

Re: AIM Send out random messages

Source: <http://www.derkeiler.com/Newsgroups/microsoft.public.security/2005-05/0907.html>

From: Jim Carlock (*anonymous_at_localhost*)

Date: 05/24/05

Date: Mon, 23 May 2005 21:38:40 -0400

"Lord Loki" <LordLoki@discussions.microsoft.com> wrote:
> *if i tell just anyone, and they WERE a hacker... they couldnt hack*
> *with that knowledge right? because... i really dont know, and i*
> *dont want to take chances*

I don't really know the full answer to that. :-) So I'll post mine. I've removed alot of the duplicate stuff, so you'll likely see svchost.exe listed a few times in yours.

If you see something different on your system you might want to ask what it is.

File Cache
Idle Process
System
smss.exe
csrss.exe
winlogon.exe
services.exe
lsass.exe
ati2evxx.exe
svchost.exe
spoolsv.exe
avgserv.exe
Runservice.exe
mdm.exe
OWSTIMER.EXE
alg.exe
explorer.exe
soundman.exe
AsusProb.exe
EM_EXEC.EXE
PRONoMgr.exe
avgcc32.exe
ATnotes.exe
gcasDtServ.exe
dllhost.exe

Tcpview.exe
gcasServ.exe
taskmgr.exe
notepad.exe
uPad.exe
firefox.exe
cmd.exe
MSDEV.EXE
msimn.exe
pstat.exe

If you have another firewall working... don't worry about Zone Alarm.

Also, you might want to check out what's happening here:
<https://www.grc.com/x/ne.dll?bh0bkyd2>

That should take you the ShieldsUp test. Run the test there and let us know what it tells you. They have a lot of information there, so you might want to look through some of it and see if it helps.

Once you get there, click on the buttons on the silver bar near the bottom:

File Sharing
Common Ports
All Service Ports

The "All Service Ports" test should show up as all green, and you'll need to read the stuff on that page. Take some time to read it all.

If you have any questions, feel free to ask. Let us know what it tells you.

Everything showed up as "green" when I ran the "All Service Ports" test. It indicated that my system "failed" at:

Unsolicited Packets: RECEIVED (FAILED)

<shrug> I'm only running the Windows XP SP2 Firewall and I think it's doing a fairly decent job.

If someone else wants to advise me against this, I'd appreciate knowing what's up.

The grc.com has been around since 1998 or thereabouts and I've used them to test systems I've set up.

Hope that helps.

--

Jim Carlock

Please post replies to newsgroup.

"Lord Loki" <LordLoki@discussions.microsoft.com> wrote:

microsoft.public.security: Re: AIM Send out random messages

ok... obviously, i o