

## Re: Help – a possible bot

**Source:** <http://www.derkeiler.com/Mailing-Lists/securityfocus/incidents/2002-11/0144.html>

---

**From:** Moshe Aelion ([ma0934@hotmail.com](mailto:ma0934@hotmail.com))

**Date:** 11/22/02

From: "Moshe Aelion" <[ma0934@hotmail.com](mailto:ma0934@hotmail.com)>  
To: "Emeric Miszti" <[emeric@uksecurityonline.com](mailto:emeric@uksecurityonline.com)>  
Date: Fri, 22 Nov 2002 16:01:36 +0200

Hi Emeric

Analyzing the PC, it does not seem it's infected by Opaserv. There is no suspicious file with \*scr\* anywhere.

Still, like you said, wht's worrying is that the PC is responding to the port probes. Apparently traffic to port 137 is blocked – so maybe it's penetrating from another port, of from an allowed program; but the PC is responding, which means SOMETHING inside is listening, then responding (very quickly). Also, when the Internet is on-line, the explorer and svchost processes are constantly active, with I/O of 25–30 kbps. This ceases when I go off-line.

Can anyone help? Thanks in advance

Moshe

----- Original

Message -----

From: Emeric Miszti

To: Moshe Aelion

Cc: incidents @ security focus

Sent: Saturday, November 16, 2002 12:59 PM

Subject: Re: Help – a possible bot

Hi Moshe,

What you are seeing with the incoming port 137 UDP requests is probably the Opeserv worm. Have a look at

<http://antivirus.about.com/library/weekly/aa100102a.htm>.

Everyone is seeing a lot of these at the moment and if you have a look at <http://isc.incidents.org/> then you will see that port 137 is far and away the most attacked port at the moment.

You can easily identify this kind of activity because the source port of

## SecurityFocus Incidents: Re: Help – a possible bot

normal UDP 137 traffic is 137 and the destination is port 137. With the worm activity the source port becomes something above 1024 with the destination as 137.

Looking at your fport traces, etc it doesn't look like your PC is infected by Opaserv but what is worrying is that you may be responding to the port probes, thus making you a target for further attack and that may explain the high usage on svchost!

Make sure that you are not infected by Opaserv by checking through the details provided by anti-virus companies such as <http://securityresponse.symantec.com/avcenter/venc/data/w32.opaserv.worm.htm>

1

Since the PC has been previously hacked I would be very suspicious anyway and wouldn't rely on the firewall doing its job properly. Dameware is a total remote control package so anything could have been installed. Personally I would rebuild the PC and then install a good firewall on a clean box. That is the only way you can ever be 100% sure you are clean.

Regards

--

Emeric Miszti  
UK Security Online  
<http://www.uksecurityonline.com>  
Tel No: 0870 088 5689  
Fax No: 0870 706 2162  
PGP Public Key available at  
<http://www.uksecurityonline.com/emeric.asc>  
On Fri, 2002-11-15 at 20:11, Moshe Aelion wrote:

```
> Hi everybody
>
> Two weeks ago, the NAT/ICMP computer on our LAN got compromised; the
hacked
> installed DameWare and was trying to work on the computer. It was
discovered
> within about 10 minutes. I then installed ZoneAlarm Pro.
>
> The problem is, I am detecting a suspicious hit/respond activity, which,
in
> my opinion, points to an active bot. Here's the evidence: when inspecting
ZA
> logs, you can see a blocked scan (coming every couple of minutes, from
> arbitrary addresses - I bet they're spoofed - and soon after, the computer
> responds with a (blocked) attempt to communicated with that address. This
> points to an active bot (in my opinion), since, although ZA claims it
> blocked the incoming attempt, the computer immediately tries to respond -
> therefore SOMETHING inside did get a message.
>
> I did a lot of port blocking, foundation fport tracking, netstat -an, and
> couldn't find anything extraordinary. I installed PestPatrol and Trojan
> Remover, they discovered nothing. (Except fport which I used). The
> "HKEY_localmachine_software...Microsoft\...currentversion\run" registry
key
> doesn't show anything suspicious.
```

