

Re: Backdoor.Nibu.E.

Source:

<http://www.tech-archive.net/Archive/WinXP/microsoft.public.windowsxp.general/2004-07/13687.html>

From: Freddyb (*freddyb_at_adelphia.net*)

Date: 07/14/04

Date: Tue, 13 Jul 2004 22:38:09 -0400

One thing I have found that really helps is to use housecall to remove the virus. Then make the changes to the registry and follow the directions that can be found on www.sarc.com for removing this virus. This worked for me.

On Thu, 8 Jul 2004 04:50:33 -0700, "Manny"
<anonymous@discussions.microsoft.com> wrote:

>I am running cable. I have done everything you mentioned,
>all in safe mode. Ended the process in task manager,
>updated virus defintions, searched the whole registry and
>deleted, numerous scans on all files eg. spybot, adaware,
>norton antivirus etc. I have tried everything. It really
>makes no sense at all. I dont have a firewall though
>apart from the generic Windows XP one.
>
>>-----Original Message-----
>>Well, something has to be loading it. After you've
>followed the instructions for removal
>>at Symantec, the registry keys shouldn't revert back
>unless your system is being
>>reinfected. Are you sure that you did all of the fixes
>in Safe Mode, making sure that
>>you've Ended the process in Task Manager if it's
>running. Are you sure you are using a
>>firewall. Because if you are NOT, you might just be
>constantly reinfesting your system
>>every time you boot if you have a DSL, LAN, or Cable
>connection. Are you sure that you've
>>ended the process in Task Manager, and then scanned with
>your antivirus program with the
>>latest definitions and have it set to scan ALL files.
>>--
>>
>>T.C.
>>t__cruise@[NoSpam]hotmail.com
>>Remove [NoSpam] to reply

>>
>>
>> "Manny" <anonymous@discussions.microsoft.com> wrote in
>message
>>news:2956001c4649f\$4fda9800\$a301280a@phx.gbl...
>>> I just did everything you mentioned in your previous
>>> post. Found a few instances of netda, netdb and
>netdc.exe
>>> deleted them. Also from the Reg Key
>>>
>HKEY_LOCAL_MACHINE\Software\Microsoft\WindowsNT\CurrentVer
>>> sion\Winlogon.
>>> Add the line to the hosts file as there was nothing in
>>> there to begin with.
>>> All in safe mode.
>>> Rebooted, log in, and once again netdb.exe is running
>and
>>> the key
>>>
>HKEY_LOCAL_MACHINE\Software\Microsoft\WindowsNT\CurrentVer
>>> sion\Winlogon has netdc.exe in the Shell section.
>>> I am beginning to think I may have to format, which is
>the
>>> last thing I want to do as I dont have the time to back
>>> everything up and instal etc.
>>> Any other ideas?
>>>
>>> >-----Original Message-----
>>> >The Hosts file is located in the folder:
>>> >
>>> >C:\WINDOWS\SYSTEM32\DRIVERS\ETC
>>> >
>>> >Right click it, left click Open, and when the dialog
>box
>>> opens click to select the radio
>>> >button for: Select Program From a List, and click the
>>> OK button. When the Open With
>>> >window opens scroll through the list of programs,
>click
>>> to select and highlight Notepad,
>>> >then click the OK button. Hosts will the open in
>>> Notepad. Edit the Hosts file with
>>> >Notepad in Safe Mode leaving the only entry:
>>> >
>>> >127.0.0.1 localhost
>>> >
>>> >If that entry isn't there, put it there, and save.
>>> >
>>> >Editing the Hosts file is VERY important because
>entries
>>> made there can prevent you from

>>> >updating your antivirus definitions, and keep you from
>>> being able to scan your hard drive
>>> >with the latest virus definitions.
>>> >
>>> >As for not being able to find the Registry string for
>>> the key mentioned, something in the
>>> >Registry is causing the file to be loaded. In Safe
>>> Mode, open Regedit, click the Edit
>>> >menu, click Find, type: netda.exe. Then click the Find
>>> Next button. When it string Is
>>> >found, right click it in the right pane and then left
>>> click delete. Then press the F3 key
>>> >to find the next instance of the file being mentioned
>in
>>> the Registry. Keep doing that
>>> >until the entire Registry has been searched.
>>> >
>>> >Avoid reinfection. Have a decent firewall (even the
>>> FREE version of Zone Alarm standard
>>> >is better than the Windows XP native firewall)
>>> >--
>>> >
>>> >T.C.
>>> >t__cruise@[NoSpam]hotmail.com
>>> >Remove [NoSpam] to reply
>>> >
>>> >
>>> >"Manny" <anonymous@discussions.microsoft.com> wrote in
>>> message
>>> >news:28bea01c46423\$b7ef6910\$a301280a@phx.gbl...
>>> >> It seems straight forward but does not work :-(
>>> >> I did a search for all files containing the
>>> words "hosts"
>>> >> in its title as it says on the symantec site.
>>> >> The files found didnt resemble what the symantec
>>> >> instructions suggested would occur. There was a file
>>> >> called Hosts with no extension. When opened with
>>> notepad
>>> >> it was empty.
>>> >> As for the registry, i edited the
>>> >> HKEY_LOCAL_MACHINE\Software\Microsoft\Windows
>>> >> NT\CurrentVersion\Winlogon
>>> >> from:
>>> >> "explorer.exe %System%\netdc.exe"
>>> >> to:
>>> >> "explorer.exe"
>>> >> However, in
>>> >>
>>>
>>>
>HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersi
>>> >> on\Run

