Global Information Assurance Certification Paper

Haruna Isa
IDIC Practical for GCIA (10 Detects)
4/24/00

Detect #1: SubSeven Scan

Snort View

```
[**] Possible SubSeven access [**]
04/08-09:43:31.945201 24.10.131.221:3104 -> a.cable.host:1243
TCP TTL:119 TOS:0x0 ID:59825  DF
**S***** Seq: 0x50CED8B   Ack: 0x0   Win: 0x2000
TCP Options => MSS: 1460 NOP NOP SackOK

[**] Possible SubSeven access [**]
04/08-09:43:32.457765 24.10.131.221:3104 -> a.cable.host:1243
TCP TTL:119 TOS:0x0 ID:5554  DF
**S***** Seq: 0x50CED8B   Ack: 0x0   Win: 0x2000
TCP Options => MSS: 1460 NOP NOP SackOK

[**] Possible SubSeven access [**]
04/08-09:43:32.967465 24.10.131.221:3104 -> a.cable.host:1243
TCP TTL:119 TOS:0x0 ID:12978  DF
**S***** Seq: 0x50CED8B   Ack: 0x0   Win: 0x2000
TCP Options => MSS: 1460 NOP NOP SackOK

[**] Possible SubSeven access [**]
04/08-09:43:33.476398 24.10.131.221:3104 -> a.cable.host:1243
TCP TTL:119 TOS:0x0 ID:19634  DF
**S***** Seq: 0x50CED8B   Ack: 0x0   Win: 0x2000
TCP Options => MSS: 1460 NOP NOP SackOK
```

1. Identity

24.10.131.xxx/cxxxxxx-a.whtrdgX.co.home.com
Whois: @Home Network, Denver
Yahoo: @Home uses the location as part of the host name, a quick search of Yahoo revealed that this prober likely lives in Wheat Ridge, Colorado. A town of about 30,000 with one high school and one community college branch.

2. Technique

Four attempt to access a SubSeven Trojan. This is probably blind scanning within the cablemodem network looking for machines that might have been compromised by SubSeven.

3. Intent

Recon/exploit. The SubSeven Trojan allows a remote 'client' complete control over the victim computer, on which the server runs. The intent behind this access is definitely malicious.

4. Active Targeting

Yes. There is no legitimate reason for the probing host to initiate contact with the victim on the targeted port. The targeted machine is probably only one of many being probed on the targeted network.

5. Evaluation

The fact that SubSeven is a Windows Trojan and the packets arrive with a TTL of 119 (indicating they likely started with a TTL of 128) means the prober is likely running Windows 98/NT. The packets arrive with

the same sequence numbers separated by .5 seconds and different IP ID's. The target machine sends RST's in response to each packet but these are apparently ignored by the client.

Bottom Line: Medium threat. Novice running SubSeven and trolling for infected machines on the cablemodem network. However, SubSeven is the current 'hot' Trojan and deserves attention.

Detect #2: SYN-FIN Scan

Snort View

```
[**] Source Port traffic [**]
04/23-14:52:09.604121 209.53.123.202:53 -> a.cable.host:53
TCP TTL:24 TOS:0x0 ID:39426
**SF**** Seq: 0x4891F7A4   Ack: 0x3E1EE7B3   Win: 0x404
```

TCPDump View

```
14:52:09.604121 mail.connected.bc.ca.domain > a.cable.host.domain: SF
1217525668:1217525668(0) win 1028 (ttl 24, id 39426)

14:52:09.604497 a.cable.host.domain > mail.connected.bc.ca.domain: R
0:0(0) ack 1217525669 win 0 (ttl 255, id 53805)
```

1. Identity

209.53.123.202/mail.connected.bc.ca
Whois: Connected Networks
WWW (www.connected.bc.ca): Connected Networks ISP Inc.

2. Technique

Both the S(SYN) and F(FIN) flags are set, indicating anomalous packets. Likely a SYN-FIN scan checking for DNS running on the targeted machine.