Re: Help – a possible bot

## SecurityFocus Incidents: Re: Help – a possible bot

```
>
> I do notice, though, that svchost is unusually active - doing about 25k
> read/write I/O per second, with nothing running.
> I did a lot of port blocking and couldn't stop the hit/response
phenomenon.
> I also stopped several processes and services and the phenomenon didn't
> stop.
>
> I'm attaching here the ZA log. The incoming attempt and the response are
> denoted with "<--".
>
> I'm also attaching the netstat -an and fport scan outputs.
>
> Thanking any assistance in advance
>
> Moshe
>
> =====          ZA log          =====
> 1  FWIN,  21:55:54, 66.139.182.144:1065,   my.net.237.99:137,UDP  <--
> 2  FWOUT, 21:55:56, my.net.237.99:1025,   66.139.182.144:137,UDP <--
> 3  FWIN,  21:58:18, 213.9.242.122:1029,   my.net.237.99:137,UDP  <--
> 4  FWOUT, 21:58:18, my.net.237.99:1025,   213.9.242.122:137,UDP <--
> 5  FWIN,  21:59:54, 192.168.0.5: 138,    192.168.0.255:138,UDP
> 6  FWIN,  22:00:38, 212.179.237.86:1026,   my.net.237.99:137,UDP
> 7  FWIN,  22:00:38, 212.179.209.67:  0,    my.net.237.99:0,ICMP
> (type:8/subtype:0)
> 8  ACCESS,22:01:52,RuLaunch blocked from connecting to Internet
> (216.49.88.100:HTTP)
> 9  FWIN,  22:02:04, 64.231.129.73:1030,   my.net.237.99:137,UDP
> 10 FWIN,  22:02:44, 61.228.26.161:1027,   my.net.237.99:137,UDP
> 11 FWIN,  22:02:56, 62.94.131.238:3375,   my.net.237.99:6588,TCP
(flags:S)
> 12 FWIN,  22:07:34, 200.76.64.2:62695,   my.net.237.99:137,UDP  <--
> 13 FWOUT, 22:07:40, my.net.237.99:1025,   200.76.64.2:137,UDP  <--
> 14 ACCESS,22:07:52,RuLaunch blocked from connecting to Internet
> (216.49.88.100:HTTP)
> 15 FWIN,  22:09:02, 200.67.76.211:1026,   my.net.237.99:137,UDP
> 16 FWIN,  22:10:40,140.186.157.226:6522,   my.net.237.99:137,UDP  <--
> 17 FWOUT, 22:10:40, my.net.237.99:1025,   140.186.157.226:137,UDP <--
> 18 FWIN,  22:10:58, 12.22.205.3:10647,   my.net.237.99:137,UDP  <--
> 19 FWOUT, 22:10:58, my.net.237.99:1025,   12.22.205.3:137,UDP  <--
> 20 FWIN,  22:11:46, 68.67.228.47:1132,   my.net.237.99:137,UDP
> 21 ACCESS,22:11:54,RuLaunch blocked from connecting to Internet
> (216.49.88.100:HTTP)
> 22 FWIN,  22:12:14, 200.75.14.169:1025,   my.net.237.99:137,UDP  <--
> 23 FWOUT, 22:12:16, my.net.237.99:1025,   200.75.14.169:137,UDP  <--
> 24 FWIN,  22:12:20, 80.235.53.242:30150,   my.net.237.99:137,UDP
> 25 FWIN,  22:13:44, 200.56.237.243:1026,   my.net.237.99:137,UDP
> 26 FWIN,  22:13:52, 64.110.231.28:1025,   my.net.237.99:137,UDP
> 27 ACCESS,22:13:54,RuLaunch blocked from connecting to Internet
> (216.49.88.100:HTTP)
> 28 FWIN,  22:15:40, 200.63.158.210:1025,   my.net.237.99:137,UDP
> 29 FWIN,  22:17:10, 203.99.155.122:1027,   my.net.237.99:137,UDP
> 30 FWIN,  22:19:16, 166.114.241.42:1037,   my.net.237.99:137,UDP  <--
> 31 FWOUT, 22:19:16, my.net.237.99:1025,   166.114.241.42:137,UDP  <--
> 32 FWIN,  22:21:28, 161.132.196.30:1027,   my.net.237.99:137,UDP
> 33 ACCESS,22:21:54,RuLaunch blocked from connecting to Internet
> (216.49.88.100:HTTP)
> 34 FWIN,  22:22:04, 209.86.1.157:1029,   my.net.237.99:137,UDP
> ===== end of ZA log
> =====
>
```

