

Forum:[Hack Forums](#)

Thread: [Safety check, please \[unclaimed\] \[logs inside\]](#)

Ordium - May 1, 2016, 9:06 am

Just had a cyber security breach in my family. I'd like to check that the cause was nothing on my PC.

I would greatly appreciate a check up from anyone.

Code FRST: <http://pastebin.com/y3uGL4Nk>

Addition: <http://pastebin.com/5kCQ2CRM>

Frukt - May 1, 2016, 9:09 am

Look at other posts and see what you have to do, they need farbar scan to analyze it.

Look around here and then upload it to pastebin and edit it in here.

(I'm not a certified white-hat virus remover here.)

Ordium - May 1, 2016, 9:13 am

(May 1, 2016 09:09 AM)KruktFPS Wrote: [\[CITE\]](#) Look at other posts and see what you have to do, they need farbar scan to analyze it.

Look around here and then upload it to pastebin and edit it in here.

(I'm not a certified white-hat virus remover here.)

I actually started to do this, but I didn't want to start with one program and have a knowledgeable person be using a different one.

Frukt - May 1, 2016, 10:45 am

(May 1, 2016 09:13 AM)Ordium Wrote: [\[CITE\]](#) I actually started to do this, but I didn't want to start with one program and have a knowledgeable person be using a different one.

If I understood you reply, You won't damage the system in any way.

It will scan it and it will help both you and the "helper".

EDIT: I saw you posted the scans now, good job! I hope you are safe, good luck!

ProtectNull™ - May 1, 2016, 1:51 pm

Hello I am here to assist you,

Please read these before we start with the procedures,

Please do not follow any other instructions other than mine, as they can cause conflict between my fixes.

Please be patient, as you can see I have other people to assist.

Please consider backing up any important files incase, (usually I will create System Restore Points if needed)

Please read the instructions carefully, as it can help a lot.

Do not login to valuable sites such as banking etc.

[img]http://nilights.info/wp-content/uploads/2014/05/divider.png[/img]

Please open notepad and copy paste the contents in the codebox below. (Do not include "Code:" tags)

Code start

CloseProcesses:

Task: {70EADB1C-86E1-4B2B-A792-2BE54100ADA3} - \CCleanerSkipUAC -> No File <====

ATTENTION

Task: C:\WINDOWS\Tasks\SUPERAntiSpyware Scheduled Task
edebb14e-0be5-4890-b59d-841657fe7708.job => C:\Program

Files\SUPERAntiSpyware\SASTask.exedC:\Program

Files\SUPERAntiSpyware\SUPERAntiSpyware.exe

Task: C:\WINDOWS\Tasks\SUPERAntiSpyware Scheduled Task
d820ce1e-bd4e-4d66-8792-c841bc6377dd.job => C:\Program

Files\SUPERAntiSpyware\SASTask.exedC:\Program

Files\SUPERAntiSpyware\SUPERAntiSpyware.exe

HKLM\...\StartupApproved\StartupFolder: => "TenClips.lnk"

FirewallRules: [MSMQ-In-TCP] => (Allow) %systemroot%\system32\mqsvc.exe

FirewallRules: [MSMQ-Out-TCP] => (Allow) %systemroot%\system32\mqsvc.exe

FirewallRules: [MSMQ-In-UDP] => (Allow) %systemroot%\system32\mqsvc.exe

FirewallRules: [MSMQ-Out-UDP] => (Allow) %systemroot%\system32\mqsvc.exe

FirewallRules: [vm-monitoring-nb-session] => (Allow) LPort=139

FirewallRules: [WCF-NetTcpActivator-In-TCP-64bit] => (Allow) LPort=808

FirewallRules: [{CEF273C7-34F1-4323-B24E-E6618D1A2228}] => (Allow)

C:\Users\TJ\AppData\Roaming\utorrent\utorrent.exe

FirewallRules: [{434182BE-3E23-4565-BEF4-7650DC09C02C}] => (Allow)

C:\Users\TJ\AppData\Roaming\utorrent\utorrent.exe

FirewallRules: [{6FB7AD27-823C-4976-B919-BB57F467735F}] => (Allow)

C:\Users\TJ\AppData\Roaming\utorrent\utorrent.exe

FirewallRules: [{9FB461D4-3C17-4DFE-ACE0-C3CECE2C6CA4}] => (Allow)

C:\Users\TJ\AppData\Roaming\utorrent\utorrent.exe

FirewallRules: [{53390235-E0B4-492C-B317-3CE785B6B369}] => (Allow)

C:\Users\TJ\AppData\Roaming\utorrent\utorrent.exe

FirewallRules: [{48133778-C688-4978-958D-D4E0DD9D7357}] => (Allow)

C:\Users\TJ\AppData\Roaming\utorrent\utorrent.exe

EmptyTemp:

Hosts:

Click File, Save As and enter fixlist.txt as the file name.

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 environment.
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.

[img]http://nilights.info/wp-content/uploads/2014/05/divider.png[/img]

Download this here [ESET Online Scanner](#)

Turn off the real time scanner of any existing antivirus program while performing the online scan.

Tick the box next to YES, I accept the Terms of Use.

Click Start

Make sure that the option Remove found threats is unticked

Click on Advanced Settings and ensure these options are ticked

- 1) Scan for potentially unwanted applications
- 2) Scan for potentially unsafe applications
- 3) Enable Anti-Stealth Technology

Click Scan

Wait for the scan to finish

If any threats were found, click the 'List of found threats' , then click Export to text file....

Save it to your desktop, then please copy and paste that log to pastebin and paste the pastebin link to your next reply.