

Forum:[Hack Forums](#)

Thread: [Known Infection - Possible Infection](#)

Geno - April 14, 2015, 6:06 pm

I was just recently infected with a RAT & Malware.

I used a series of tools to clean my computer like -

Hijackthis
Malwarebytes
Microsoft Security Essentials
CCleaner

After using these, I also found a couple backdoor bots with some others different kinds of malware, then my registry settings were also effected pretty badly.

My browser (google chrome) was hijacked as well. I also still have malware related programs that won't remove from my control panel "installed programs" list.

I need some help from a trusted member on here to help me remove the rest of this nonsense and make sure that I'm no longer infected by a RAT that I was previously caught by.

Please let me know if you can help by replying to this thread or PMing me.

Thanks,

- Geno

TazzyOpz - April 14, 2015, 6:42 pm

[-Running NoBot-]

Download NoBot from [here](#) and save it to your Desktop.

? Double-click NoBot.exe

Go to File -> Settings and make sure the following are checked

?• Detect Suspicious File Paths

?• Scan Registry

• Detect Dropped Files

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

? Then Click the Scan button.

? Once the scan is finished You can view the Scan log by going to File -> Scan Logs. Then copy and paste the scan log here.

It is recommend to post the scan log here before removing any files detected unless you know for sure the file found is infected.

[-Running RogueKiller-]

Download RogueKiller from [here](#) and save it to your Desktop.

?• Double-click RogueKiller.exe

?• Click the Scan button.

? Once the scan is finished You can view the Scan log by clicking the Report button. Then copy and paste the scan log here.

It is recommend to post the scan log here before removing any files detected unless you know for sure the file found is infected.

[-Running SuperAntiSpyware-]

Download RogueKiller from [here](#) and save it to your Desktop.

?• Double-click SUPERAntiSpyware.exe

?• Proceed through the Install.

?• Click the Scan This Computer button.

?• Then Click the Complete Scan button. (This will do a full scan of your computer)

?Once the scan is finished remove what it finds.

If you have any Anti-Virus I'd recommend running a full scan with that as well.

Tha Sneak - April 14, 2015, 7:38 pm

Run this:

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

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

Press Scan button.

It will produce a log called FRST.txt.

Please copy and paste log in [Code] or [Quote].

The first time the tool is ran 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.

@Tazzyops, he can run all the scans he wants, but automatic tools will never completely get rid of that. You have to have some kind of diagnostics and you have to do one thing at a time with no more than 2 tools ran at the same instance.

Geno - April 14, 2015, 9:05 pm

Thank you, Tha Sneak.

They were too large to post here, but I have used pastebin.

FRST: <http://pastebin.com/gSW7Wden>

Addition: <http://pastebin.com/tYE1JfbE>

Tha Sneak - April 14, 2015, 9:54 pm

If you ran RogueKiller could you please post that log here as well?

Geno - April 15, 2015, 3:06 pm

(Apr 14, 2015 09:54 PM)Tha Sneak Wrote: [\[CITE\]](#) If you ran RogueKiller could you please post that log here as well?

Code RogueKiller V10.5.10.0 [Apr 14 2015] by Adlice Software

mail : <http://www.adlice.com/contact/>

Feedback : <http://forum.adlice.com>
Website : <http://www.adlice.com/softwares/roguekiller/>
Blog : <http://www.adlice.com>

Operating System : Windows 7 (6.1.7601 Service Pack 1) 64 bits version
Started in : Normal mode
User : Admin [Administrator]
Started from : C:\Users\Admin\Downloads\RogueKiller.exe
Mode : Scan -- Date : 04/15/2015 17:03:38

Processes : 1

[Suspicious.Path] Deorro Bootie In Your Face Original Mix No Rock Drop.exe(2920) --
C:\ProgramData\{cb6578e7-9ebb-967c-cb65-578e79ebe39e}\Deorro Bootie In Your Face Original
Mix No Rock Drop.exe[-] -> Killed [TermProc]

Registry : 7

[PUM.Dns] (X64)

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters\Interfaces\{FD10C
BC6-AA50-4E82-A0E2-065D798FD45B} | DhcpNameServer : 131.210.201.96 131.210.1.24
131.210.201.95 131.210.1.26 [UNITED STATES (US)][UNITED STATES (US)][UNITED STATES
(US)][UNITED STATES (US)] -> Found

[PUM.Dns] (X64)

HKEY_LOCAL_MACHINE\System\ControlSet001\Services\Tcpip\Parameters\Interfaces\{FD10CBC
6-AA50-4E82-A0E2-065D798FD45B} | DhcpNameServer : 131.210.201.96 131.210.1.24
131.210.201.95 131.210.1.26 [UNITED STATES (US)][UNITED STATES (US)][UNITED STATES
(US)][UNITED STATES (US)] -> Found