3. Intent

Recon. Probably checking for a machine running DNS. Next step might have been an attempted zone transfer or buffer overflow.

4. Active Targeting

Yes. The victim computer has never visited/received mail/sent mail to the probing computer. Also, packets with SYN-FIN both set are not naturally occurring.

5. Evaluation

A machine which is not running DNS will respond with a R(RST) (as this machine did in the TCPDump view). Machines that don't respond/respond with SYN/FIN are likely running DNS. Also, Linux will respond with SYN-FIN-ACK to this connection attempt letting the prober know that the machine is running DNS on a Linux platform. A traceroute back to the prober revealed a hop count of 12. The source name seems to indicate the machine is the mail server for the ISP? Since it is generating anomalous traffic on a low numbered port, it might have been rooted.

Bottom Line: Low threat. The connection was rejected and no DNS is running on the target machine.

Detect #3: NetBus Scan

Snort View

```
[**] Netbus/GabanBus [**]
04/21-23:21:18.907913 212.49.253.111:4563 -> a.cable.host:12345
TCP TTL:115 TOS:0x0 ID:9229  DF
**S***** Seq: 0x1277C56   Ack: 0x0   Win: 0x2000
TCP Options => MSS: 536 NOP NOP SackOK

[**] Netbus/GabanBus [**]
04/21-23:21:19.710271 212.49.253.111:4563 -> a.cable.host:12345
TCP TTL:115 TOS:0x0 ID:20237  DF
**S***** Seq: 0x1277C56   Ack: 0x0   Win: 0x2000
TCP Options => MSS: 536 NOP NOP SackOK

[**] Netbus/GabanBus [**]
04/21-23:21:20.559012 212.49.253.111:4563 -> a.cable.host:12345
TCP TTL:115 TOS:0x0 ID:26381  DF
**S***** Seq: 0x1277C56   Ack: 0x0   Win: 0x2000
TCP Options => MSS: 536 NOP NOP SackOK

[**] Netbus/GabanBus [**]
04/21-23:21:21.469024 212.49.253.111:4563 -> a.cable.host:12345
TCP TTL:115 TOS:0x0 ID:34573  DF
**S***** Seq: 0x1277C56   Ack: 0x0   Win: 0x2000
TCP Options => MSS: 536 NOP NOP SackOK
```

TCPDump View

```
23:21:18.907913 212.49.253.111.4563 > a.cable.host.12345: S
19364950:19364950(0) win 8192 <mss 5
36,nop,nop,sackOK> (DF) (ttl 115, id 9229)

23:21:18.908532 a.cable.host.12345 > 212.49.253.111.4563: R 0:0(0) ack
19364951 win 0 (ttl 255,
id 12964)

23:21:19.710271 212.49.253.111.4563 > a.cable.host.12345: S
19364950:19364950(0) win 8192 <mss 5
36,nop,nop,sackOK> (DF) (ttl 115, id 20237)

23:21:19.710501 a.cable.host.12345 > 212.49.253.111.4563: R 0:0(0) ack
1 win 0 (ttl 255, id 1296
5)

23:21:20.559012 212.49.253.111.4563 > a.cable.host.12345: S
19364950:19364950(0) win 8192 <mss 5
36,nop,nop,sackOK> (DF) (ttl 115, id 26381)

23:21:20.559250 a.cable.host.12345 > 212.49.253.111.4563: R 0:0(0) ack
1 win 0 (ttl 255, id 12966)

23:21:21.469024 212.49.253.111.4563 > a.cable.host.12345: S
19364950:19364950(0) win 8192 <mss 5
36,nop,nop,sackOK> (DF) (ttl 115, id 34573)

23:21:21.469242 a.cable.host.12345 > 212.49.253.111.4563: R 0:0(0) ack
1 win 0 (ttl 255, id 12967)
```

1. Identity

212.49.253.111/(reverse lookup fails)
Whois: Screaming Free ISP for Dial Customers, London

2. Technique

Scanning for the NetBus/GabanBus Trojans on the targeted machine. Four packets sent attempting to initiate a connection.

