

Forum:[Hack Forums](#)

Thread: [Infected by Trojan.Win32.Agent.nfboam](#)

crimezy - September 28, 2017, 12:35 pm

Hi there!

I accidentally ran a malicious file that opened and installed plenty of garbage on my other PC. Now I find myself scanning with Kaspersky Total Security and Malwarebytes (that first found 170 new infected files) but it seems like there's a process in System32 that's called xupdate.exe and gets deleted by Kaspersky and then appears again. I just can't remove it even in safe mode because it comes back every minute.

I'm willing to scan and provide logs if you need me to do so, thank you in advance!

5chn4pp - September 28, 2017, 12:43 pm

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.

crimezy - September 28, 2017, 12:52 pm

Hope that .exe I was talking about is still there in the logs and was not deleted by my antivirus in the middle of the scan. Seems like it comes always back though.

Addition.txt

<https://pastebin.com/ZcKXesHT>

FRST.txt

<https://pastebin.com/F6HNP09v>

Thank you.

5chn4pp - September 28, 2017, 10:48 pm

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.

Please download [RogueKiller](#) and save it to your desktop. Quit all running programs.

Right-click on the program and select Run as Administrator to start and when prompted allow it to run.

Read and accept the EULA (End User License Agreement)

Click Scan to scan the system.

When the scan completes select "Report", a log will open. Close the program > Don't Fix anything!

Post the contents of the log in your next reply.

crimezy - September 29, 2017, 3:10 am

Alright, here I am!

I followed what you said and got the logs.

This is the fixlog: <https://pastebin.com/QTx2dnce>

and this is the report from RogueKiller (hope the language isn't an issue):

<https://pastebin.com/EyRE1YrL>

5chn4pp - September 29, 2017, 8:07 am

Make Roguekiller delete everything it found, then please post fresh FRST logs so I can see if it worked.

crimezy - September 29, 2017, 12:52 pm

Seems like another file xxdate.exe is detected instead of xupdate.exe by Kaspersky.

FRST is here: <https://pastebin.com/WzWaAhwz>

Addition: <https://pastebin.com/cmuGd0Sg>

Thank you again in advance.

5chn4pp - September 30, 2017, 12:10 am

C:\WINDOWS\system32\Drivers\DrToolKrl.sys

That file is very interesting to me, it's probably the rootkit that drops the files, could you upload that file and send it to me for analysis?

crimezy - September 30, 2017, 3:20 am

Seems like I cannot copy or upload the file anywhere because access is denied. Seems like that file

is kind of new and could be causing the problem.. What should I do to show that file to you?

5chn4pp - September 30, 2017, 8:53 am

Try this:

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.

crimezy - September 30, 2017, 11:03 am

Seems like the process can't be stopped.

Have a look: <https://pastebin.com/m8P66KB0>

5chn4pp - September 30, 2017, 10:37 pm

Please download [Malwarebytes Anti-Rootkit](#) and save the file to your desktop. Please rename the file MBAR.exe to abc.exe

Right-Click abc.exe and select Run as administrator to run the installer.

Select your Desktop as the location to extract the contents and click OK. The program should open upon completion.

Click Next, followed by Update. Upon update completion, click Next.

Ensure Drivers, Sectors & System are checked and click Scan.

Do not use your computer during the scan.

Upon completion: If no malware is found, close the MBAR window.

If malware is found, ensure Create Restore Point is checked and click Cleanup. Reboot when prompted.

Two logs (mbar-log.txt and system-log.txt) will be created. Copy the contents of both logs and paste them to pastebin.com. Both logs can be found in the MBAR folder.

crimezy - October 1, 2017, 3:25 am

I followed the steps and I found something but I don't think it solved the problem..

This is the log: <https://pastebin.com/xKYma21Q>

5chn4pp - October 1, 2017, 4:35 am

(Oct 1, 2017 03:25 AM)crimezy Wrote: [\[CITE\]](#) I followed the steps and I found something but I don't think it solved the problem..

This is the log: <https://pastebin.com/xKYma21Q>

Doesn't MBAR create 2 logs if I remember correctly?

crimezy - October 1, 2017, 5:27 am

You're right, I'm sorry.

This is the second log you're asking for: <https://pastebin.com/2xHFhm0D>

5chn4pp - October 1, 2017, 5:30 am

Interesting.

Please download [HitmanPro](#) and save it to your desktop. Quit all running programs.

Right-click on the program and select Run as Administrator to start and when prompted allow it to run.

Click the settings tab and go into Advanced, then enable Early Warning Scoring.

Click OK and Next then select No, I only want to perform a one-time scan to check this computer.

Click Next and it should start the scan, please be patient.

When the scan completes click "Save log", and save it to your desktop. Close the program > Don't Fix anything!

Post the contents of the log in your next reply.

crimezy - October 1, 2017, 5:38 am

Here you go!

