

Forum: [Hack Forums](#)

Thread: Good chance of being infected

skelly76 - April 27, 2016, 9:46 pm

ZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZ

ProtectNull™ - April 27, 2016, 9:49 pm

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

Farbar Recovery Scanning ToolRight click to run as administrator (XP users click run after receipt of Windows Security Warning - Open File). When the tool opens click Yes to disclaimer.

Press Scan button.

It will produce a log called FRST.txt in the same directory the tool is run from.

Please copy and paste the log back here

The first time the tool is run it generates another log (Addition.txt - also located in the same directory as FRST.exe/FRST64.exe). Please also paste that along with the FRST.txt into your reply.

TDSSKillerPlease download [TDSSKiller](#) and save the file to your Desktop.

Right-Click TDSSKiller.exe and select Run as Administrator

Click Change parameters. Place a checkmark next to Detect TDLFS file system and Verify file digital signatures.

Click Start Scan. Do not use the computer during the scan.

If objects are found, change the action to skip.

Click Continue and close the window.

A log will be created and saved to the root directory (usually C:\). Paste the file contents to pastebin.com and post the link in your next reply.

skelly76 - April 27, 2016, 10:03 pm

FRST.txt : <http://pastebin.com/V54khzeg>

Addition.txt : <http://pastebin.com/wf0iMp6R>

TDSS Log : <http://pastebin.com/FUiWDJWN>

ProtectNull™ - April 27, 2016, 10:09 pm

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

tags)

Code start

CloseProcesses:

HKLM-x32\...\Run: [] => [X]

HKU\S-1-5-21-1289391877-2754865104-1441491105-1000\...\MountPoints2:

{416f5da7-a9e3-11e5-ac84-806e6f6e6963} - D:\Autorun.exe

C:\Users\Aerial\AppData\Local\????????????????

FirewallRules: [{5F6687B4-A278-4403-BB2A-A7A27F19D8FE}] => (Allow) LPort=9143

FirewallRules: [{08EA0C79-EB6F-4A93-A823-A52D1C6094EE}] => (Allow) LPort=2333

FirewallRules: [TCP Query

User{D53CE6A0-01DD-46DD-959F-1781C47B63B7}C:\users\Aerial\AppData\Local\akamai\netsession_win.exe] => (Allow) C:\users\Aerial\AppData\Local\akamai\netsession_win.exe

FirewallRules: [UDP Query

User{C46B6EAD-C0AC-46F6-BD8D-ED7E4F8B593E}C:\users\Aerial\AppData\Local\akamai\netsession_win.exe] => (Allow) C:\users\Aerial\AppData\Local\akamai\netsession_win.exe

FirewallRules: [TCP Query User{59235C32-4539-454F-BC03-B1BA6F06D3A9}B:\program files

(x86)\minecraft\runtime\jre-x64\1.8.0_25\bin\javaw.exe] => (Allow) B:\program files

(x86)\minecraft\runtime\jre-x64\1.8.0_25\bin\javaw.exe

FirewallRules: [UDP Query User{A9CC614E-FC61-480F-83A6-8C2904F2A7CF}B:\program files

(x86)\minecraft\runtime\jre-x64\1.8.0_25\bin\javaw.exe] => (Allow) B:\program files

(x86)\minecraft\runtime\jre-x64\1.8.0_25\bin\javaw.exe

FirewallRules: [TCP Query

User{ED6A00C4-A740-41F6-8BDA-8CD1003FFADB}C:\users\Aerial\Desktop\+\\luminosity.exe] => (Allow) C:\users\Aerial\Desktop\+\\luminosity.exe

FirewallRules: [UDP Query

User{9A9705FC-E9EC-4552-82B4-4EA40E2DE7B1}C:\users\Aerial\Desktop\+\\luminosity.exe] => (Allow) C:\users\Aerial\Desktop\+\\luminosity.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

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.

ESET Online Scanner

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.

skelly76 - April 27, 2016, 10:23 pm

Fix Log: <http://pastebin.com/k8KZTxQ4>

Will update with ESET when done.

ProtectNull™ - April 27, 2016, 10:36 pm

(Apr 27, 2016 10:23 PM)Aerial Wrote: [\[CITE\]](#) Fix Log: <http://pastebin.com/k8KZTxQ4>

Will update with ESET when done.

