

Forum:[Hack Forums](#)

Thread: [Weird Virus \(virus.neshta\) \[STILL NEED HELP!!!\]](#)

Xogg - May 7, 2017, 9:47 am

So i got this virus and its doing a few things, one when I try to open for example: Notepad++ its prompting saying to run in svchost.com. If i click yes sometimes it will open and other times it will open the wizard which asks me to chose what to run it in. This has resulted to me not being able to open 95% of the things on my pc. Here are a few

- Google Chrome
- Internet Explorer
- Mozilla Firefox
- Explorer.exe
- CMD

I have bypassed this for some programs by for example opening: Explorer.exe in Explorer.exe so opening the program that wont open in itself, (If that makes any since)

My pc is currently on and in safe mode with networking, this allowed me to open and use google chrome. But still is prompting with svchost.com

I used malwareBytes to do a FULL scan yesterday and here is the main detection I kept getting.

The "Type" is virus.neshta

If you cant read the image here is a direct link

Spoiler ([Click to View](#))

https://images.discordapp.net/eJwFwdsNwyAMAMBdGADzsAtkG0QQiZpgBI76UXX33n3VMy-1qUNkrA1gP1fhuesIPHOujG3q-ZxLI34hiySy3HXLgschmQSuuDdy5NHE8FbQylYsg4tecIY4envzp-uR2_q9wcG_CLa.w7vkUouXI8JrDIZSi-vf8-300Q4?width=600&height=219

Also in the image it gives a directory in where the virus is, I DID delete the whole directory of where it was all occurring.

EDIT: So i did scans using RKILL64 and ADWcleaner but i was in safe mode on my PC I restarted my PC and redid them and got differnt results logs soon!

LOGS

ADWcleaner

Spoiler ([Click to View](#))

DETECTION LOG

Code # AdwCleaner v6.046 - Logfile created 07/05/2017 at 13:20:06
Updated on 24/04/2017 by Malwarebytes
Database : 2017-05-05.1 [Local]
Operating System : Windows 7 Professional Service Pack 1 (X64)
Username : OWNER - OWNER-PC
Running from : C:\Users\OWNER\Desktop\adwcleaner_6.046.exe
Mode: Scan
Support : <https://www.malwarebytes.com/support>

***** [Services] *****

No malicious services found.

***** [Folders] *****

No malicious folders found.

***** [Files] *****

No malicious files found.

***** [DLL] *****

No malicious DLLs found.

***** [WMI] *****

No malicious keys found.

***** [Shortcuts] *****

No infected shortcut found.

***** [Scheduled Tasks] *****

No malicious task found.

***** [Registry] *****

No malicious registry entries found.

***** [Web browsers] *****

No malicious Firefox based browser items found.

Chrome pref Found: [C:\Users\OWNER\AppData\Local\Google\Chrome\User Data\Default\Web data] - aol.com

Chrome pref Found: [C:\Users\OWNER\AppData\Local\Google\Chrome\User Data\Default\Web data] - ask.com

C:\AdwCleaner\AdwCleaner[C0].txt - [2750 Bytes] - [07/05/2017 13:08:46]

C:\AdwCleaner\AdwCleaner[S0].txt - [2673 Bytes] - [07/05/2017 13:07:11]

C:\AdwCleaner\AdwCleaner[S1].txt - [1464 Bytes] - [07/05/2017 13:16:37]

C:\AdwCleaner\AdwCleaner[S2].txt - [1385 Bytes] - [07/05/2017 13:20:06]

EOF - C:\AdwCleaner\AdwCleaner[S2].txt - [1458 Bytes]

CLEANING VIRUSES LOG

Code # AdwCleaner v6.046 - Logfile created 07/05/2017 at 13:23:15

Updated on 24/04/2017 by Malwarebytes

Database : 2017-05-05.1 [Local]

Operating System : Windows 7 Professional Service Pack 1 (X64)

