Global Information Assurance Certification Paper

Northcutt, I like this one. Note the analyst has done a good deal of research into the attackers and has looked for correlation activity. Clearly David knows his stuff, the analysis is free form but accurate. 88. *

David Hesprich

Incident Analysis 03/01/2000 – 03/31/2000

Incident Summary

CGI script fishing.

Log Data

```
128.175.13.74 - - [19/Mar/2000:11:47:23 -0500] "GET /cgi-
bin/counterfiglet/nc/f=;echo;echo%20{_begin-counterfiglet_};uname%20-a;id;w;echo%20{_end-
counterfiglet_};echo HTTP/1.0" 404 207 "-" "-"
128.175.13.74 - - [19/Mar/2000:21:49:25 -0500] "POST /cgi-bin/test-cgi HTTP/1.0" 404 207
"-" "-"
128.175.13.74 - - [20/Mar/2000:00:09:58 -0500] "POST /cgi-bin/phf?Qname=x%0a/bin/sh+-s%0a
HTTP/1.0" 404 207 "-" "-"
128.175.13.74 - - [20/Mar/2000:01:04:56 -0500] "GET /cgi-
bin/aglimpse/80|IFS=_;CMD=_echo\;echo_id-aglimpse\;uname_-a\;id;eval$CMD; HTTP/1.0" 404
207 "-" "-"
128.175.13.74 - - [20/Mar/2000:18:54:14 -0500] "POST /cgi-bin/perl HTTP/1.0" 404 207 "-"
"-"
128.175.13.74 - - [21/Mar/2000:00:35:16 -0500] "POST /cgi-bin/sh HTTP/1.0" 404 207 "-" "-
"
128.175.13.74 - - [21/Mar/2000:01:31:06 -0500] "GET /cgi-
bin/query?x=%3C%21%2D%2D%23%65%78%65%63%20%63%6D%64%3D%22%2F%75%73%72%2F%62%69%6E%2F%69%6
4%22%2D%2D%3E HTTP/1.0" 404 207 "-" "-"
128.175.13.74 - - [21/Mar/2000:02:34:30 -0500] "GET
/%3C%21%2D%2D%23%65%78%65%63%20%63%6D%64%3D%22%2F%75%73%72%2F%62%69%6E%2F%69%64%22%2D%2D%
3E/index.html HTTP/1.0" 404 207 "-" "-"

[19/Mar/2000:11:47:23] warning (25171): for host 128.175.13.74 trying to GET /cgi-
bin/counterfiglet/nc/f=;echo;echo {_begin-counterfiglet_};uname -a;id;w;echo {_end-
counterfiglet_};echo, cgieng_start_exec reports: cannot find CGI program
/usr/netscape/enterprise/cgi-bin/counterfiglet/nc/f=;echo;echo {_begin-
counterfiglet_};uname -a;id;w;echo {_end-counterfiglet_};echo (File not found)
[19/Mar/2000:21:49:26] warning (25171): for host 128.175.13.74 trying to POST /cgi-
bin/test-cgi, cgieng_start_exec reports: cannot find CGI program
/usr/netscape/enterprise/cgi-bin/test-cgi (File not found)
[20/Mar/2000:00:09:59] warning (25171): for host 128.175.13.74 trying to POST /cgi-
bin/phf, cgieng_start_exec reports: cannot find CGI program /usr/netscape/enterprise/cgi-
bin/phf (File not found)
[20/Mar/2000:01:04:56] warning (25171): for host 128.175.13.74 trying to GET /cgi-
bin/aglimpse/80|IFS=_;CMD=_echo\;echo_id-aglimpse\;uname_-a\;id;eval$CMD;,
cgieng_start_exec reports: cannot find CGI program /usr/netscape/enterprise/cgi-
bin/aglimpse/80|IFS=_;CMD=_echo\;echo_id-aglimpse\;uname_-a\;id;eval$CMD; (File not
found)
[20/Mar/2000:18:54:14] warning (25171): for host 128.175.13.74 trying to POST /cgi-
bin/perl, cgieng_start_exec reports: cannot find CGI program
/usr/netscape/enterprise/cgi-bin/perl (File not found)
[21/Mar/2000:00:35:16] warning (25171): for host 128.175.13.74 trying to POST /cgi-
bin/sh, cgieng_start_exec reports: cannot find CGI program /usr/netscape/enterprise/cgi-
bin/sh (File not found)
[21/Mar/2000:01:31:07] warning (25171): for host 128.175.13.74 trying to GET /cgi-
bin/query, cgieng_start_exec reports: cannot find CGI program
/usr/netscape/enterprise/cgi-bin/query (File not found)
```

Note that log times are EST.

Protagonist

Obfuscated Class C 333.444.555.666

Antagonist

strauss.udel.edu 128.175.13.74

Network

```
University of Delaware (NET-UDELNET)
   Network and Systems Services  192
   South Chapel Street, Room 240A
   Newark, DE 19716
   US

   Netname: UDELNET
   Netnumber: 128.175.0.0

   Coordinator:
      ,    (DJG2-ARIN)  grim@UDEL.EDU
      (302) 831-3700 (302) 831-1990 (FAX) (302)831-3717

   Domain System inverse mapping provided by:

   COPLAND.UDEL.EDU            128.175.13.92
   STRAUSS.UDEL.EDU            128.175.13.74
   NOC2.DCCS.UPENN.EDU         128.91.254.1
   NOC3.DCCS.UPENN.EDU         128.91.254.4

   Record last updated on 29-Oct-1999.
   Database last updated on 17-Apr-2000 17:38:08 EDT.

The ARIN Registration Services Host contains ONLY Internet
Network Information: Networks, ASN's, and related POC's.
Please use the whois server at rs.internic.net for DOMAIN related
Information and whois.nic.mil for NIPRNET Information.
```

