

Re: Attacker disabling firewall security....

Source: <http://www.derkeiler.com/Newsgroups/microsoft.public.security/2003-06/0168.html>

From: Sandi – Microsoft MVP (sandi_hardmeier_at_mvps.org)

Date: 06/08/03

Date: Sun, 8 Jun 2003 15:58:15 +0800

Jeez I developing a dislike of Norton Internet Security. As far as I can see there was no successful access against your machine. The inability to change passwords in Norton, inability to remove software etc etc are, as far as I'm concerned, all related to problems with Norton's software, not your computer being hacked.

tgcmd.exe (legitimate but unnecessary software; disable via msconfig)

sdcmn – Comcast support?

cmanager.exe (legitimate; try disabling via msconfig)

wsbho2ko.dll (unrecognised; use BHODEMON to detect and disable)

Generic Host Process for Win32 – legitimate.

svshost.exe –legitimate

hid.dll – legitimate

hidphone – legitimate

uniplat – legitimate

unimdm.tsp – legitimate

wbemess.dll – legitimate

<sheesh> I think I'll give up now.

--

Hyperlinks are used to ensure answers remain current.

Sandi Hardmeier - Microsoft MVP since 1999

<http://www.mvps.org/inetexplorer>

Full list of Microsoft MVPs:

<http://mvp.support.microsoft.com/default.aspx?scid=/default.aspx?scid=fh;en-us;mvpaward&style=to>

"Dennis Macklin" <dennis.macklin@sbcglobal.net> wrote in message news:031b01c32b8a\$01272650\$a301280a@phx.gbl...

> An attacker is somehow gaining access to my computer
> (standalone w/SBC Yahoo DSL service) even though I have
> the Norton Internet Security 2003 Firewall set up, and
> also have IP addresses from where the attacks are coming
> from listed in my Restricted IP address listing within
> Norton Internet Security. The attacker is somehow

microsoft.public.security: Re: Attacker disabling firewall security....

> disabling the administrative supervisor password/s I use
> within Norton Internet Security 2003 so that I can no
> longer set up the firewall within your program nor
> uninstall it. Therefore if I access the Internet after this
> type of incident I am suspect to attacks or viruses. This
> started to happen last month (May 2003) with the following
> alert messages from Norton Internet Security 2003:
>
> Attack #1(May 29, 2003, 6:20pm): Intrusion via Portscan
> Attack, IP Attacker Address(206.204.10.201), Risk Level
> (Medium), Note that at least 11 ports were probed.
>
> Attack #2(May 29, 2003, 6:31pm): Protocol(TCP-inbound),
> Remote Address(68.159.148.91:50686), Local Address
> (68.21.169.59:27374), Note high risk attempt to connect to
> local computer using the Backdoor/Subseven Trojan horse
> blocked.
>
> Attacks #3-4-5(May 30, 2003, 8:31pm): Remote Address
> (68.21.95.161 or 68.21.203.63 or 68.21.7.118), Note high
> risk attempt to connect to local computer using the
> HTTP_IIS_ISAPI Extension blocked.
>
> Attack #6(May 30, 2003, 9:07pm): Remote Address
> (68.60.255.241), Note high risk attempt to connect to
> local computer using Nimda_Propagation blocked.
>
> Attack #7(May 30, 2003, 9:07pm): Remote Address
> (220.85.25.125), Note high risk attempt to connect to
> local computer using Backdor Subseven Trojan horse blocked
> (Norton Internet Security Visual Tracking gave the
> location of this attack to be from Australia).
>
> Other Remote IP Addresses that have triggered one of the
> above attacks over the last month(203.173.164.131,
> 68.78.68.176, 68.33.132.140, 68.22.198.224, 68.21.139.5,
> 68.55.116.93, 68.21.95.74, 68.21.7.101, 68.54.86.49,
> 68.22.145.208, 68.22.104.201, 68.33.141.19, 68.41.34.77,
> 68.39.189.127, 68.21.17.37, 68.32.30.25, 68.38.171.233,
> 80.11.61.192, 67.195.218.34).
>
> I had Windows Millenium at the beginning of May 2003 when
> I started to get these attacks, and was informed it was a
> good idea to disable the "File Download" option within
> Internet Explorer 6.0 Internet Security Options section of
> the browser. I did that, but I didn't do this in the SBC
> Yahoo DSL browser(IE 6.0 also). Eventually someone must
> have used a Internet related program on my PC to change a
> file so that my computer wouldn't reboot properly under
> Windows ME. I had to delete the DOS partition, reformat
> the hard drive and I decided to upgrade to Windows XP
> Professional at that time for a fresh start.
>
> I also noticed that in the above listed attacks, Norton
> Internet Security 2003 would alert me that some
> unauthorized program was trying to access my PC via the
> SBC Yahoo DSL Browser or the Internet Connection Manager
> software that comes with the SBC Yahoo DSL software:
>
> Example Messages: (1)Tgcmd.exe or CCD.exe is attempting to
> access the Internet using one or more unrecognized
> modules...Pathname(C:\Program

microsoft.public.security: Re: Attacker disabling firewall security....