Username : OWNER - OWNER-PC

Running from : C:\Users\OWNER\Desktop\adwcleaner_6.046.exe

Mode: Clean

Support : <https://www.malwarebytes.com/support>

***** [Services] *****

***** [Folders] *****

***** [Files] *****

***** [DLL] *****

***** [WMI] *****

***** [Shortcuts] *****

***** [Scheduled Tasks] *****

***** [Registry] *****

***** [Web browsers] *****

[-] [C:\Users\OWNER\AppData\Local\Google\Chrome\User Data\Default\Web data] [Search Provider] Deleted: aol.com

[-] [C:\Users\OWNER\AppData\Local\Google\Chrome\User Data\Default\Web data] [Search Provider] Deleted: ask.com

:: "Tracing" keys deleted

:: Winsock settings cleared

C:\AdwCleaner\AdwCleaner[C0].txt - [2750 Bytes] - [07/05/2017 13:08:46]

C:\AdwCleaner\AdwCleaner[C2].txt - [1067 Bytes] - [07/05/2017 13:23:15]

C:\AdwCleaner\AdwCleaner[S0].txt - [2673 Bytes] - [07/05/2017 13:07:11]

C:\AdwCleaner\AdwCleaner[S1].txt - [1464 Bytes] - [07/05/2017 13:16:37]

C:\AdwCleaner\AdwCleaner[S2].txt - [1537 Bytes] - [07/05/2017 13:20:06]

EOF - C:\AdwCleaner\AdwCleaner[C2].txt - [1359 Bytes]

RKILL64

Spoiler ([Click to View](#))

Code Cant open ./ giving me the same error as everything else.

Farbar Recovery Scan Tool

Spoiler ([Click to View](#))

FRST.txt

Code <https://pastebin.com/SbkfkHG3>

Addition.txt

Code <https://pastebin.com/26Ehwa2w>

Rexethic - May 7, 2017, 9:52 am

Seems like adware, with bunch of popups and injected into svhost.

Try MalwareBytes Anti-Malware.

Xogg - May 7, 2017, 9:54 am

(May 7, 2017 09:52 AM)Rexethic Wrote: ([CITE](#)) Seems like adware, with bunch of popups and injected into svhost.

Try MalwareBytes Anti-Malware.

Is this the same as the regular MalwareBytes or a different program, I already scanned in malwareBytes

DelziumTheProudWhale_temp - May 7, 2017, 10:01 am

scan your pc with eset antivirus

KyFu - May 7, 2017, 10:03 am

Use Adwcleaner by Malwarebytes. [FREE]

Panda Cloud Cleaner is also a very good program to use. [Takes awhile on full scan, but accurate.] [FREE]

Xogg - May 7, 2017, 10:04 am

(May 7, 2017 10:03 AM)KyFu-Engineering Wrote: [\[CITE\]](#) Use Adwcleaner by Malwarebytes. [FREE]

Panda Cloud Cleaner is also a very good program to use. [Takes awhile on full scan, but accurate.] [FREE]

I will give these both a go.

5chn4pp - May 7, 2017, 10:32 am

Only FRST can remove viruses such as this, virus.neshta is like a ramnit infection, its severe and no antimalware tool expect for FRST and similar will remove it.

EDIT: It's also known as "Predator logger" which is a RAT, so please change your passwords.

Please download [Farbar Recovery Scan Tool](#) and save it to your Desktop.

Note: You need to run the version compatible with your system. If you are not sure which version applies to your system download both of them and try to run them. Only one of them will run on your system, that will be the right version.

Right click to run as administrator. When the tool opens click Yes to disclaimer.

Press Scan button.

It will produce logs called FRST.txt and Addition.txt in the same directory the tool is run from.

Please copy and paste the logs back here.

Xogg - May 7, 2017, 3:43 pm

(May 7, 2017 10:32 AM)Satudarah Wrote: [\[CITE\]](#) Only FRST can remove viruses such as this, virus.neshta is like a ramnit infection, its severe and no antimalware tool expect for FRST and similar will remove it.