3. Intent

Recon/exploit. The NetBus and GabanBus Trojans allows a remote 'client' near complete control over the victim computer, on which the server runs. The intent behind this access is definitely malicious.

4. Active Targeting

Yes. There is no legitimate reason for the probing host to initiate contact with the victim on the targeted port. The targeted machine is probably only one of many being probed on the targeted network.

5. Evaluation

The whois information seems to indicate this is an English user using a free dial-up service. TTL's and Trojan type indicate the prober is likely running Windows 98/NT. Four packets sent out, about 1 second apart with the same TCP sequence number but different IP ID's. The probing software sends out the subsequent packets despite the RST from the target, indicating the tool being used doesn't give up in response to RST's from the victim.

Bottom Line: Low threat. UK free dial-up user running Windows 98/NT scanning a US cablemodem network looking for Windows boxes compromised by NetBus/GabanBus.

Detect #4: Ring0

Apache Access Log View

194.209.172.145 - - [03/Feb/2000:15:06:27 -0500] "GET http://www.rusftpsearch.net/cgi-bin/pst.pl?pstmode=writeip &psthost=a.cable.host&pstport=80 HTTP/1.0" 404 292

1. Identity

194.209.172.145/border1.leunet.ch
Whois: Leunet, Frauenfeld, Switzerland
WWW (www.leunet.ch): Leunet Internet Provider

2. Technique

Attempting to send back to web server www.rusftpsearch.net that the targeted host is running an anonymous web proxy. The machine conducting the probe has likely been compromised by the Ring0 trojan.

3. Intent

Compiling a list of anonymous web proxies. If the targeted machine had been running an anonymous web proxy, it would have accessed the cgi-script at www.resftpsearch.com and passed its IP address as an argument. Presumably, the cgi script would add the IP address to a list of anonymous web proxies it was compiling. Trojan'd computers do the scanning, therefore the owner of the originating computer in this case might be unaware of the activity.

4. Active Targeting

Sort of. The Trojan randomly selects addresses to probe for web proxies. Also, the owner of the source machine is likely unaware of

the activities of the Trojan.

5. Evaluation

Anonymous web proxies allow any user to proxy a web connection through them thus hidng the source address of that user. A web site accessed through the proxy would record the address of the proxy as the source. This mechanism is a favorite with hackers to hide their identity when mounting attacks or doing recon. These probes are conducted by the Ring0 trojan. The source name 'border1' seems to be indicative of some type of network border device (firewall, NAT device, etc…) Since this is an ISP, the actual compromised machine might be behind the 'border' device thus the address we have is not necessarily the address of the compromised machine.

Bottom Line: Low threat. The targeted machine is not running an anonymous web proxy. The web server which logged the access denied the request.

Detect #5: Portmapper Probe

Snort View (from GIAC – 4/23/00)

```
[**] IDS013 - RPC - portmap-request-mountd [**]
04/20-22:44:25.962806 129.142.224.3:797 -> z.y.x.98:111
UDP TTL:48 TOS:0x0 ID:62984
Len: 64
39 F2 7B F4 00 00 00 00 00 00 00 02 00 01 86 A0 9.{.............
00 00 00 02 00 00 00 03 00 00 00 00 00 00 00 00 ................
00 00 00 00 00 00 00 00 00 01 86 A5 00 00 00 01 ................
00 00 00 06 00 00 00 00 ........

[**] IDS013 - RPC - portmap-request-mountd [**]
04/20-22:44:26.112434 129.142.224.3:798 -> z.y.x.98:111
UDP TTL:48 TOS:0x0 ID:63026
Len: 64
39 FF 1E 5C 00 00 00 00 00 00 00 02 00 01 86 A0 9..\............
00 00 00 02 00 00 00 03 00 00 00 00 00 00 00 00 ................
00 00 00 00 00 00 00 00 00 01 86 A5 00 00 00 01 ................
00 00 00 11 00 00 00 00 ........
```

1. Identity

129.142.224.3/smaug-if0.netropolis.dk
Whois: UNI2/Netropolis, Denmark

2. Technique

Request the port on which NFS is running (mountd). The portmapper keeps tracks of the high numbered ports on which particular RPC services are running and gives the information out to hosts that request it. The idea is that this would allow other machines to find the services easily. Here, the probing host is trying to find out on which port NFS is being run, presumably to then attempt to exploit it in some way.

