

Forum: [Hack Forums](#)

Thread: [I'm infected with Win32.Neshta](#)

Excore - September 8, 2012, 3:09 pm

Hello.

I've identified that I've been infected with the win32.neshta virus. It runs every time an executable opens.

<http://www.microsoft.com/security/portal/Threat/Encyclopedia/Entry.aspx?Name=Virus%3AWin32%2FNeshta.A>

How would I go about removing this?

Retribute - September 8, 2012, 3:20 pm

Please download [exeHelper](#) to your desktop.

Double-click on exeHelper.com to run the fix.

A black window should pop up, press any key to close once the fix is completed.

Post the contents of exehelperlog.txt (Will be created in the directory where you ran exeHelper.com, and should open at the end of the scan)

Simkecg - September 8, 2012, 3:22 pm

Can you post SS of you processes in Task Manager, i will help you

Excore - September 8, 2012, 3:23 pm

Code exeHelper by Raktor

Build 20100414

Run at 17:21:35 on 09/08/12

Now searching...

Checking for numerical processes...

Checking for sysguard processes...

Checking for bad processes...

Checking for bad files...

Checking for bad registry entries...

Resetting filetype association for .exe

Resetting filetype association for .com

Resetting userinit and shell values...

Resetting policies...

--Finished--

(Sep 8, 2012 03:22 PM)Simkecg Wrote: [\[CITE\]](#) Can you post SS of you processes in Task Manager, i will help you <https://puu.sh/13h3U>
<https://puu.sh/13h4v>

Retribute - September 8, 2012, 3:25 pm

Can you open executables now? If so,

Please download [Malwarebytes' AntiMalware](#).

Double click mbam-setup.exe to install the application. Make sure a checkmark is placed next to Update Malwarebytes' Anti-Malware and Launch Malwarebytes' Anti-Malware, then click Finish.

If an update is found, it will download and install the latest version.

Once the program has loaded, select Perform Quick Scan, then click Scan. The scan may take some time to finish, so please be patient.

When the scan is complete, click OK, then Show Results to view the results.

Make sure that everything is checked, and click Remove Selected.

When disinfection is completed, a log will open in Notepad and you may be prompted to restart. Restart if it tells you to.

The log is automatically saved by MBAM and can be viewed by clicking the Logs tab in MBAM.

Copy and paste the entire report in your next reply.

Excore - September 8, 2012, 3:39 pm

Im running a Kaspersky Pure scan. It's scanning and also disinfecting all the files that the Virus infected.

Retribute - September 8, 2012, 6:54 pm

Hi, do you still want assistance, or has your issue been resolved?

Excore - September 8, 2012, 7:17 pm

(Sep 8, 2012 06:54 PM)Rub?ks Wrote: [\[CITE\]](#) Hi, do you still want assistance, or has your issue been resolved? I did a system restore from a few weeks ago, and everything seems to be fine. I'll notify you if the problem continues.

Retribute - September 8, 2012, 7:21 pm

It really isn't advised to do a system restore, but all right.

#Skyline - September 8, 2012, 7:50 pm

if its coming back on startup Follow These Steps START>Type in "msconfig" In Search>Go Startup> and Untick the box which is win32

if that didnt work try find the file on your PC and end it in processes or maybe system restore

Excore - September 8, 2012, 8:09 pm

(Sep 8, 2012 07:21 PM)Rub?ks Wrote: [\[CITE\]](#) It really isn't advised to do a system restore, but all right. Can you explain why?

(Sep 8, 2012 07:50 PM)siegew0w Wrote: [\[CITE\]](#) if its coming back on startup Follow These Steps START>Type in "msconfig" In Search>Go Startup> and Untick the box which is win32

if that didnt work try find the file on your PC and end it in processes or maybe system restore its a system service, and I cant find it. I can delete the files all I want, but the service keeps dropping them again.

Shizune - September 8, 2012, 8:10 pm

Because viruses can drop in or infect restore points rendering them useless.

Retribute - September 8, 2012, 8:11 pm

(Sep 8, 2012 08:09 PM)Excore Wrote: [\[CITE\]](#) Can you explain why?
Malware can easily hide in your restore points.

Excore - September 8, 2012, 8:12 pm

(Sep 8, 2012 08:11 PM)Rub?ks Wrote: [\[CITE\]](#) Malware can easily hide in your restore points.Ah, didn't know that. Thanks for the information, although I did research on the virus and it was not shown that this virus does that. It doesn't seem to be coming back so I think I'm okay. I'll keep my eyes open though,

Retribute - September 8, 2012, 8:32 pm

Yup. If you need any assistance in the future, just PM me.