

Re: netstat command

Source: <http://www.derkeiler.com/Newsgroups/microsoft.public.security.virus/2003-10/1961.html>

From: Taishi (taishi_bak_at_hotmail.com)

Date: 10/12/03

Date: Sat, 11 Oct 2003 22:34:02 -0500

Kenny,

Thanks... Here are the apps. I don't see anything suspicious. I will check out those other 2 websites. It seems like normal Windows Apps. except for 02k.exe... and actually I don't see port 3440. uhmmm Strange. Any ideas?

Regards,

T

```
02k.exe:700 TCP my200srv:15000 my200srv:0 LISTENING
02k.exe:700 TCP my200srv:5555 my200srv:0 LISTENING
dns.exe:1040 TCP my200srv:domain my200srv:0 LISTENING
dns.exe:1040 TCP my200srv:1029 my200srv:0 LISTENING
dns.exe:1040 UDP my200srv:1028 *.*
dns.exe:1040 UDP my200srv:domain *.*
dns.exe:1040 UDP my200srv:1027 *.*
dns.exe:1040 UDP my200srv:domain *.*
explorer.exe:1388 UDP my200srv:1410 *.*
IEXPLORE.EXE:1984 UDP my200srv:3125 *.*
IEXPLORE.EXE:2168 UDP my200srv:3476 *.*
IEXPLORE.EXE:2176 UDP my200srv:1644 *.*
IEXPLORE.EXE:2376 UDP my200srv:3465 *.*
IEXPLORE.EXE:636 UDP my200srv:3437 *.*
IEXPLORE.EXE:636 TCP my200srv:3891 my200srv:0 LISTENING
IEXPLORE.EXE:636 TCP my200srv:3891 199.181.132.151:http ESTABLISHED
inetinfo.exe:1068 TCP my200srv:ftp my200srv:0 LISTENING
inetinfo.exe:1068 TCP my200srv:smtp my200srv:0 LISTENING
inetinfo.exe:1068 TCP my200srv:http my200srv:0 LISTENING
inetinfo.exe:1068 TCP my200srv:https my200srv:0 LISTENING
inetinfo.exe:1068 TCP my200srv:1036 my200srv:0 LISTENING
inetinfo.exe:1068 TCP my200srv:4505 my200srv:0 LISTENING
inetinfo.exe:1068 UDP my200srv:1037 *.*
inetinfo.exe:1068 UDP my200srv:3456 *.*
lsass.exe:248 UDP my200srv:isakmp *.*
msimn.exe:2204 TCP my200srv:3675 my200srv:0 LISTENING
msimn.exe:2204 TCP my200srv:3743 my200srv:0 LISTENING
msimn.exe:2204 TCP my200srv:3817 my200srv:0 LISTENING
```

microsoft.public.security.virus: Re: netstat command

msimn.exe:2204 TCP my200srv:3675 msnews.microsoft.com:nntp ESTABLISHED
msimn.exe:2204 TCP my200srv:3743 newssvr23-ext.news.prodigy.com:nntp

ESTABLISHED

msimn.exe:2204 TCP my200srv:3817 msnews.microsoft.com:nntp ESTABLISHED
msimn.exe:2204 UDP my200srv:3556 *.*
msimn.exe:2204 UDP my200srv:1537 *.*
mstask.exe:648 TCP my200srv:1026 my200srv:0 LISTENING
OUTLOOK.EXE:1208 UDP my200srv:4008 *.*
Save.exe:1620 UDP my200srv:1046 *.*
services.exe:236 UDP my200srv:1035 *.*
snmp.exe:864 UDP my200srv:snmp *.*
svchost.exe:424 TCP my200srv:epmap my200srv:0 LISTENING
svchost.exe:424 UDP my200srv:epmap *.*
svchost.exe:508 UDP my200srv:1645 *.*
svchost.exe:508 UDP my200srv:1646 *.*
svchost.exe:508 UDP my200srv:radius *.*
svchost.exe:508 UDP my200srv:radacct *.*
svchost.exe:508 UDP my200srv:1030 *.*
svchost.exe:508 UDP my200srv:1031 *.*
System:8 TCP my200srv:3888 swbellpop-cluster.prodigy.net:pop3

TIME_WAIT

System:8 TCP my200srv:microsoft-ds my200srv:0 LISTENING
System:8 TCP my200srv:1040 my200srv:0 LISTENING
System:8 TCP my200srv:netbios-ssn my200srv:0 LISTENING
System:8 UDP my200srv:microsoft-ds *.*
System:8 UDP my200srv:netbios-ns *.*
System:8 UDP my200srv:netbios-dgm *.*
System:8 TCP my200srv:3889 swbellpop-cluster.prodigy.net:pop3