## SecurityFocus Incidents: Re: Help – a possible bot

```
> Note: the 10.0.0.1:3028 to 10.0.0.138:1723 link is the ADSL ptp.
>
> ===== "netstat -an"
> output=====
>
> Active Connections
>
> Proto Local Address           Foreign Address         State
> TCP    0.0.0.0:135             0.0.0.0:0              LISTENING
> TCP    0.0.0.0:445             0.0.0.0:0              LISTENING
> TCP    0.0.0.0:1025            0.0.0.0:0              LISTENING
> TCP    0.0.0.0:1026            0.0.0.0:0              LISTENING
> TCP    0.0.0.0:1723            0.0.0.0:0              LISTENING
> TCP    0.0.0.0:3006            0.0.0.0:0              LISTENING
> TCP    0.0.0.0:3028            0.0.0.0:0              LISTENING
> TCP    10.0.0.1:3028           10.0.0.138:1723       ESTABLISHED
> TCP    10.0.0.1:7732           0.0.0.0:0              LISTENING
> TCP    192.168.0.1:139         0.0.0.0:0              LISTENING
> TCP    192.168.0.1:3002        0.0.0.0:0              LISTENING
> TCP    192.168.0.1:3003        0.0.0.0:0              LISTENING
> TCP    192.168.0.1:3004        0.0.0.0:0              LISTENING
> TCP    192.168.0.1:14810       0.0.0.0:0              LISTENING
> TCP    my.net.217.125:13145    0.0.0.0:0              LISTENING
> UDP    0.0.0.0:135             *:*
> UDP    0.0.0.0:445             *:*
> UDP    0.0.0.0:1027            *:*
> UDP    0.0.0.0:3001            *:*
> UDP    0.0.0.0:3239            *:*
> UDP    0.0.0.0:3240            *:*
> UDP    10.0.0.1:500            *:*
> UDP    10.0.0.1:6979           *:*
> UDP    192.168.0.1:53          *:*
> UDP    192.168.0.1:67          *:*
> UDP    192.168.0.1:68          *:*
> UDP    192.168.0.1:137         *:*
> UDP    192.168.0.1:138         *:*
> UDP    192.168.0.1:500         *:*
> UDP    192.168.0.1:10900       *:*
> UDP    192.168.0.1:17985       *:*
> UDP    192.168.0.1:17987       *:*
> UDP    my.net.217.125:500      *:*
> UDP    my.net.217.125:9504     *:*
> ===== end of "netstat -an" output
> =====
>
> ===== "fport /p" output
> =====
> FPort v1.33 - TCP/IP Process to Port Mapper
> Copyright 2000 by Foundstone, Inc.
>
> Pid  Process           Port  Proto Path
> 400  svchost            -> 135  TCP   C:\WINNT\system32\svchost.exe
> 8    System             -> 139  TCP
> 8    System             -> 445  TCP
> 516  MSTask             -> 1025 TCP   C:\WINNT\system32\MSTask.exe
> 8    System             -> 1026 TCP
> 8    System             -> 1723 TCP
> 612  vsmon              -> 3002 TCP   C:\WINNT\system32\ZoneLabs\vsmon.exe
> 472  svchost            -> 3006 TCP   C:\WINNT\System32\svchost.exe
> 8    System             -> 3657 TCP
> 8    System             -> 4629 TCP
> 8    System             -> 4775 TCP
```

## SecurityFocus Incidents: Re: Help – a possible bot

```
>
> 400  svchost      -> 135  UDP  C:\WINNT\system32\svchost.exe
> 8    System       -> 137  UDP
> 8    System       -> 138  UDP
> 8    System       -> 445  UDP
> 228  lsass        -> 500  UDP  C:\WINNT\system32\lsass.exe
> 216  services     -> 1027 UDP  C:\WINNT\system32\services.exe
> 472  svchost      -> 3001 UDP  C:\WINNT\System32\svchost.exe
> 1276 RuLaunch     -> 3167 UDP  C:\Program Files\McAfee\McAfee Shared
> Components\Instant Updater\RuLaunch.exe
> 612  vsmon        -> 17985 UDP  C:\WINNT\system32\ZoneLabs\vsmon.exe
> 612  vsmon        -> 17987 UDP  C:\WINNT\system32\ZoneLabs\vsmon.exe
>
> ===== end of "fport /p" output
> =====
>
>
>
>
>
> -----
--
> This list is provided by the SecurityFocus ARIS analyzer service.
> For more information on this free incident handling, management
> and tracking system please see: http://aris.securityfocus.com
>
>
-----
This list is provided by the SecurityFocus ARIS analyzer service.
For more information on this free incident handling, management
and tracking system please see: http://aris.securityfocus.com
```