81 S=35095 Rst Seq=1634474261 Len=0 Win=8760
<snip… to 232>
```