> Files\Support.com\bin\tgcmd.exe or sdcmon.dll); (2)
> CManager.exe is attempting to access the Internet using
> one or more unrecognized modules...Pathname(C:\Program
> Files\SBC\Connection Manager\CManager.exe or
> AgentConfiguration.dll)...with a remote address of
> 209.184.198.60(https:443).
>
> After installing Windows XP Professional I also installed
> the following programs(since I build webpages and do
> computer programming)...Microsoft IIS, WS-FTP Professional
> (during deletion I received a message saying that "someone
> or another person was using the following
> file...wsbho2ko.dll"...and I could not delete the
> program...I eventually was able to delete it though),
> Microsoft SQL Server 2000 Personal Edition, SBC Yahoo DSL,
> Quicktime & RealOne Players, Netscape 7.0, Adobe Photoshop
> & ImageReady, Adobe Acrobat, Coldfusion 4.5, Norton
> Internet Security 2003.
>
> I did not install the Windows XP Professional Critical
> Updates, and Windows update didn't prompt me to update
> these items after the initial installation of Windows XP
> Pro. I set the NIS 2003 firewall up with my supervisor
> password, scanned my hard drive for viruses(none found),
> and started my SBC Yahoo DSL connection manager to access
> the Internet. No problems with attacks for a few hours,
> then the attacks started back again this week(same as the
> ones listed above). Once again I could not change the
> administrative supervisor password for the firewall within
> NIS 2003 nor could I uninstall NIS 2003...got a message
> saying I was not authorized and needed supervisor
> priveleges to uninstall NIS 2003.
>
> I review help manuals on the Symantec, Gateway, Microsoft
> and SBC Yahoo DSL websites to see what I could do. The
> Symantec site mentioned to remove Microsoft IIS/WS-FTP/SQL
> Server components and/or programs if not using them due to
> possible access holes an attacker could use...so I
> uninstalled those programs.
>
> I then went to the Microsoft support website for Windows
> XP Pro and was able to upgrade my IE browser to Service
> Pack 1, and install all the critical updates, but since my
> NIS 2003 firewall was disabled I decided to use the
> firewall that comes with Windows XP for protection until I
> could uninstall NIS 2003.
>
> I deleted SBC Yahoo DSL and re-installed it...note that it
> asks for permission to scan your system settings in case
> problems occur in the future...so I okay'd this...although
> they have an option that says you don't have to do this
> and the DSL software will still work.
>
> After successfully connecting to the Internet this time
> everything was okay using the Win XP firewall instead of
> the NIS 2003 firewall, but I then started getting the
> message:
>
> Microsoft Generic Host Process for Win32 services is
> attempting to access the Internet using one or more
> unrecognized modules at 239.255.255.250:1900(Port 1286),
> with a path name referencing various files on my computer

microsoft.public.security: Re: Attacker disabling firewall security....

> like the following:
>
> C:\windows\system32\(\svchote.exe or hid.dll or
> hidphone.tsp or uniplat.dll or unimdm.tsp or
> wbem\wbemess.dll or wbemcore.dll or ssdpapi.dll or
> upnp.dll or mstlsapi.dll or authz.dll...even referencing
> adobe acrobat dlls also). Now I can't access Microsoft
> Outlook email or webpages through IE 6.0
>
> My guess is somehow the attacker/s are scanning any files
> that I have that access the Internet as a potential
> opening through a random port, and once they gain access
> to an open port they are able to change the NIS 2003
> firewall settings. I don't want to have to constantly have
> to uninstall and re-install the NIS 2003 software to re-
> start the firewall, nor do I want to have to reformat my
> hard drive constantly to remove a possible file that may
> have been slipped onto my computer...if possible.
>
> Do you have any suggestions as to what I should do, or is
> there anyone I can call for further assistance on this
> issue at your company??? Sorry for writing this book, but
> I'm looking for help from anyone who may have suggestions
> and/or answers.
>
> My contact information is listed below for further follow-
> up:
>
> Dennis Macklin
>
> Home Email Address: dennis.macklin@sbcglobal.net
> Work Email Address: dmacklin@ccc.edu