3. Intent

Recon/exploit. The intent is to find out if the victim computer is running NFS and on which port. If the targeted host responds, the prober might then attempt some type of NFS exploit.

4. Active Targeting

Yes. The targeted machine is probably only one of many being probed on the targeted network.

5. Evaluation

The arrival TTL of 48 seems to indicate the original TTL was between 60 and 64 which is the default UDP TTL for a variety of Unix boxen including FreeBSD, Linux, Irix and HP/UX 10. Since the prober is likely a Unix box, the source port below 1023 indicates root privilege on the machine (prober has legitimate root accesses on the machine or the machine has been rooted.)

Bottom Line: Medium threat. Scan for RPC NFS services on the target computer. RPC services are notoriously vulnerable to a variety of exploits.

Detect #6: Port Scan

(From GIAC 4/22/00)

```
Apr 18 15:08:09 208.3.198.166:1100 -> z.y.x.34:22 SYN **S*****
Apr 18 15:08:10 208.3.198.166:1103 -> z.y.x.34:42 SYN **S*****
Apr 18 15:08:09 208.3.198.166:1104 -> z.y.x.34:53 SYN **S*****
Apr 18 15:08:11 208.3.198.166:1105 -> z.y.x.34:69 SYN **S*****
Apr 18 15:08:09 208.3.198.166:1106 -> z.y.x.34:79 SYN **S*****
Apr 18 15:08:10 208.3.198.166:1107 -> z.y.x.34:80 SYN **S*****
Apr 18 15:08:10 208.3.198.166:1108 -> z.y.x.34:110 SYN **S*****
Apr 18 15:08:10 208.3.198.166:1109 -> z.y.x.34:111 SYN **S*****
Apr 18 15:08:10 208.3.198.166:1110 -> z.y.x.34:119 SYN **S*****
Apr 18 15:08:10 208.3.198.166:1111 -> z.y.x.34:143 SYN **S*****
Apr 18 15:08:12 208.3.198.166:1113 -> z.y.x.34:5191 SYN **S*****
Apr 18 15:08:10 208.3.198.166:1114 -> z.y.x.34:5192 SYN **S*****
Apr 18 15:08:12 208.3.198.166:1115 -> z.y.x.34:5193 SYN **S*****
Apr 18 15:08:12 208.3.198.166:1116 -> z.y.x.34:5631 SYN **S*****
Apr 18 15:08:12 208.3.198.166:1117 -> z.y.x.34:5632 SYN **S*****
Apr 18 15:08:12 208.3.198.166:1118 -> z.y.x.34:5800 SYN **S*****
Apr 18 15:08:12 208.3.198.166:1119 -> z.y.x.34:5900 SYN **S*****
Apr 18 15:08:11 208.3.198.166:1121 -> z.y.x.34:8000 SYN **S*****
Apr 18 15:08:12 208.3.198.166:1124 -> z.y.x.34:9100 SYN **S*****
Apr 18 15:08:11 208.3.198.166:1125 -> z.y.x.34:12345 SYN **S*****
Apr 18 15:08:12 208.3.198.166:1126 -> z.y.x.34:25867 SYN **S*****
Apr 18 15:08:12 208.3.198.166:1099 -> z.y.x.34:21 SYN **S*****
Apr 18 15:08:12 208.3.198.166:1101 -> z.y.x.34:23 SYN **S*****
Apr 18 15:08:13 208.3.198.166:1120 -> z.y.x.34:6000 SYN **S*****
Apr 18 15:08:14 208.3.198.166:1122 -> z.y.x.34:8010 SYN **S*****
Apr 18 15:08:14 208.3.198.166:1123 -> z.y.x.34:8080 SYN **S*****
Apr 18 15:08:15 208.3.198.166:1122 -> z.y.x.34:8010 SYN **S*****
Apr 18 15:08:15 208.3.198.166:1123 -> z.y.x.34:8080 SYN **S*****
Apr 18 15:08:17 208.3.198.166:1108 -> z.y.x.34:110 SYN **S*****
Apr 18 15:08:17 208.3.198.166:1107 -> z.y.x.34:80 SYN **S*****
Apr 18 15:08:17 208.3.198.166:1114 -> z.y.x.34:5192 SYN **S*****
Apr 18 15:08:20 208.3.198.166:1112 -> z.y.x.34:5190 SYN **S*****
Apr 18 15:08:23 208.3.198.166:1103 -> z.y.x.34:42 SYN **S*****
Apr 18 15:08:24 208.3.198.166:1121 -> z.y.x.34:8000 SYN **S*****
```