Domain

```
The Data in Network Solutions' WHOIS database is provided by Network
Solutions for information purposes, and to assist persons in obtaining
information about or related to a domain name registration record.
Network Solutions does not guarantee its accuracy.  By submitting a
WHOIS query, you agree that you will use this Data only for lawful
purposes and that, under no circumstances will you use this Data to:
(1) allow, enable, or otherwise support the transmission of mass
unsolicited, commercial advertising or solicitations via e-mail
(spam); or  (2) enable high volume, automated, electronic processes
that apply to Network Solutions (or its systems).  Network Solutions
reserves the right to modify these terms at any time.  By submitting
this query, you agree to abide by this policy.

Registrant:
University of Delaware (UDEL-DOM)
   192 South Chapel Street
   Newark, DE 19716
   US

   Domain Name: UDEL.EDU

   Administrative Contact, Technical Contact, Zone Contact, Billing
Contact:
      Grim, Daniel J  (DJG2)  grim@UDEL.EDU
      University of Delaware
      192 South Chapel Street, Room 240A
      Newark, DE 19716
      302-831-3700 (302) 831-1990 (FAX) 302-831-3717
```

```
Record last updated on 08-Oct-1999.
Record expires on 22-Jun-2001.
Record created on 24-Jul-1985.
Database last updated on 16-Apr-2000 16:40:27 EDT.

Domain servers in listed order:

COPLAND.UDEL.EDU            128.175.13.92
STRAUSS.UDEL.EDU            128.175.13.74
NOC2.DCCS.UPENN.EDU         128.91.254.1
NOC3.DCCS.UPENN.EDU         128.91.254.4
```

Analysis

This particular trace comes from a Solaris box that is sparsely instrumented.

These logs, *grep*ped from a month's worth of logging, show a bit of "CGI fishing". Each attempt is very evidently highly targeted, and with purposeful intent – looking for exploitable software or misconfigurations in a Webserver's cgi-bin directory.

The speed of the scan, spread out over the period of three days, suggests a handcrafted approach. Another possibility is that it is part of a much larger scan that is iterating through tests performed across multiple Webservers.

The antagonist, "strauss.udel.edu," is one of the general-use UNIX hosts at the Univeristy of Delaware. It offers e-mail services, acts as an XDMP host, and supports classwork.

Had any of the above attempts successfully completed, they would represent a considerable threat to the integrity of the Webserver, as they would result in commands being executed at the privilege level that the Webserver's cgi-bin process executes at.

Similar detects was posted on GIAC http://www.sans.org/y2k/031700-1830.htm on March 17, 2000 – 1830; http://www.sans.org/y2k/032100-2000.htm on March 21, 2000 - 2000; http://www.sans.org/y2k/040400-030.htm on April 4, 2000; http://www.sans.org/y2k/040500-1000.htm on April 5, 2000 1000; http://www.sans.org/y2k/041300.htm on April 13, 2000; and http://www.sans.org/y2k/041400.htm on April 14, 2000.

Incident Analysis 03/19/2000 – 04/04/2000

Incident Summary

Access attempt to *rexecd* daemon service.

Log Data

```
tcpdlog:Mar 19 02:37:24 megaboz in.rexecd[27452]: refused connect from svstud.win.tue.nl
tcpdlog:Mar 19 05:16:16 megaboz in.rexecd[27997]: refused connect from svstud.win.tue.nl
tcpdlog:Mar 19 06:28:01 megaboz in.rexecd[28235]: refused connect from svstud.win.tue.nl
tcpdlog:Mar 19 06:30:26 megaboz in.rexecd[28244]: refused connect from svstud.win.tue.nl
tcpdlog:Mar 19 10:11:54 megaboz in.rexecd[28976]: refused connect from svstud.win.tue.nl

proftpdlog:Apr  4 16:22:35 megaboz proftpd[20042]: megaboz
(svstud.win.tue.nl[131.155.69.100]) - ANON ftp: Login successful.
proftpdlog:Apr  4 20:22:35 megaboz proftpd[20042]: megaboz
(svstud.win.tue.nl[131.155.69.100]) - FTP session closed.
```

Note that log times are EST.

Protagonist

Obfuscated Class C	333.444.555.666

Antagonist

svstud.win.tue.nl	131.155.69.100

Network

```
Eindhoven University of Technology (NET-TUEINDHOVEN)
   Den Dolech 2
   Eindhoven
   NETHERLANDS

   Netname: TUENET1
   Netnumber: 131.155.0.0

   Coordinator:
      Schillemans, Joop F.A.  (JFAS-ARIN)  rcjoop@URC.TUE.NL
      +31 40-472147

   Domain System inverse mapping provided by:

   TUEGATE.TUE.NL             131.155.2.3
   KWEETAL.TUE.NL             131.155.2.7
   NS1.SURFNET.NL             192.87.106.101

   Record last updated on 22-Aug-1994.
   Database last updated on 14-Apr-2000 17:40:43 EDT.

The ARIN Registration Services Host contains ONLY Internet
Network Information: Networks, ASN's, and related POC's.
Please use the whois server at rs.internic.net for DOMAIN related
Information and whois.nic.mil for NIPRNET Information.
```

Domain

```
Domain name:
      tue.nl

   Organisation:
      Technische Universiteit Eindhoven
      P.O. Box 513
```

```
   5600 MB Eindhoven

Administrative Contact:
   Joop Schillemans
   Phone: +31 40 2472147
   E-mail: rcjoop@urc.tue.nl

Technical Contact:
   Tonny van Lankveld
   Phone: +31 40 2472139
   E-mail: A.L.M.G.v.Lankveld@urc.tue.nl

Record last updated: 08-Feb-1995
Record maintained by: NL Domain Registry

Domain Nameservers:
   tuegate.tue.nl               131.155.2.3
   kweetal.tue.nl               131.155.2.7
   ns1.surfnet.nl               192.87.106.101
```

Analysis

This particular trace comes from a Solaris box that is sparsely instrumented.