>>> >> *I couldnt find the value:*
>>> >> *"load32"="%System%\netda.exe..."*
>>> >>
>>> >> *I reboot, open task manager, and there once again i*
>>> *find*
>>> >> *netda/b/c.exe and the registry i edited is the same*
>>> *as*
>>> *it*
>>> >> *was before i edited it.*
>>> >>
>>> >> *I have disabled system restore and everything else.*
>>> >> *Followed instructions perfectly. Trying for 2 days*
>>> *to*
>>> >> *repair. :-(*
>>> >>
>>> >> *A desperate Manny :-(*
>>> >>
>>> >>
>>> >> >-----Original Message-----
>>> >> >*I looked at:*
>>> >> >
>>> >> >
>>> >>
>>> >> ><http://securityresponse.symantec.com/avcenter/venc/data/b>
>>> >> *ackdoor.nibu.e.html*
>>> >> >
>>> >> >*It seems straight forward. Are you sure that you*
>>> *edited*
>>> >> *your Host file with Notepad to*
>>> >> >*delete all entries but:*
>>> >> >
>>> >> >*127.0.0.1 localhost*
>>> >> >
>>> >> >*Are you sure that you edited the registry as*
>>> *directed?*
>>> >> >
>>> >> >*If so, in what way is Backdoor.Nibu.E effecting*
>>> *your*
>>> >> *system?*
>>> >> >--
>>> >> >
>>> >> >*T.C.*
>>> >> >[t_cruise@\[NoSpam\]hotmail.com](mailto:t_cruise@[NoSpam]hotmail.com)
>>> >> >*Remove [NoSpam] to reply*
>>> >> >
>>> >> >
>>> >> >
>>> >> >
>>> >> >*"Manny" <anonymous@discussions.microsoft.com>*
>>> *wrote in*
>>> >> *message*

microsoft.public.windowsxp.general: Re: Backdoor.Nibu.E.

>>> >> >news:2742001c463ea\$95a74140\$a601280a@phx.gbl...
>>> >> >> *I have disabled system restore, rebooted and run
>all
>>> >> the
>>> >> >> anti-virus and spyware software at my disposal.
>All
>>> in
>>> >> >> Safe Mode. Doesn't find anything! I have never
>been
>>> so
>>> >> >> puzzled.
>>> >> >>
>>> >> >>
>>> >> >> >-----Original Message-----
>>> >> >> >The nasty little virus could be hiding in System
>>> >> Restore.
>>> >> >> >Turn off System Restore, reboot, and run a virus
>>> scan
>>> >> >> again.
>>> >> >> >
>>> >> >> >How to Turn On and Turn Off System Restore in
>>> Windows
>>> XP
>>> >> >> >[http://support.microsoft.com/default.aspx?
>>> scid=kb;en-
>>> us;310405&Product=winxp](http://support.microsoft.com/default.aspx?scid=kb;en-us;310405&Product=winxp)
>>> >> >> >
>>> >> >> >--
>>> >> >> >Carey Frisch
>>> >> >> >Microsoft MVP
>>> >> >> >Windows XP - Shell/User
>>> >> >> >
>>> >> >> >Be Smart! Protect your PC!
>>> >> >> >[http://www.microsoft.com/security/protect/
>>> >> >> >
>>> >> >> >-----
>----
>>> ----
>>> >> ----
>>> >> >> -----
>>> >> >> >
>>> >> >> >"Bram L." <anonymous@discussions.microsoft.com>
>>> wrote
>>> >> in
>>> >> >> message:
>>> >> >> >news:278c701c463a2\\$87e52650\\$a501280a@phx.gbl...
>>> >> >> >
>>> >> >> >| Sounds exactly like the problem I am having
>>> trying
>>> >> to
>>> >> >> get](http://www.microsoft.com/security/protect/)*

Re: Backdoor.Nibu.E.

>>> >> >> >| *rid of backdoor.coreflood. The file it is in,*
>>> >> >> >| *windows/system32/DS32GVXS.dll can't be*
>*deleted as*
>>> >> *it's*
>>> >> >> >| *always running! I've followed Symantec's*
>*advice*
>>> *and*
>>> >> >> >| *removed a link in the registry, in safe mode,*
>*and*
>>> >> >> *after*
>>> >> >> >| *turning off the system restore function. I ran*
>>> *Ad-*
>>> >> >> >| *Aware...all to no avail. We both need similar*
>>> *help!*
>>> >> >> >
>>> >> >> >.
>>> >> >> >
>>> >> >
>>> >> >
>>> >> >----
>>> >> >*Outgoing mail is certified Virus Free.*
>>> >> >*Checked by AVG anti-virus system*
>>> >> >*(<http://www.grisoft.com>).*
>>> >> >*Version: 6.0.716 / Virus Database: 472 – Release*
>*Date:*
>>> >> >*7/5/2004*
>>> >> >
>>> >> >
>>> >> >.
>>> >> >
>>> >
>>> >
>>> >----
>>> >*Outgoing mail is certified Virus Free.*
>>> >*Checked by AVG anti-virus system*
>>> >*(<http://www.grisoft.com>).*
>>> >*Version: 6.0.716 / Virus Database: 472 – Release Date:*
>>> >*7/5/2004*
>>> >
>>> >
>>> >.
>>> >
>>
>>
>>----
>>*Outgoing mail is certified Virus Free.*
>>*Checked by AVG anti-virus system*
>*(<http://www.grisoft.com>).*
>>*Version: 6.0.716 / Virus Database: 472 – Release Date:*
>>*7/5/2004*
>>

microsoft.public.windowsxp.general: Re: Backdoor.Nibu.E.

>>
>>.
>>