1. Identity

208.3.198.166/ppp166.usr198.pioneeris.net
Whois: Pioneer Internet Services

2. Technique

Attempting to initiate TCP connections to well known ports on the victim computer. The scanner is searching for running services. Short

differences in arrival times indicate an automated probe. A running service will return a SYN-ACT letting the prober know that service is running on a given port.

3. Intent

Recon. The scanner is searching for services running on the target computer. Next might be to attempt exploits against any services he finds open.

4. Active Targeting

Yes. The targeted machine is probably only one of many being probed on the targeted network. There is no legitimate reason for the prober to attempt to contact all those ports on the target in such a short duration.

5. Evaluation

It appears to be a linear iteration through the list of well known ports. The source ports are above 1023 and they iterate as well indicating the attacker might be using the OS services to attempt the connects (no root access?) Short duration between connection attempts indicates an automated tool. Services: 21-FTP, 22-SSHD, 42-nameserver, 53-DNS, 69-TFTP, 79-Finger, 80-WWW, 110-POP3, 111-Portmapper, 119-News, etc…

Bottom Line: Medium threat. The prober is looking for running services. They will likely be found at which time the prober may then attempt an exploit tailored to the discovered service.

Detect #7: Linuxconf

(From GIAC 4/21/00)

Apr 13 21:27:15 zion kernel: Packet log: bad-if REJECT eth0 PROTO=6 209.196.17.122:2905 MY.SUB.NET.103:98 L=60 S=0x00 I=34971 F=0x4000 T=53 SYN(#33)

1. Indentity

209.196.17.122/(reverse lookup fails)
Whois: Interliant, Atlanta GA
Google: Web hosting/ISP.

2. Technique

Appears to be search for a linux machine running linuxconf. The prober is attempting to establish a connection (TCP:SYN) to the linuxconf process if it is running on the victim computer. Since the source address is registered as belonging to an ISP/ASP, the prober is likely one of the ISP's customers.

3. Intent

Recon/Attack. There can't be a benign reason why a user on a machine unknown to us is attempting to remotely manage our computer.

4. Active Targeting

Yes. The prober is attempting to initiate a connection to a port normally hosting the linuxconf service well outside of their normal address space.

5. Evaluation

Arrival TTL of 53 seems to rule out a Windows box as the probing platform. Since the attempt is to access linuxconf, the prober is likely running on Linux which has a default TCP TTL or 64. Linuxconf is a powerful utility that can be used to configure a large variety of things on a Linux platform including; boot parameters (which partition boots), adding/removing routes, shadow account policies, NFS startup/shutdown and config, etc… Linuxconf supports a web based interface which is accessible over port 98. Someone gaining access to linuxconf gains complete control of the target machine.

Bottom Line: Malicious user on home/commercial computer in Georgia attempting to remotely manage/control the victim computer via linuxconf.