EDIT: It's also known as "Predator logger" which is a RAT, so please change your passwords.

Please download [Farbar Recovery Scan Tool](#) and save it to your Desktop.

Note: You need to run the version compatible with your system. If you are not sure which version applies to your system download both of them and try to run them. Only one of them will run on your system, that will be the right version.

Right click to run as administrator. When the tool opens click Yes to disclaimer.

Press Scan button.

It will produce logs called FRST.txt and Addition.txt in the same directory the tool is run from.

Please copy and paste the logs back here.

Thanks for the help working on c=scanning now.

Mr. Kim - May 7, 2017, 5:17 pm

If it's still happening in safemode you have a bad situation friend. The malware is running from kernel space. The malware has the same integrity as the OS itself. I would use a rescue disk.

[One from Kaspersky](#)

[One from Comodo](#)

[One from Avast](#)

I can promise you it will not be removed if you boot to your current OS. If it looks like it's gone, it's just hiding.

5chn4pp - May 7, 2017, 11:13 pm

(May 7, 2017 05:17 PM)M?m?ry Wrote: [\[CITE\]](#) I can promise you it will not be removed if you boot to your current OS.

Spoiler [\(Click to View\)](#)

You can remove it in normal mode if you want to, the only requirement is will power.

Download [fixlist.txt](#) file and save it to the Desktop.

NOTE. It's important that both files, FRST/FRST64 and fixlist.txt are in the same location or the fix will not work.

NOTICE: This script was written specifically for this user, for use on that particular machine. Running this on another machine may cause damage to your operating system

Run FRST/FRST64 and press the Fix button just once and wait.

If for some reason the tool needs a restart, please make sure you let the system restart normally. After that let the tool complete its run.

When finished FRST will generate a log on the Desktop (Fixlog.txt). Please post it to your reply.

Brainsdotco - May 8, 2018, 4:53 pm

Aw dude you are formed, this is one pickle

ltpg2010 - July 8, 2018, 7:22 am

lets hope and see what happens

VENI - July 15, 2018, 5:15 am

(May 7, 2017 09:47 AM)ParadoxTheDev Wrote: [\[CITE\]](#) So i got this virus and its doing a few things, one when I try to open for example: Notepad++ its prompting saying to run in svchost.com. If i click yes sometimes it will open and other times it will open the wizard which asks me to chose what to run it in. This has resulted to me not being able to open 95% of the things on my pc. Here are a few

- Google Chrome
- Internet Explorer

- Mozilla Firefox
- Explorer.exe
- CMD

I have bypassed this for some programs by for example opening: Explorer.exe in Explorer.exe so opening the program that wont open in itself, (If that makes any since)

My pc is currently on and in safe mode with networking, this allowed me to open and use google chrome. But still is prompting with svchost.com

I used malwareBytes to do a FULL scan yesterday and here is the main detection I kept getting.

The "Type" is virus.neshta

If you cant read the image here is a direct link
Spoiler ([Click to View](#))

https://images.discordapp.net/eJwFwdsNwyAMAMBdGADzsAtkG0QQiZpgBI76UXX33n3VMy-1qUNkrA1gP1fhueslPHOrujG3q-ZxLI34hiySy3HXLgschmQSuuDdy5NHE8FbQylYsg4tecIY4envzp-uR2_q9wcG_CLa.w7vkUouXI8JrDIZSi-vf8-300Q4?width=600&height=219

Also in the image it gives a directory in where the virus is, I DID delete the whole directory of where it was all occurring.

EDIT: So i did scans using RKILL64 and ADWcleaner but i was in safe mode on my PC I restarted my PC and redid them and got differnt results logs soon!