Five *rexecd* attempts on the same day, blocked by TCP Wrappers. Somewhat ironic, as it's of note the apparent point of origin of the traffic is from the Eindhoven University of Technology in The Netherlands - the same university, where Wietse Venema, the author of TCP Wrappers, used to work.

This particular incident appears to be targeted and with intent.

The timing of the accesses is interesting: starting at 2:37.24 AM and looking at the time differentials: another attempt 2:38.52 later, 1:11.45 later, one following 0:02.25 later, and the last after a delay of 3:41.28. The irregular pattern could be a segment of a larger sweep, especially one where the scan targets were randomized, and perhaps also offset by a random delay. However, it's likely this was a handcrafted series of events. Perhaps a series of exploit attempts using slightly different approaches, albeit all unsuccessful.

It's not clear what the FTP access approximately two weeks later was meant to accomplish.

The *rexecd* service is classically abused. Most versions of it allow anyone to check if an account exists (by having a different message for "login incorrect" and "password incorrect"), and to execute commands without much logging. In addition, *rexecd* allows redirection of stderr stream to an arbitrary port on the client machine. This stream is opened by *rexecd* before authentication of the user.

A *grep* of other system logs (including Web access and error logs, and FTP access logs) revealed no other traffic from this source that might have indicated additional sorties against this protagonist.

A similar detect (also occurring on March 19) was posted on GIAC http://www.sans.org/y2k/032100-2000.htm on March 21, 2000 - 2000.

Incident Analysis 03/27/2000

Incident Summary

NetBIOS port access attempt.

Log Data

```
psentrylog:Mar 27 21:11:18 megaboz portsentry[23266]: attackalert: Connect from
host: 63.77.68.27/63.77.68.27 to UDP port: 161
psentrylog:Mar 27 21:11:18 megaboz portsentry[23266]: attackalert: Host 63.77.68
.27 has been blocked via wrappers with string: "ALL: 63.77.68.27"
psentrylog:Mar 27 21:11:18 megaboz portsentry[23266]: attackalert: Connect from
host: 63.77.68.27/63.77.68.27 to UDP port: 161
psentrylog:Mar 27 21:11:18 megaboz portsentry[23266]: attackalert: Host: 63.77.6
8.27 is already blocked. Ignoring
psentrylog:Mar 27 21:11:18 megaboz portsentry[23266]: attackalert: Connect from
host: 63.77.68.27/63.77.68.27 to UDP port: 161
psentrylog:Mar 27 21:11:18 megaboz portsentry[23266]: attackalert: Host: 63.77.6
8.27 is already blocked. Ignoring
```

Note that log times are EST.

Protagonist

Obfuscated Class C	333.444.555.666

Antagonist

unknown	63.77.68.27

Network

UUNET Technologies, Inc. (NETBLK-UUNET63)
3060 Williams Drive, Suite 601
Fairfax, Virginia 22031

Netname: UUNET63
Netblock: 63.64.0.0 - 63.99.255.255
Maintainer: UU

Coordinator:
UUnet, AlterNet - Technical Support (OA12-ARIN) <A
href="mailto:help@UUNET.UU.NET">help@UUNET.UU.NET</A>
() -

Domain System inverse mapping provided by:

AUTH03.NS.UU.NET	198.6.1.83
AUTH00.NS.UU.NET	198.6.1.65

ADDRESSES WITHIN THIS BLOCK ARE NON-PORTABLE

Record last updated on 22-Mar-2000.

Database last updated on 17-Apr-2000 05:36:03 EDT.

The ARIN Registration Services Host contains ONLY Internet
Network Information: Networks, ASN's, and related POC's.
Please use the whois server at rs.internic.net for DOMAIN related
Information and whois.nic.mil for NIPRNET Information.

Analysis

This particular trace comes from a Solaris box with rudimentary instrumentation.

This trace shows three rapid-fire (within hundredths of a second) access attempts to the NetBIOS port. The static source port is suspicious.

Use of NetBIOS across the Internet is discouraged for a number of reasons: it is very easy to accidentally share files without a password, accidentally giving anybody/everybody on the Internet access to them. It is easy to accidentally expose the entire hard-drive, giving everyone on the Internet the capability to completely control the vulnerable machine. Even if passwords are in use on the 'shares', a password guessing attack can attempt password combinations. Some versions of Windows are inherently vulnerable to exploitation even if passwords are in use. Lastly, a listening NetBIOS process can assist in identifying available system resources as well as the system type.

A *grep* of other system logs (including Web access and error logs, and FTP access logs) revealed no other traffic from this source that might have indicated additional sorties against this protagonist.

Incident Analysis 04/07/2000

Incident Summary

Multiple service access attempts.