Sweet ?

skelly76 - April 27, 2016, 10:56 pm

ESET: <http://pastebin.com/AB8wYjL6>

ProtectNull™ - April 27, 2016, 10:59 pm

(Apr 27, 2016 10:56 PM)Aerial Wrote: [\[CITE\]](#) ESET: <http://pastebin.com/AB8wYjL6>

I see a trojan dropper instance,

Download this [NPE](#)

Click Download Norton Power Eraser, above.

On the File Download dialog, click Save.

Select the location to where you want the file saved, and click Save.

Go to the location of the downloaded file and double-click the NPE icon.

Then click 'Scan for risks', let this do its thing and once its done and it shows detected items, please DO NOT DO ANYTHING but screenshot the detected items, upload it to imgur and past image link

here.

RKill

Download this here [RKILL](#)

Double-click on the Rkill icon to run the tool.

If using Vista or Windows 7/8/10, right-click on it and Run As Administrator.

A black DOS box will briefly flash and then disappear. This is normal and indicates the tool ran successfully.

A log pops up at the end of the run. This log file is located at C:\rkill.log. Please post this in your next reply (pastebin link)

If you do not see the black box flash on the screen delete the icon from the desktop and go back to the link for the download, select the next button and try to run the tool again, continue to repeat this process using the remaining buttons until the tool runs.

If they detect anything, I will create a fix file. ?

skelly76 - April 27, 2016, 11:15 pm

NPE:

rkill: <http://pastebin.com/LRuHuPUG>

ProtectNull™ - April 27, 2016, 11:50 pm

(Apr 27, 2016 11:15 PM)Aerial Wrote: [\[CITE\]](#) NPE:

rkill: <http://pastebin.com/LRuHuPUG>

in NPE can you export the log file and send it over @ pastebin? ?

skelly76 - April 28, 2016, 12:13 am

(Apr 27, 2016 11:50 PM)ProtectNull™ Wrote: [\[CITE\]](#) in NPE can you export the log file and send it over @ pastebin? ?

I'll have this done sometime tomorrow gotta head to bed. I'll pm you when I update.

ProtectNull™ - April 28, 2016, 12:41 am

(Apr 28, 2016 12:13 AM)Aerial Wrote: [\[CITE\]](#) I'll have this done sometime tomorrow gotta head to bed. I'll pm you when I update.

Sweet ?

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

Code start

CloseProcesses:

c:\programdata\package cache\{d5391b46-ec3d-3030-828d-5199900ab768}\v0.5.21002\jay.exe

c:\program files (x86)\iobit\liveupdate\liveupdate.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 [AdwCleaner](#)
Double click on AdwCleaner.exe to run the tool.

Click on the Scan button.

When it's done you'll see: Pending: Please uncheck elements you don't want removed.

Now click on the Report button...a logfile (AdwCleaner[R0].txt) will open in Notepad for review.

Look over the log especially under Files/Folders for any program you want to save.

If there's a program you may want to save, just uncheck it from AdwCleaner.

If you're not sure, post the log for review in pastebin.com and paste link in next reply.

If you're ready to clean it all up, click the Clean button.

After rebooting, a logfile report (AdwCleaner[S0].txt) will open automatically.

Copy and paste the contents of that logfile in your next reply.

A copy of that logfile will also be saved in the C:\AdwCleaner folder.

skelly76 - May 1, 2016, 9:32 pm

FRST: <http://pastebin.com/UjFLHVbX>

Adw: <http://pastebin.com/OXChgktc>

Also at random times now my AV keeps reporting viruses in my Temp folder that has the same item

name every time. Did we miss something?

ProtectNull™ - May 1, 2016, 10:14 pm

(May 1, 2016 09:32 PM)Aerial Wrote: [\[CITE\]](#) FRST: <http://pastebin.com/UjFLHVbX>
Adw: <http://pastebin.com/0XChgkctc>

Also at random times now my AV keeps reporting viruses in my Temp folder that has the same item name every time. Did we miss something?

Interesting, I deleted the TEMP Folder (2gb worth)

Please do ESET again.

skelly76 - May 2, 2016, 9:30 pm

(May 1, 2016 10:14 PM)ProtectNull™ Wrote: [\[CITE\]](#) Interesting, I deleted the TEMP Folder (2gb worth)

Please do ESET again.

Nothing that was suspicious came up on ESET. So am I all set?

ProtectNull™ - May 2, 2016, 9:53 pm

(May 2, 2016 09:30 PM)Aerial Wrote: [\[CITE\]](#) Nothing that was suspicious came up on ESET. So am I all set?