This is the log from HitmanPro: <https://pastebin.com/DK4VP7M6>

5chn4pp - October 1, 2017, 5:51 am

Alright, lets try some commands that I haven't used before, this should probably work:

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.

crimezy - October 1, 2017, 10:39 am

The file in question doesn't want to get deleted I see.

Check the logs out: <https://pastebin.com/N88u5qQE>

5chn4pp - October 1, 2017, 10:46 am

Last tool before we go to safemode or something like that to remove it:

Please download [aswMBR](#) and save the file to your desktop. Right-Click aswMBR.exe and select Run as administrator to run the program.

Click Yes when prompted to download avast! virus definitions. Wait until AVAST engine defs: ### appears.

If you are prompted to enable the use of "Virtualization Technology", click Yes.

Click the AV Scan: drop down box and click C:\.

Click Scan.

Upon completion, you will see Scan finished successfully. Click Save log. Save the log to your Desktop.

Copy the contents of the log to pastebin.com and paste the link in your next reply.

Note: Do NOT click Fix or FixMBR.

Note: A file (MBR.dat) will be created on your Desktop. Do NOT click or delete it.

crimezy - October 1, 2017, 11:13 am

Alright, when I run aswMBR it asks me for virtualization but If I click yes windows crashes (the screen with the sad smile :(). I tried without virtualization, updated virus defs but at some point it crashes and doesn't scan anymore. I saw it detected DrToolKrl.sys as a locked file though, the text was in yellow.

Another question, I may be away from my PC for a few days, do you think I will be able to remote control my desktop and use it to follow along and remove the virus?

Thank you for your patience!

5chn4pp - October 1, 2017, 11:18 am

I think you can do it remotely, but its probably best if you are there physically.

Do you know how to enter safemode?

crimezy - October 1, 2017, 11:40 am

Yes I do! Connection required?

5chn4pp - October 1, 2017, 11:54 am

Yeah why not.

When you are in safemode, try aswmbR again with virtualization, if it does not work, try this fixlist with FRST:

<https://pastebin.com/raw/bk157cyV>

crimezy - October 6, 2017, 6:59 am

I'm really sorry for the delay but I've been away from my PC and I thought it'd be better to wait and come home.

aswMBR doesn't ask me for virtualization in safemode, however it crashes as soon as it starts scanning. The crash gives the same error of the other crashes while in normal mode (it's happening frequently since I got infected)

and it's the following: IRQL_NOT_LESS_OR_EQUAL

I tried FRST but it seems like it's not working either. This is the log file:

<https://pastebin.com/2ufU6XCu>

EDIT: I downloaded Kaspersky TDSS Killer and ran it in safemode. It detected DrToolKrl.sys and deleted it after reboot. These are new FRST logs in case you want to check if it's all clear.

FRST: <https://pastebin.com/gx32QZy4>

Addition: <https://pastebin.com/TDEQ1uHs>

5chn4pp - October 6, 2017, 7:47 am

Could you provide the logs created by TDSSKiller?

C:\WINDOWS\Minidump\

I'd like a .dmp file from here, upload it to share.riseup.net and post a link here.

crimezy - October 6, 2017, 11:38 am

There are like 30-40 files but this is the most recent.

There you go: <https://share.riseup.net/#6iLRmRyMWfi3eJf6WVwDow>

5chn4pp - October 6, 2017, 11:47 am

C:\TDSSKiller.3.1.0.15_06.10.2017_16.19.36_log.txt

C:\TDSSKiller.3.1.0.15_06.10.2017_16.18.23_log.txt

Need these also pls

crimezy - October 7, 2017, 2:39 am

This is TDSSKiller.3.1.0.15_06.10.2017_16.18.23_log: <https://pastebin.com/qdK5kESb>

TDSSKiller.3.1.0.15_06.10.2017_16.19.36_log: <https://pastebin.com/7JN1FVTU>

5chn4pp - October 7, 2017, 3:21 am

Your system looks fairly clean now, do you get any crashes now?

C:\TDSSKiller_Quarantine\

There should be a file here, could you send that to me for analysis?

Last scan:

Please download [Junkware Removal Tool](#) to your desktop. Run the tool by double-clicking it. If you are using Windows Vista, 7, or 8; instead of double-clicking, right-mouse click JRT.exe and select "Run as Administrator".

The tool will open and start scanning your system.

Please be patient as this can take a while to complete depending on your system's specifications.

On completion, a log (JRT.txt) is saved to your desktop and will automatically open.

Post the contents of JRT.txt into your next message.

crimezy - *October 7, 2017, 6:04 am*

This is the log: <https://pastebin.com/ZTKRMxG1>

And this is the compressed quarantine folder:

<https://share.riseup.net/#GOwn-jO0oHM2QVuvM508Og>

5chn4pp - *October 7, 2017, 6:26 am*

Your system should be good now, there are no other signs of malware.

Have a nice day. ?

crimezy - *October 7, 2017, 10:41 am*

Thank you for your help and for guiding me through the solution :)

Have a nice day too!

Voxilities651 - *October 12, 2017, 3:57 am*

thanks for ur help, helped me 2