Log Data

```
proftpdlog:Apr  7 10:05:30 megaboz proftpd[1902]: megaboz (adsl-63-199-169-
91.dsl.snfc21.pacbell.net[63.199.169.91]) - FTP session closed.

tcpdlog:Apr  7 10:05:30 megaboz in.proftpd[1902]: connect from adsl-63-199-169-
91.dsl.snfc21.pacbell.net
tcpdlog:Apr  7 10:05:31 megaboz in.telnetd[1903]: connect from adsl-63-199-169-
91.dsl.snfc21.pacbell.net
tcpdlog:Apr  7 10:05:37 megaboz in.rexecd[1905]: refused connect from adsl-63-199-169-
91.dsl.snfc21.pacbell.net
tcpdlog:Apr  7 10:05:38 megaboz in.rlogind[1906]: refused connect from adsl-63-199-169-
91.dsl.snfc21.pacbell.net
tcpdlog:Apr  7 10:05:39 megaboz in.rshd[1907]: refused connect from adsl-63-199-169-
91.dsl.snfc21.pacbell.net

proftpdlog:Apr  7 10:07:17 megaboz proftpd[1908]: megaboz (adsl-63-199-169-
91.dsl.snfc21.pacbell.net[63.199.169.91]) - FTP session closed.

tcpdlog:Apr  7 10:07:17 megaboz in.proftpd[1908]: connect from adsl-63-199-169-
91.dsl.snfc21.pacbell.net
tcpdlog:Apr  7 10:07:18 megaboz in.telnetd[1909]: connect from adsl-63-199-169-
91.dsl.snfc21.pacbell.net
tcpdlog:Apr  7 10:07:23 megaboz in.rlogind[1911]: refused connect from adsl-63-199-169-
91.dsl.snfc21.pacbell.net
tcpdlog:Apr  7 10:07:24 megaboz in.rexecd[1912]: refused connect from adsl-63-199-169-
91.dsl.snfc21.pacbell.net
tcpdlog:Apr  7 10:07:27 megaboz in.rshd[1913]: refused connect from adsl-63-199-169-
91.dsl.snfc21.pacbell.net
```

Note that log times are EST.

Protagonist

Obfuscated Class C	333.444.555.666

Antagonist

adsl-63-199-169-91.dsl.snfc21.pacbell.net	63.199.169.91

Network

Marc Jones (NETBLK-SBCIS72959)
310 Palisades Avenue
Santa Cruz, CA 95062
USA

Netname: SBCIS72959
Netblock: 63.199.169.88 - 63.199.169.95

Coordinator:
PBI IP Administrator (PIA2-ORG-ARIN) ip-admin@PBI.NET
415-278-5963

Fax- 415-442-4999

Record last updated on 23-Dec-1999.
Database last updated on 14-Apr-2000 17:40:43 EDT.

The ARIN Registration Services Host contains ONLY Internet
Network Information: Networks, ASN's, and related POC's.
Please use the whois server at rs.internic.net for DOMAIN related
Information and whois.nic.mil for NIPRNET Information.

Domain

Whois Server Version 1.1

Domain names in the .com, .net, and .org domains can now be registered
with many different competing registrars. Go to http://www.internic.net
for detailed information.

Domain Name: PACBELL.NET
Registrar: NETWORK SOLUTIONS, INC.
Whois Server: whois.networksolutions.com
Referral URL: www.networksolutions.com
Name Server: NS2.PBI.NET
Name Server: NS1.PBI.NET
Updated Date: 07-apr-2000

>>> Last update of whois database: Fri, 14 Apr 00 04:27:15 EDT <<<

The Registry database contains ONLY .COM, .NET, .ORG, .EDU domains and
Registrars.

Analysis

This particular trace comes from a Solaris box that is only barely instrumented.

This trace appears to be a fairly straightforward selective port scan sourcing from an ADSL customer. Note the timing is somewhat irregular (1-6-1-1 seconds in the first group, and 1-5-1-3 in the second group), but still close enough to suggest some sort of automation. The sequential port numbers suggest the antagonist is a lightly loaded box. Also of note is the skipped port number between the *telnetd* and *rlogind* ports, which strongly suggests that one other port was scanned between those two that was not logged.

A *grep* of other system logs (including Web access and error logs, and FTP access logs) revealed no other traffic from this source that might have indicated additional sorties against this protagonist.

Port scans can reveal critical system information and expose potential services for exploitation – the R-commands being fished for here are classically vulnerable, and the *telnetd* service helps identify this system as a likely UNIX host as well as provide a method for username/password guessing attempts.

Incident Analysis 04/11/2000

Incident Summary

NETBIOS port access attempt.

Log Data

```
psentrylog:Apr 11 15:03:42 megaboz portsentry[3422]: attackalert: Connect from host:
m20677145097.austin.cc.tx.us/206.77.145.97 to UDP port: 161
psentrylog:Apr 11 15:03:42 megaboz portsentry[3422]: attackalert: Host 206.77.145.97 has
been blocked via wrappers with string: "ALL: 206.77.145.97"
```

Note that log times are EST.

Protagonist

Obfuscated Class C	333.444.555.666

Antagonist

m20677145097.austin.cc.tx.us	206.77.145.97

Network

Austin Community College (NETBLK-AUSTIN-CC)
5390 Middle Fiskville Road
Austin, TX 78752
US

Netname: AUSTIN-CC
Netblock: 206.77.144.0 - 206.77.151.0

Coordinator:
Haney, Roger (RH1527-ARIN) rhaney@AUSTIN.CC.TX.US
512-223-7171

Record last updated on 02-May-1996.
Database last updated on 14-Apr-2000 17:40:43 EDT.

The ARIN Registration Services Host contains ONLY Internet
Network Information: Networks, ASN's, and related POC's.
Please use the whois server at rs.internic.net for DOMAIN related
Information and whois.nic.mil for NIPRNET Information.