I need logs so I can just see. ?

skelly76 - May 2, 2016, 11:13 pm

ESET: <http://pastebin.com/PStyVM5v>

It's the same as last time. None of them are malicious software.

ProtectNull™ - May 2, 2016, 11:51 pm

(May 2, 2016 11:13 PM)Aerial Wrote: [\[CITE\]](#) ESET: <http://pastebin.com/PStyVM5v>

It's the same as last time. None of them are malicious software.

Please download [SecurityCheck](#)

Please save the file into your desktop. And run the program as administrator.

A CMD box should popup, please press any key for it to proceed.

After it is done, it should show a 'Checkup.txt' file/notepad.

Copy contents into pastebin and post it in your next reply.

skelly76 - May 3, 2016, 12:38 am

SecurityCheck: <http://pastebin.com/WrdmWgve>

ProtectNull™ - May 3, 2016, 12:39 am

Are you using HDD or SSD for your Operating Drive?

skelly76 - May 3, 2016, 12:39 am

(May 3, 2016 12:39 AM)ProtectNull™ Wrote: [\[CITE\]](#) Are you using HDD or SSD for your Operating

Drive?
SSD.

ProtectNull™ - May 3, 2016, 12:40 am

(May 3, 2016 12:39 AM)Aerial Wrote: [\[CITE\]](#) SSD.Please download [RougeKiller](#) and save the file to your Desktop.

Right-Click RougeKiller.exe and select Run as Administrator

Click Scan. Do not use the computer during the scan.

A log will be created and saved to the root directory. Paste the file contents to pastebin.com and post the link in your next reply.

skelly76 - May 3, 2016, 12:45 am

(May 3, 2016 12:40 AM)ProtectNull™ Wrote: [\[CITE\]](#) Please download [RougeKiller](#) and save the file to your Desktop.

Right-Click RougeKiller.exe and select Run as Administrator

Click Scan. Do not use the computer during the scan.

A log will be created and saved to the root directory. Paste the file contents to pastebin.com and post the link in your next reply.

Most of my files are on an HDD just by the way. Scanning now.

ProtectNull™ - May 3, 2016, 12:47 am

(May 3, 2016 12:45 AM)Aerial Wrote: [\[CITE\]](#) Most of my files are on an HDD just by the way. Scanning now.

What OS are you in btw? Sorry If I've said this before.

skelly76 - May 3, 2016, 12:51 am

(May 3, 2016 12:47 AM)ProtectNull™ Wrote: [\[CITE\]](#) What OS are you in btw? Sorry If I've said this before.

Rogue: <http://pastebin.com/piwDQSDu>

ProtectNull™ - May 3, 2016, 1:31 am

(May 3, 2016 12:51 AM)Aerial Wrote: [\[CITE\]](#) Windows 7 Home Premium

Rogue: <http://pastebin.com/piwDQSDu>

Please in start menu type in 'Disk Defragmenter' and just screenshot what it shows. ?

skelly76 - May 4, 2016, 3:29 pm

(May 3, 2016 01:31 AM)ProtectNull™ Wrote: [\[CITE\]](#) Please in start menu type in 'Disk Defragmenter' and just screenshot what it shows. ?

The program "Disk Defragmenter" shows up. Nothing else.

I can't take a screenshot of the start menu while searching. I can make a short .gif if you really want to see.

Nuworld - May 4, 2016, 6:40 pm

(May 3, 2016 12:47 AM)ProtectNull™ Wrote: [\[CITE\]](#) What OS are you in btw? Sorry If I've said this before.

The OS was included in the FRST logs.

Quote:Platform: Windows 7 Home Premium Service Pack 1 (X64) Language: English (United States)

OP Try using the Snipping tool in windows to post screen shots.

skelly76 - May 4, 2016, 6:59 pm

I just did this.

<https://gyazo.com/4917038fe0e752a668511f62fa842ead>

ProtectNull™ - May 4, 2016, 9:35 pm

(May 4, 2016 06:59 PM)Aerial Wrote: [\[CITE\]](#) I just did this.

<https://gyazo.com/4917038fe0e752a668511f62fa842ead>

I mean also click on it. ?

(May 4, 2016 06:40 PM)Nuworld Wrote: [\[CITE\]](#) The OS was included in the FRST logs.

OP Try using the Snipping tool in windows to post screen shots.

Yeah, It was in the morning and didn't think about FRST having the OS.