Detect #8: Host Scan

(From GIAC 4/10/00)

```
Apr 7 10:51:28 144.92.98.76:3671 -> x.y.z.101:53 UDP
Apr 7 10:51:28 144.92.98.76:3708 -> x.y.z.116:53 UDP
Apr 7 10:51:28 144.92.98.76:3714 -> x.y.z.118:53 UDP
Apr 7 10:51:29 144.92.98.76:3736 -> x.y.z.128:53 UDP
Apr 7 10:51:29 144.92.98.76:3752 -> x.y.z.135:53 UDP
Apr 7 10:51:29 144.92.98.76:3768 -> x.y.z.142:53 UDP
Apr 7 10:51:55 144.92.98.76:3829 -> x.y.z.161:53 UDP
Apr 7 10:51:55 144.92.98.76:3835 -> x.y.z.164:53 UDP
Apr 7 10:51:55 144.92.98.76:3885 -> x.y.z.186:53 UDP
Apr 7 10:51:55 144.92.98.76:3904 -> x.y.z.195:53 UDP
Apr 7 10:51:55 144.92.98.76:3920 -> x.y.z.200:53 UDP
Apr 7 10:51:55 144.92.98.76:3922 -> x.y.z.201:53 UDP
Apr 7 10:51:55 144.92.98.76:3966 -> x.y.z.217:53 UDP
Apr 7 10:52:50 144.92.98.76:4132 -> x.y.z.52:53 UDP
Apr 7 10:52:50 144.92.98.76:4144 -> x.y.z.58:53 UDP
Apr 7 10:52:50 144.92.98.76:4166 -> x.y.z.67:53 UDP
Apr 7 10:52:50 144.92.98.76:4192 -> x.y.z.79:53 UDP
Apr 7 10:52:50 144.92.98.76:4204 -> x.y.z.83:53 UDP
Apr 7 10:52:50 144.92.98.76:4238 -> x.y.z.97:53 UDP
Apr 7 10:52:54 144.92.98.76:4226 -> x.y.z.91:53 UDP
```

1. Identity

144.92.98.76/orson.lis.wisc.edu
Whois: University of Wisconsin

2. Technique

Scan for DNS server within a class C network using UDP. Probably using an automated port scanner (i.e. nmap) due to the closeness of the timestamps.

3. Intent

Recon. The scanner is looking for a DNS server living somewhere in the x.y.z.0 network. Once found, the prober might attempt a zone transfer or some type of DNS buffer overflow exploit (depending on what version/type of DNS was discovered.)

4. Active Targeting

Yes. The methodical scanning of all addresses within a network does not happen by mistake.

5. Evaluation

Source ports on the host appear to increase in a near linear fashion to the host number being scanned indicating the user is likely using the scanner is likely using the OS services to perform the scan (doesn't have root privilege?). Versions of BIND, the most common DNS server, are susceptible to a variety of buffer overflows and other exploits. The prober might be looking for vulnerable DNS server to exploit.

Bottom Line: College student scanning for DNS server/hosts within the target network for possible follow-on exploitation depending on vulnerability.

Detect #9: Trojan Scan

(From GIAC 4/11/00)

Apr 8 01:37:56 cc1014244-a kernel: securityalert: tcp if=ef0 from 216.77.245.249:2606 to 24.3.21.199 on unserved port 1243
Apr 8 01:37:56 cc1014244-a kernel: securityalert: tcp if=ef0 from 216.77.245.249:2607 to 24.3.21.199 on unserved port 12345
Apr 8 01:37:56 cc1014244-a kernel: securityalert: tcp if=ef0 from 216.77.245.249:2608 to 24.3.21.199 on unserved port 20034
Apr 8 01:37:56 cc1014244-a kernel: securityalert: tcp if=ef0 from 216.77.245.249:2609 to 24.3.21.199 on unserved port 27374

1. Identity

24.3.21.199/ccXXXXXXX-a.hwrd1.md.home.com
Whois: @Home network
Yahoo: Again, @Home uses the location as part of the hostname, likely in Howard County, Maryland

2. Technique

Generalized multiple trojan scan. Looking for a variety of Trojans; 1243-BackDoor-G,SubSeven; 12345-GabanBus,NetBus,Pie Bill Gates,X-bill; 200034-NetBus;27374-SubSeven 2.1. by iterating through the ports they normally listen on.