Domain

University of Texas System Office of Telecommunication Services (NETBLK-THENET-CIDR-5) THENET-CIDR-5
206.76.0.0 - 206.77.255.0
Austin Community College (NETBLK-AUSTIN-CC) AUSTIN-CC
206.77.144.0 - 206.77.151.0

To single out one record, look it up with "!xxx", where xxx is the handle, shown in parenthesis following the name, which comes first.

The ARIN Registration Services Host contains ONLY Internet Network Information: Networks, ASN's, and related POC's. Please use the whois server at rs.internic.net for DOMAIN related Information and whois.nic.mil for NIPRNET Information.

Analysis

This particular trace comes from a Solaris box that is only barely instrumented.

This trace shows a single access attempt to the NETBIOS port apparently sourcing from a system located at Austin Community College.

Use of NetBIOS across the Internet is discouraged for a number of reasons: it is very easy to accidentally share files without a password, accidentally giving anybody/everybody on the Internet access to them. It is easy to accidentally expose the entire hard-drive, giving everyone on the Internet the capability to completely control the vulnerable machine. Even if passwords are in use on the 'shares', a password guessing attack can attempt password combinations. Some versions of Windows are inherently vulnerable to exploitation even if passwords are in use. Lastly, a listening NetBIOS process can assist in identifying available system resources as well as the system type.

A *grep* of other system logs (including Web access and error logs, and FTP access logs) revealed no other traffic from this source that might have indicated additional sorties against this protagonist.

Incident Analysis 03/24/2000

Incident Summary

Access attempt to unserved ports.

From "Global Incident Analysis Center: Detects Analyzed 3/25/00".

Log Data

```
Mar 24 01:54:58 cc1014244-a kernel:
securityalert: tcp if=ef0 from 24.3.57.38:11111 to 24.3.21.199 on unserved port 12345
Mar 24 03:14:13 cc1014244-a kernel:
securityalert: tcp if=ef0 from 171.214.113.228:2766 to 24.3.21.199 on unserved port 1243
Mar 24 04:45:01 cc1014244-a kernel:
securityalert: tcp if=ef0 from 208.61.109.243:3578 to 24.3.21.199 on unserved port 1243
Mar 24 04:45:06 cc1014244-a kernel:
securityalert: tcp if=ef0 from 208.61.109.243:3832 to 24.3.21.199 on unserved port 27347
Mar 24 05:40:42 cc1014244-a kernel:
securityalert: udp if=ef0 from 24.24.100.172:2147 to 24.3.21.199 on unserved port 137
Mar 24 14:56:08 cc1014244-a kernel:
securityalert: udp if=ef0 from 63.17.79.40:4294 to 24.3.21.199 on unserved port 137
Mar 24 17:20:44 cc1014244-a kernel:
securityalert: tcp if=ef0 from 62.6.100.45:1828 to 24.3.21.199 on unserved port 27374
Mar 24 20:50:47 cc1014244-a kernel:
securityalert: tcp if=ef0 from 194.27.62.179:4857 to 24.3.21.199 on unserved port 27374
```

Protagonist

Unknown @Home user	24.3.21.199

Antagonists

cc940888-a.owml1.md.home.com	24.3.57.38
ABD671E4.ipt.aol.com	171.214.113.228
adsl-61-109-243.sdf.bellsouth.net	208.61.109.243
m8hDs1n172.midsouth.rr.com	24.24.100.172
1Cust40.tnt33.dfw5.da.uu.net	63.17.79.40
host62-6-100-45.btinternet.com	62.6.100.45
p179.eng.deu.edu.tr	194.27.62.179

Analysis

This trace sourced from an @Home user.

The selection of ports is of interest, all are classical trojan ports (with the exception of port 137/udp, which is not only a good indicator of a vulnerable system, but also an indicator of a Windows-based system).

137/udp	Netbios
1243/tcp	BackDoor-G, SubSeven, SubSeven Apocalypse
12345/tcp	GabanBus, NetBus, Pie Bill Gates, X-bill
27347/tcp	*<unknown>*
27374/tcp	SubSeven

The source networks are somewhat interesting, being an assortment of dial-up, ADSL, or similar addresses. However, the last address (194.27.62.179) is somewhat interesting, belonging to a block of addresses in Turkey.

Given the broad, irregular spacing of the timing and that few of the ports repeat it is somewhat unlikely that this is a source-spoofed *nmap* scan. Since @Home (as its name suggests) caters mostly to home users, most of whom are likely to be unsophisticated users running a Microsoft Windows-based platform, it is not unsurprising to see a great deal of NETBIOS and Windows trojan activity directed towards @Home-owned network blocks.

A similar scan attempt trace sourcing from 24.24.100.172 was posted on GIAC http://www.sans.org/y2k/032300-2000.htm on March 23, 2000 - 2000 and http://www.sans.org/y2k/032600-2000.htm March 26, 2000 1700.

Incident Analysis 03/22/2000 – 03/23/2000

Incident Summary

Multiple access attempts to port 116 (NNTP).

From "Global Incident Analysis Center: Detects Analyzed 3/26/00".