[PUM.Dns] (X64)

HKEY_LOCAL_MACHINE\System\ControlSet002\Services\Tcpip\Parameters\Interfaces\{FD10CBC
6-AA50-4E82-A0E2-065D798FD45B} | DhcpNameServer : 131.210.201.96 131.210.1.24
131.210.201.95 131.210.1.26 [UNITED STATES (US)][UNITED STATES (US)][UNITED STATES
(US)][UNITED STATES (US)] -> Found

[PUM.DesktopIcons] (X64)

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Explorer\HideDesktopIcons\
NewStartPanel | {20D04FE0-3AEA-1069-A2D8-08002B30309D} : 1 -> Found

[PUM.DesktopIcons] (X64)

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Explorer\HideDesktopIcons\
NewStartPanel | {59031a47-3f72-44a7-89c5-5595fe6b30ee} : 1 -> Found

[PUM.DesktopIcons] (X86)

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Explorer\HideDesktopIcons\
NewStartPanel | {20D04FE0-3AEA-1069-A2D8-08002B30309D} : 1 -> Found

[PUM.DesktopIcons] (X86)

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Explorer\HideDesktopIcons\
NewStartPanel | {59031a47-3f72-44a7-89c5-5595fe6b30ee} : 1 -> Found

Tasks : 0

Files : 1

[Suspicious.Path][File] Deorro Bootie In Your Face Original Mix No Rock Drop.lnk --
C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Deorro Bootie
In Your Face Original Mix No Rock Drop.lnk [LNK@] C:\PROGRA~3\{CB657~1\DEORRO~1.EXE
--startup=1 -> Found

Hosts File : 0

Antirootkit : 0 (Driver: Not loaded [0xc000036b])

Web browsers : 0

MBR Check :

+++++ PhysicalDrive0: INTEL SSDSC2CW120A3 ATA Device +++++

--- User ---

[MBR] 6809e626665f4f227797762aee36534a

[BSP] e37c4b250a2f18b7a6e376ed38562c38 : Windows Vista/7/8 MBR Code

Partition table:

User = LL1 ... OK

User = LL2 ... OK

Tha Sneak - April 16, 2015, 11:11 am

One more thing I want to look at before I give you a fixlist.

Please download ComboFix from BleepingComputer.com

[Alternate link: GeeksToGo.com](http://GeeksToGo.com)

[Alternate link: Forospyware.com](http://Forospyware.com)

Rename ComboFix.exe to commy.exe before you save it to your DesktopDisable your AntiVirus and AntiSpyware applications, usually via a right click on the System Tray icon. They may otherwise interfere with our tools A guide to do this can be found [here](#)

Click Start then copy paste the following command into the search box & hit enter:

"%userprofile%\desktop\commy.exe" /stepdel

As part of it's process, ComboFix will check to see if the Microsoft Windows Recovery Console is installed. This will not install in Vista. Just continue scanning, and skip the console install.

When finished, it shall produce a log for you. Please include the contents of C:\ComboFix.txt in your next reply.

Geno - April 16, 2015, 11:31 am

(Apr 16, 2015 11:11 AM)Tha Sneak Wrote: [\[CITE\]](#) One more thing I want to look at before I give you a fixlist.

Please download ComboFix from BleepingComputer.com

[Alternate link: GeeksToGo.com](http://GeeksToGo.com)

[Alternate link: Forospyware.com](http://Forospyware.com)

Rename ComboFix.exe to commy.exe before you save it to your DesktopDisable your AntiVirus and AntiSpyware applications, usually via a right click on the System Tray icon. They may otherwise interfere with our tools A guide to do this can be found [here](#)

Click Start then copy paste the following command into the search box & hit enter:

"%userprofile%\desktop\commy.exe" /stepdel

As part of it's process, ComboFix will check to see if the Microsoft Windows Recovery Console is installed. This will not install in Vista. Just continue scanning, and skip the console install.

When finished, it shall produce a log for you. Please include the contents of C:\ComboFix.txt in your next reply.

Alright here are the results: [Click here](#)

Thanks again for helping me with this.

Tha Sneak - April 18, 2015, 11:48 am

Re-running ComboFix to remove infections:

Close any open browsers.

Close/disable all anti virus and anti malware programs so they do not interfere with the running of ComboFix.

Open notepad and copy/paste the text in the quotebox below into it:

Quote:File::

c:\users\Admin\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\
Deorro Bootie In Your Face Original Mix No Rock Drop.lnk

Folder::

c:\programdata\{cb6578e7-9ebb-967c-cb65-578e79ebe39e} Save this as CFScript.txt, in the same location as ComboFix.exe

Referring to the picture above, drag CFScript into ComboFix.exe

When finished, it shall produce a log for you at C:\ComboFix.txt

Please post the contents of the log in your next reply.