TIME_WAIT

tcpvcs.exe:852 TCP my200srv:echo my200srv:0 LISTENING
tcpvcs.exe:852 TCP my200srv:discard my200srv:0 LISTENING
tcpvcs.exe:852 TCP my200srv:daytime my200srv:0 LISTENING
tcpvcs.exe:852 TCP my200srv:qotd my200srv:0 LISTENING
tcpvcs.exe:852 TCP my200srv:chargen my200srv:0 LISTENING
tcpvcs.exe:852 TCP my200srv:1039 my200srv:0 LISTENING
tcpvcs.exe:852 UDP my200srv:echo *.*
tcpvcs.exe:852 UDP my200srv:discard *.*
tcpvcs.exe:852 UDP my200srv:daytime *.*
tcpvcs.exe:852 UDP my200srv:qotd *.*
tcpvcs.exe:852 UDP my200srv:chargen *.*
tcpvcs.exe:852 UDP my200srv:bootpc *.*
tcpvcs.exe:852 UDP my200srv:bootps *.*
tcpvcs.exe:852 UDP my200srv:bootpc *.*
tcpvcs.exe:852 UDP my200srv:2535 *.*
wins.exe:984 TCP my200srv:nameserver my200srv:0 LISTENING
wins.exe:984 TCP my200srv:1034 my200srv:0 LISTENING
wins.exe:984 UDP my200srv:nameserver *.*
wins.exe:984 UDP my200srv:1033 *.*

"YoKenny" <YKnot@home.invalid> wrote in message
news:ukuqP4GkDHA.1456@tk2msftngp13.phx.gbl...

> Taishi wrote:

>> I can see alot of activity on my ports. Netstat output listed below.

>> I think I have a worm or a trojan. If this is true, Do any of you

>> know what it is?

>>

>> Is it possible for a hacker to view my keystrokes, passwords for my

>> banking account and other private passwords?

>>

>> Regards,

>> T

>>

>> Proto Local Address Foreign Address State

>> TCP my200srv:echo my200srv:0 LISTENING

>> TCP my200srv:discard my200srv:0 LISTENING

>> TCP my200srv:daytime my200srv:0 LISTENING

>> TCP my200srv:qotd my200srv:0 LISTENING

>> TCP my200srv:chargen my200srv:0 LISTENING

>> TCP my200srv:ftp my200srv:0 LISTENING

>> TCP my200srv:smtp my200srv:0 LISTENING

>> TCP my200srv:nameserver my200srv:0 LISTENING

>> TCP my200srv:domain my200srv:0 LISTENING

>> TCP my200srv:http my200srv:0 LISTENING

>> TCP my200srv:epmap my200srv:0 LISTENING

>> TCP my200srv:https my200srv:0 LISTENING

>> TCP my200srv:microsoft-ds my200srv:0 LISTENING

>> TCP my200srv:1026 my200srv:0 LISTENING

>> TCP my200srv:1029 my200srv:0 LISTENING

>> TCP my200srv:1034 my200srv:0 LISTENING

>> TCP my200srv:1036 my200srv:0 LISTENING

>> TCP my200srv:1039 my200srv:0 LISTENING

>> TCP my200srv:1040 my200srv:0 LISTENING

>> TCP my200srv:1873 my200srv:0 LISTENING

>> TCP my200srv:3439 my200srv:0 LISTENING

>> TCP my200srv:3440 my200srv:0 LISTENING

>> TCP my200srv:3441 my200srv:0 LISTENING

>> TCP my200srv:3743 my200srv:0 LISTENING

>> TCP my200srv:4505 my200srv:0 LISTENING

>> TCP my200srv:15000 my200srv:0 LISTENING

>> TCP my200srv:5555 my200srv:0 LISTENING

>> TCP my200srv:netbios-ssn my200srv:0 LISTENING

>> TCP my200srv:1873 msnews.microsoft.com:nntp

>> ESTABLISHED

>> TCP my200srv:3436 64.71.159.243:http TIME_WAIT

>> TCP my200srv:3439 199.181.132.151:http ESTABLISHED

>> TCP my200srv:3440 64.71.159.243:http ESTABLISHED

>> TCP my200srv:3441 64.71.159.243:http SYN_SENT

>> TCP my200srv:3743 newssvr23-ext.news.prodigy.com:nntp

>> ESTABLISHED

>

microsoft.public.security.virus: Re: netstat command

- > *Q1: Need the names of the applications running on your system.*
- > *Try TCPView as it will give you the application name that is associated with*
- > *the connection.*
- > <http://www.sysinternals.com/ntw2k/source/tcpview.shtml>
- >
- > *Q2: Yes. A keylogger application or trojan can capture and transmit all*
- > *your information.*
- >
- > *Get a copy of HijackThis from this site:*
- > <http://www.tomcoyote.org/hjt/>
- >
- > *Go to this forum:*
- >
- > <http://forums.spywareinfo.com/index.php?s=d920245b6997106a8e25af1c3d810783&showforum=11>
- >