Log Data

```
Mar 22 13:23:36 box.at.victim.com /ipmon[4872]: 13:23:36.638478 le0 @0:19 b
24.0.94.130,38945 -> IP.OF.VICTIM.COM,119 PR tcp len 20 44 -S Mar 22 13:23:37
box.at.victim.com /ipmon[4872]: 13:23:37.315117 le0 @0:19 b 24.0.94.130,38945 ->
IP.OF.VICTIM.COM,119 PR tcp len 20 40 -R Mar 22 13:23:37 box.at.victim.com /ipmon[4872]:
13:23:37.326922 le0 @0:19 b 24.0.94.130,39317 -> IP.OF.VICTIM.COM,119 PR tcp len 20 44 -S
Mar 22 13:23:38 box.at.victim.com /ipmon[4872]: 13:23:38.312697 le0 @0:19 b
24.0.94.130,39317 -> IP.OF.VICTIM.COM,119 PR tcp len 20 40 -R Mar 22 18:04:02
box.at.victim.com /ipmon[4872]: 18:04:01.661131 le0 @0:19 b 24.0.94.130,59273 ->
IP.OF.VICTIM.COM,119 PR tcp len 20 44 -S Mar 22 18:04:03 box.at.victim.com /ipmon[4872]:
18:04:03.188819 le0 @0:19 b 24.0.94.130,59273 -> IP.OF.VICTIM.COM,119 PR tcp len 20 40 -R
Mar 22 18:04:03 box.at.victim.com /ipmon[4872]: 18:04:03.210320 le0 @0:19 b
24.0.94.130,60187 -> IP.OF.VICTIM.COM,119 PR tcp len 20 44 -S Mar 22 18:04:04
box.at.victim.com /ipmon[4872]: 18:04:03.811455 le0 @0:19 b 24.0.94.130,60187 ->
IP.OF.VICTIM.COM,119 PR tcp len 20 40 -R Mar 22 22:48:17 box.at.victim.com /ipmon[4872]:
22:48:16.835881 le0 @0:19 b 24.0.94.130,50230 -> IP.OF.VICTIM.COM,119 PR tcp len 20 44 -S
Mar 22 22:48:18 box.at.victim.com /ipmon[4872]: 22:48:18.161571 le0 @0:19 b
24.0.94.130,50230 -> IP.OF.VICTIM.COM,119 PR tcp len 20 40 -R Mar 22 22:48:18
box.at.victim.com /ipmon[4872]: 22:48:18.173064 le0 @0:19 b 24.0.94.130,50678 ->
IP.OF.VICTIM.COM,119 PR tcp len 20 44 -S Mar 22 22:48:19 box.at.victim.com /ipmon[4872]:
22:48:18.986828 le0 @0:19 b 24.0.94.130,50678 -> IP.OF.VICTIM.COM,119 PR tcp len 20 40 -R
Mar 23 03:20:08 box.at.victim.com /ipmon[4872]: 03:20:07.585219 le0 @0:19 b
24.0.94.130,62610 -> IP.OF.VICTIM.COM,119 PR tcp len 20 44 -S Mar 23 03:20:08
box.at.victim.com /ipmon[4872]: 03:20:08.045238 le0 @0:19 b 24.0.94.130,62610 ->
IP.OF.VICTIM.COM,119 PR tcp len 20 40 -R Mar 23 03:20:08 box.at.victim.com /ipmon[4872]:
03:20:08.056194 le0 @0:19 b 24.0.94.130,62931 -> IP.OF.VICTIM.COM,119 PR tcp len 20 44 -S
Mar 23 03:20:09 box.at.victim.com /ipmon[4872]: 03:20:08.858156 le0 @0:19 b
24.0.94.130,62931 -> IP.OF.VICTIM.COM,119 PR tcp len 20 40 -R Mar 23 07:46:43
box.at.victim.com /ipmon[4872]: 07:46:42.379020 le0 @0:19 b 24.0.94.130,61302 ->
IP.OF.VICTIM.COM,119 PR tcp len 20 44 -S Mar 23 07:46:44 box.at.victim.com /ipmon[4872]:
07:46:43.418154 le0 @0:19 b 24.0.94.130,61302 -> IP.OF.VICTIM.COM,119 PR tcp len 20 40 -R
Mar 23 07:46:44 box.at.victim.com /ipmon[4872]: 07:46:43.442809 le0 @0:19 b
24.0.94.130,62218 -> IP.OF.VICTIM.COM,119 PR tcp len 20 44 -S Mar 23 07:46:44
box.at.victim.com /ipmon[4872]: 07:46:44.091157 le0 @0:19 b 24.0.94.130,62218 ->
IP.OF.VICTIM.COM,119 PR tcp len 20 40 -R
```

Protagonist

Obfuscated @Home user	IP.OF.VICTIM.COM

Antagonist

authorized-scan.security.home.net	24.0.94.130

Analysis

This trace almost certainly sourced from an @Home user.

@Home is an Internet service that provides high bandwidth Internet access over cable TV cables.

@Home has a good abuse policy but often does not enforce it. This allows spammers based at @Home to run rampant. In addition, computers connected to the Internet via

@Home are often misconfigured to act as relays. These are quickly discovered by spammers and used to relay spam. As part of the measures to avoid a Usenet Death Penalty (UDP), @Home is scanning its users for open NNTP port relays.

Similar scans have been submitted to GIAC: http://www.sans.org/y2k/030500.htm on March 5, 2000; http://www.sans.org/y2k/030800.htm on March 8, 2000; http://www.sans.org/y2k/031000.htm on March 10, 2000; and http://www.sans.org/y2k/032800.htm on March 28, 2000 900.

Incident Analysis 03/25/2000

Incident Summary

Access attempt to unserved ports.

From **"**Global Incident Analysis Center: Detects Analyzed 3/26/00".