LOGS

ADWcleaner
Spoiler ([Click to View](#))

DETECTION LOG

Code # AdwCleaner v6.046 - Logfile created 07/05/2017 at 13:20:06
Updated on 24/04/2017 by Malwarebytes
Database : 2017-05-05.1 [Local]
Operating System : Windows 7 Professional Service Pack 1 (X64)
Username : OWNER - OWNER-PC
Running from : C:\Users\OWNER\Desktop\adwcleaner_6.046.exe
Mode: Scan
Support : <https://www.malwarebytes.com/support>

***** [Services] *****

No malicious services found.

***** [Folders] *****

No malicious folders found.

***** [Files] *****

No malicious files found.

***** [DLL] *****

No malicious DLLs found.

***** [WMI] *****

No malicious keys found.

***** [Shortcuts] *****

No infected shortcut found.

***** [Scheduled Tasks] *****

No malicious task found.

***** [Registry] *****

No malicious registry entries found.

***** [Web browsers] *****

No malicious Firefox based browser items found.

Chrome pref Found: [C:\Users\OWNER\AppData\Local\Google\Chrome\User Data\Default\Web data] - aol.com

Chrome pref Found: [C:\Users\OWNER\AppData\Local\Google\Chrome\User Data\Default\Web data] - ask.com

C:\AdwCleaner\AdwCleaner[C0].txt - [2750 Bytes] - [07/05/2017 13:08:46]

C:\AdwCleaner\AdwCleaner[S0].txt - [2673 Bytes] - [07/05/2017 13:07:11]

C:\AdwCleaner\AdwCleaner[S1].txt - [1464 Bytes] - [07/05/2017 13:16:37]

C:\AdwCleaner\AdwCleaner[S2].txt - [1385 Bytes] - [07/05/2017 13:20:06]

EOF - C:\AdwCleaner\AdwCleaner[S2].txt - [1458 Bytes] #####
CLEANING VIRUSES LOG

Code # AdwCleaner v6.046 - Logfile created 07/05/2017 at 13:23:15
Updated on 24/04/2017 by Malwarebytes
Database : 2017-05-05.1 [Local]
Operating System : Windows 7 Professional Service Pack 1 (X64)
Username : OWNER - OWNER-PC
Running from : C:\Users\OWNER\Desktop\adwcleaner_6.046.exe
Mode: Clean
Support : <https://www.malwarebytes.com/support>

***** [Services] *****

***** [Folders] *****

***** [Files] *****

***** [DLL] *****

***** [WMI] *****

***** [Shortcuts] *****

***** [Scheduled Tasks] *****

***** [Registry] *****

***** [Web browsers] *****

[-] [C:\Users\OWNER\AppData\Local\Google\Chrome\User Data\Default\Web data] [Search
Provider] Deleted: aol.com
[-] [C:\Users\OWNER\AppData\Local\Google\Chrome\User Data\Default\Web data] [Search
Provider] Deleted: ask.com

:: "Tracing" keys deleted
:: Winsock settings cleared

C:\AdwCleaner\AdwCleaner[C0].txt - [2750 Bytes] - [07/05/2017 13:08:46]
C:\AdwCleaner\AdwCleaner[C2].txt - [1067 Bytes] - [07/05/2017 13:23:15]
C:\AdwCleaner\AdwCleaner[S0].txt - [2673 Bytes] - [07/05/2017 13:07:11]
C:\AdwCleaner\AdwCleaner[S1].txt - [1464 Bytes] - [07/05/2017 13:16:37]
C:\AdwCleaner\AdwCleaner[S2].txt - [1537 Bytes] - [07/05/2017 13:20:06]

EOF - C:\AdwCleaner\AdwCleaner[C2].txt - [1359 Bytes]

RKILL64

Spoiler ([Click to View](#))

Code Cant open :/ giving me the same error as everything else.

Farbar Recovery Scan Tool

Spoiler ([Click to View](#))

FRST.txt

Code <https://pastebin.com/SbkfkHG3>

Addition.txt

Code <https://pastebin.com/26Ehwa2w>

Use HitmanPro it is the best scanner. <https://www.hitmanpro.com/en-us.aspx>