3. Intent

Recon/exploit. If the victim answered on any of the ports targeted, the prober would likely have then run the appropriate Trojan control program to exploit the victim machine.

4. Active Targeting

Yes. You don't run Trojan scanners by accident. Victim computer is likely only on of many being scanned by the prober.

5. Evaluation

Source ports iterate by 1 between each scan and all four scans occur within 1 second. The scanner is probably using the OS to send the packets (not crafting all of the packet.) More sophisticated than simply scanning for one trojan, scanning for multiple Trojans allows the attacker to have a variety of means getting into the victim machine if it has been infected with any of the Trojans.

Bottom Line: Medium Threat. Scanning to see if the victim has been compromised by one of four Trojans. It one of these ports answers, the prober would likely run the corresponding Trojan exploit program to mess with the victim machine.

Detect #10: Pcanywhere

Snort View

```
[**] PCAnywhere [**]
04/24-12:17:25.252836 24.13.248.68:1751 -> cabole.host:22
UDP TTL:127 TOS:0x0 ID:57529
Len: 10
```

TCPDump View

```
12:17:25.252836 cj429219-a.alex1.va.home.com.1751 > a.cable.host.ssh:
udp 2 (ttl 127, id 57529)

12:17:25.265113 a.cable.host > cj429219-a.alex1.va.home.com: icmp:
a.cable.host
udp port ssh unreachable [tos 0xc0] (ttl 255, id 18665)
~
```

1. Identity

24.13.248.xxx/cjxxxxxx-a.alex1.va.home.com
Whois: @Home network
Yahoo: Cablemodem user in Alexandria, VA.

2. Technique

A machine running pcAnywhere on the same subnet as the target is looking for other machines running pcAnywhere. This is not necessarily a attack but probably a misconfigured computer running pcAnywhere.

3. Intent

Benign. Probably a misconfigured client running pcAnywhere.

4. Active Targeting

Not necessarily. Since pcAnywhere just searches the local subnet, there is no evidence of active targeting by the user of the remote computer.

5. Evaluation

Probably nothing to worry about unless the victim is running pcAnywhere. Since the source machine is in fact on the same subnet as the destination, it is unlikely this is a deliberate/user initiated scan for pcAnywhere hosts.

Bot

Last Updated: July 24th, 2017

Upcoming Training

SANS San Antonio 2017	San Antonio, TX	Aug 06, 2017 - Aug 11, 2017	Live Event
SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
SANS vLive - SEC503: Intrusion Detection In-Depth	SEC503 - 201709,	Sep 11, 2017 - Oct 18, 2017	vLive
Baltimore Fall 2017 - SEC503: Intrusion Detection In-Depth	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	vLive
SANS London September 2017	London, United Kingdom	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Scottsdale SEC503	Scottsdale, AZ	Oct 02, 2017 - Oct 07, 2017	Community SANS
SANS October Singapore 2017	Singapore, Singapore	Oct 09, 2017 - Oct 28, 2017	Live Event
Community SANS Ottawa SEC503	Ottawa, ON	Oct 16, 2017 - Oct 21, 2017	Community SANS
SANS Berlin 2017	Berlin, Germany	Oct 23, 2017 - Oct 28, 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 Seattle 2017	Seattle, WA	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 Cyber Defense Initiative 2017	Washington, DC	Dec 12, 2017 - Dec 19, 2017	Live Event
SANS Security East 2018	New Orleans, LA	Jan 08, 2018 - Jan 13, 2018	Live Event
SANS Las Vegas 2018	Las Vegas, NV	Jan 28, 2018 - Feb 02, 2018	Live Event
SANS Dallas 2018	Dallas, TX	Feb 19, 2018 - Feb 24, 2018	Live Event
SANS OnDemand	Online	Anytime	Self Paced
SANS SelfStudy	Books & MP3s Only	Anytime	Self Paced