Log Data

All log entries are from 3/25/2000.

```
Message: Deny inbound tcp src outside:200.249.238.9/8803
dst DMZ:my.net.60.98/5317 13:26
Message: Deny inbound tcp src outside:200.249.238.9/8803
dst DMZ:my.net.60.98/7877 13:31
Message: Deny inbound tcp src outside:200.249.238.9/8803
dst DMZ:my.net.60.98/18117 13:39
Message: Deny inbound tcp src outside:200.249.238.9/8803
dst DMZ:my.net.60.98/15557 13:53
Message: Deny inbound tcp src outside:200.249.238.9/8803
dst DMZ:my.net.60.98/20677 13:56
Message: Deny inbound tcp src outside:200.249.238.9/8803
dst DMZ:my.net.60.98/25797 14:07
Message: Deny inbound tcp src outside:200.249.238.9/8803
dst DMZ:my.net.60.98/23237 14:19
Message: Deny inbound tcp src outside:200.249.238.9/8803
dst DMZ:my.net.60.98/25797 14:29
Message: Deny inbound tcp src outside:200.249.238.9/8803
dst DMZ:my.net.60.98/28357 14:39
Message: Deny inbound tcp src outside:200.249.238.9/8803
dst DMZ:my.net.60.98/28357 14:39
```

Protagonist

Obfuscated	my.net.60.98

Antagonist

irc.elogica.com.br	200.249.238.9

Network

RNP (Brazilian Research Network) (NETBLK-BRAZIL-BLK2)
Rua Pio XI, 1500
Sao Paulo, 05468-901
BR

Netname: BRAZIL-BLK2
Netblock: 200.128.0.0 - 200.255.255.0
Maintainer: RNP

Coordinator:

Gomide, Alberto Courrege (ACG8-ARIN) <A
href="mailto:gomide@nic.br">gomide@nic.br</A>
+55 11 9308-5675 (FAX) +55 11 3645-2420

Domain System inverse mapping provided by:

NS.DNS.BR	143.108.23.2
NS1.DNS.BR	200.255.253.234
NS2.DNS.BR	200.19.119.99

Record last updated on 13-Apr-1999.
Database last updated on 17-Apr-2000 05:36:03 EDT.

The ARIN Registration Services Host contains ONLY Internet
Network Information: Networks, ASN's, and related POC's.
Please use the whois server at rs.internic.net for DOMAIN related
Information and whois.nic.mil for NIPRNET Information.

Analysis

This log shows a slow (spaced on a 5-8-4-3-11-12-10-10-0 second pattern) TCP port scan. The static source port suggests that the packets were crafted.

The destination port selection is unusual, as it does not appear to correspond to anything in particular, either services or common trojans.

One might wonder if this is the return response from a TCP client-server application that is being thwarted by NAT.

Incident Analysis 04/09/2000

Incident Summary

Multiple access attempts to port 116 (NNTP).

From "Global Incident Analysis Center: Detects Analyzed 4/12/00".

Log Data

```
Apr 9 09:14:11 bigfoot tcplog: nntp connection attempt from 213.47.7.92
Apr 9 09:14:11 picard tcplog: nntp connection attempt from 213.47.7.92
```

Protagonists

Obfuscated	bigfoot
Obfuscated	picard

Antagonist

Unknown	213.47.7.92

Network

```
inetnum:     213.47.0.0 - 213.47.15.255
netname:     VIE-11-CUSTOMER-CABLE
descr:       chello Austria
descr:       Customers in Vienna headend 11
country:     AT
admin-c:     HMCB1-RIPE
tech-c:      HMCB1-RIPE
status:      ASSIGNED PA
notify:      hostmaster@chello.at
mnt-by:      CHELLO-MNT
changed:     hostmaster@chello.at 20000225
source:      RIPE

route:       213.46.0.0/15
descr:       AT-TELEKABEL-19991230
descr:       NL-CHELLO-991108
origin:      AS6830
mnt-by:      CHELLO-MNT
changed:     sbaumann@chello.at 20000303
source:      RIPE

role:        Hostmaster Chello Broadband
address:     Chello Broadband
address:     Internet Services
address:     Erlachgasse 116
address:     A-1100 Wien
address:     Austria
phone:       +43 1 96060
fax-no:      +43 1 96060 716
e-mail:      hostmaster@chello.at
trouble:     help@chello.at
admin-c:     AK991-RIPE
tech-c:      SB9000-RIPE
tech-c:      MH392-RIPE
tech-c:      MG872-RIPE
tech-c:      AK991-RIPE
nic-hdl:     HMCB1-RIPE
notify:      hostmaster@chello.at
notify:      hm-dbm-msgs@ripe.net
mnt-by:      CHELLO-MNT
```

```
changed:      sbaumann@chello.at 19991129
source:       RIPE
```

Analysis

This log is most likely a scan looking for open NNTP hosts or proxies.

NNTP proxies are especially attractive to spammers, since they usually have little or no authentication and are typically poorly monitored.

This scan appears to source from a broadband provider's address space. If the target is a member of that provider's address space, the scan may be a "valued added" service to look for open relays in their client's systems (to avoid punitive measures such as a Usenet Death Penalty being leveled by the community at large).

If the scan originates from a completely foreign network, it may be an attempt to map public, proxy, and/or vulnerable NNTP servers that may be exploited.

Incident Analysis 04/13/2000

Incident Summary

Multiple access attempts to port 12345 (NetBus).

From "Global Incident Analysis Center: Detects Analyzed 4/15/00".

Log Data

```
Apr 13 15:27:37 hostc portsentry[15996]: attackalert:
Connect from host: R0621.RESNET.CORNELL.EDU/128.253.27.174
to TCP port: 12345
Apr 13 15:29:54 hostp portsentry[522]: attackalert:
Connect from host: R0621.RESNET.CORNELL.EDU/128.253.27.174
to TCP port: 12345
Apr 13 15:29:54 hostp portsentry[522]: attackalert:
Connect from host: R0621.RESNET.CORNELL.EDU/128.253.27.174
to TCP port: 12345
Apr 13 15:29:54 hostr portsentry[418]: attackalert:
Connect from host: R0621.RESNET.CORNELL.EDU/128.253.27.174
to TCP port: 12345
Apr 13 15:29:54 hostb portsentry[334]: attackalert:
Connect from host: R0621.RESNET.CORNELL.EDU/128.253.27.174
to TCP port: 12345
Apr 13 15:37:00 dns1 portsentry[438328]: attackalert:
Connect from host: R0621.RESNET.CORNELL.EDU/128.253.27.174
to TCP port: 12345
Apr 13 15:37:01 dns2 portsentry[2259]: attackalert:
Connect from host: R0621.RESNET.CORNELL.EDU/128.253.27.174
to TCP port: 12345
Apr 13 15:37:01 dns3 portsentry[6017]: attackalert:
Connect from host: R0621.RESNET.CORNELL.EDU/128.253.27.174
to TCP port: 12345
Apr 13 15:37:14 dns1 portsentry[438328]: attackalert:
Connect from host: R0621.RESNET.CORNELL.EDU/128.253.27.174
to TCP port: 12345
```

Protagonists

Obfuscated	dns1
Obfuscated	dns2
Obfuscated	dns3
Obfuscated	hostb
Obfuscated	hostc
Obfuscated	hostp
Obfuscated	hostr

Antagonist

R0621.RESNET.CORNELL.EDU 128.253.27.174

Network

```
Cornell University (NET-CCS-NET)
```

```
   Cornell Information Technologies
   Network Resources
   143 Caldwell Hall
   Ithaca, NY 14853

   Netname: CCS-NET
   Netnumber: 128.253.0.0

   Coordinator:
      Redick, Don  (DR69-ARIN)  dredick@NMC.CIT.CORNELL.EDU
      607 255-9900

   Domain System inverse mapping provided by:

   BIGRED.CIT.CORNELL.EDU      128.253.180.2
   SEISMO.CSS.GOV              140.162.1.25
   CAYUGA.CS.ROCHESTER.EDU     192.5.53.209
   DNS.CIT.CORNELL.EDU                 192.35.82.50

   Record last updated on 15-Mar-1994.
   Database last updated on 17-Apr-2000 17:38:08 EDT.

The ARIN Registration Services Host contains ONLY Internet
Network Information: Networks, ASN's, and related POC's.
Please use the whois server at rs.internic.net for DOMAIN related
Information and whois.nic.mil for NIPRNET Information.
```

Domain

```
The Data in Network Solutions' WHOIS database is provided by Network
Solutions for information purposes, and to assist persons in obtaining
information about or related to a domain name registration record.
Network Solutions does not guarantee its accuracy.  By submitting a
WHOIS query, you agree that you will use this Data only for lawful
purposes and that, under no circumstances will you use this Data to:
(1) allow, enable, or otherwise support the transmission of mass
unsolicited, commercial advertising or solicitations via e-mail
(spam); or  (2) enable high volume, automated, electronic processes
that apply to Network Solutions (or its systems).  Network Solutions
reserves the right to modify these terms at any time.  By submitting
this query, you agree to abide by this policy.

Registrant:
Cornell University (CORNELL-DOM)
   Cornell Information Technologies
   Network Operations Center 100 CCC
   Ithaca, NY 14853

   Domain Name: CORNELL.EDU

   Administrative Contact, Billing Contact:
      Pishioneri, Philip  (PP6437)  pgp1@CORNELL.EDU
      Cornell University
      425 Rhodes Hall
      Cornell University
      Ithaca, NY 14853
      +1 607 255-9495 (FAX) +1 607 255-8169
   Technical Contact, Zone Contact:
      Eckstrom, Daniel  (DE723)  de10@CORNELL.EDU
      Cornell Information Technologies
      445 Rhodes Hall
      Ithaca, NY 14853
      (607) 255-9900

   Record last updated on 04-Oct-1999.
   Record expires on 22-Aug-2000.
   Record created on 15-Jul-1985.
   Database last updated on 16-Apr-2000 16:41:52 EDT.

   Domain servers in listed order:
```

BIGRED.CIT.CORNELL.EDU	128.253.180.2
DNS.CIT.CORNELL.EDU	192.35.82.50
SEISMO.CSS.GOV	140.162.8.25
CAYUGA.CS.ROCHESTER.EDU	192.5.53.209

Analysis

This is a simple scan for the NetBus trojan. The timing (within a few seconds) suggests an automated scan.

The source ports appear to intentionally randomized, as the sequencing would suggest that the antagonist system is far busier than it could possibly be – it's doubtful it could be initiating that many connections to roll over the ephemeral port counters while still hammering the protagonist network that quickly.

The source domain of "R0621.RESNET.CORNELL.EDU" would suggest it sourcing from a residence hall or office. This is probably sourcing from a student dorm at Cornell.

NetBus is a particularly popular client/server application that allows the remote user to have a great deal of control over the trojanized system.

Last Updated: September 24th, 2017

Upcoming Training

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
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
SANS Seattle 2017	Seattle, WA	Oct 30, 2017 - Nov 04, 2017	Live Event
SANS San Diego 2017	San Diego, CA	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 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
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 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	Tysons, 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 OnDemand	Online	Anytime	Self Paced
SANS SelfStudy	Books & MP3s Only	Anytime	Self Paced