

Forum:[Hack Forums](#)

Thread: [Virus is duplicating, taking up all the resources and freezing my computer](#)

Big Chuck - February 16, 2014, 9:25 am

After doing a full scan with Malwarebytes and removed over 80 items, my computer became really slow and the user Aura assisted me through Teamviewer and noticed that I was infected with a malware that duplicates itself and takes up all my computer resources. The process is called dynope.exe.

Posting this thread now as I don't know how long I have till the virus freezes my computer again. I'll be updating one log at the time.

Paradoxum - February 16, 2014, 5:07 pm

Firstly, I am not sure why others thought it was fine to post in this section if they are not official helpers, regardless of whether or not you had logs posted. Second, I am not sure where you got the idea to run all these scanners that will not solve the problem. ?

Step 1

Please download Farbar Recovery Scan Tool from one of the following links and save it to the root of your flash drive.

['32-bit'](#)

['64-bit'](#)

With the flash drive still plugged in, reboot your computer.

Continuously tap F8 when the BIOS loads until you get to the Advanced Boot Options screen. Select Repair Your Computer > Enter.

Select English > Next.

Select your operating system > Next.

Select your administrator account > Next.

On the System Recovery Options menu, choose Command Prompt. Type Notepad and press Enter.

Notepad will pop-up. Proceed to File > Open....

Select Computer. Take note of the drive letter of the flash drive.

Back to the command prompt, type X:\frst.exe (32-bit) or X:\frst64 (64-bit), where X should be replaced with the letter you took note of earlier.

Farbar Recovery Scan Tool will run. Click Yes > Scan.

FRST.txt will be created after a short while.

Reboot the system normally. Copy and paste the content of the log into your next reply.

In your next post, please provide the following:

Farbar Recovery Scan Tool Log

Big Chuck - February 16, 2014, 8:53 pm

Hello there. Thanks for the assistance. I took note of the first drive letter and replaced it with the F. I get the error "the device is not ready" in the CP menus. I went into notepad and opened computer, and it said that there is nothing in the drive even though I do have a flash drive plugged in. And I did do the steps before and made sure the program was on the flash drive.

Paradoxum - February 17, 2014, 1:24 am

May I ask that you use another flash drive? The computer has to be able to read it. Otherwise the process is not going to work and I'll have to give you an alternative solution. Do remember the following: Your computer is 64-bit so choose the appropriate download and follow the correct steps.

The flash drive has to be inserted and recognized by the computer first before you follow the above steps. That means: Boot your computer normally.

Plug in your flash drive.

Wait for it to recognize the flash drive.

Once it has, download the 64-bit version of FRST and paste it at the root of the flash drive.

Follow the remaining instructions stated [here](#).

Big Chuck - February 17, 2014, 9:55 am

Well, I tried a new flash drive and everything and it still doesn't work. Still getting the device is not ready. It still says under computer that there is no removable disk in the (F:) drive, but the flash drive is plugged in and on.

Paradoxum - February 17, 2014, 5:06 pm

Are you able to produce a normal FRST scan before you computer "spikes"?

Big Chuck - February 17, 2014, 5:17 pm

I can certainly try. Is that what you want me to do? I have a feeling I could, but it will take a very long

time. I can leave it on overnight if need be.

Paradoxum - February 17, 2014, 8:35 pm

It shouldn't take longer than 5 minutes on a normal computer. Give it a shot. If it goes on for about 30 minutes, terminate it and let me know. I'll think of another solution. Do you have a CD and CD reader, by the way? How about an extra computer you can use momentarily?

Big Chuck - February 17, 2014, 8:40 pm

Okay, I will run it tomorrow and will report back. Late here and have had another frustrating day. Not sure what you mean by cd and cd reader, sorry I'm not very computer savvy like yourself :P.

The only other computers I have are my parents which are owned by the government, so I can't really download or do anything that could help I assume.

Paradoxum - February 17, 2014, 8:46 pm

[This](#) is a CD. ? Anyway, please post once done. I only check threads in which I am not the last poster. Curious--how about an external drive (HDD)? Do you have one?

Big Chuck - February 17, 2014, 8:51 pm

HAHA, I'm very sorry. I figured it was something more complex then that, seeing as I think everyone has a cd and cd reader. I'm not that dumb, sorry :P.

And no, I do not believe I have an external hard drive. I'm on a dell laptop, Inspiron.

Paradoxum - February 18, 2014, 1:06 am

That means you have one, right? We'll need it because your flash drive is being naughty. Anyway, post back after you've tried producing a scan. ?

Big Chuck - February 18, 2014, 12:01 pm

I got the logs, scan took roughly 20 minutes. It gave me two different notepad documents, so I will post both. I attempted to post them both right into the post, but it said the post was too big. Not sure how much time my comp will run for so I decided to just make them pastebins. Sorry.

<http://pastebin.com/zC0R9xps>

<http://pastebin.com/jpVvNv0U>

Paradoxum - February 19, 2014, 10:18 am

Yay, logs. ? Don't take my word for it, but I have a feeling this issue isn't 100% malware-related... Do you remember installing a few updates from Windows Update?

Step 1

Run FRST.exe.

Copy and paste this to Notepad. Save it as fixlist.txt.

```
Quote:(JenMeramkul S.O.L.) C:\Users\Conjon\AppData\Roaming\Byevig\dynop.exe
C:\Users\Conjon\AppData\Roaming\Byevig
(Microsoft Corporation) C:\Windows\syswow64\dlhhost.exe
HKU\DEFAULT\...\RunOnce: [SpUninstallDeleteDir] - rmdir /s /q "\SearchProtect"
HKU\S-1-5-21-49055449-2376379733-193483228-1001\...\Run: [Goepuwvuugimr] -
C:\Users\Conjon\AppData\Roaming\Byevig\dynop.exe [283757 2013-12-21] (JenMeramkul S.O.L.)
HKU\S-1-5-21-49055449-2376379733-193483228-1001\...\MountPoints2: F - F:\Autorun.exe
HKU\S-1-5-21-49055449-2376379733-193483228-1001\...\MountPoints2:
```

{1fc2f716-e743-11e2-8d96-bc7737c94b35} - H:\Autorun.exe
HKU\S-1-5-21-49055449-2376379733-193483228-1001\...\MountPoints2:
{ff3d5f11-de30-11e2-9072-9c509db6af32} - F:\Autorun.exe
HKU\S-1-5-21-49055449-2376379733-193483228-1001\...409d6c4515e9\InprocServer32:
[Default-shell32]
\\?\globalroot\Device\HarddiskVolume3\Users\Conjon\AppData\Local\Temp\susfoxp\smerpsp\wow.d
ll ATTENTION! =====> ZeroAccess?
Applnit_DLLs: C:\PROGRA~2\SearchProtect\SearchProtect\bin\SPVC64Loader.dll => File Not
Found
Applnit_DLLs-x32: C:\PROGRA~2\SearchProtect\SearchProtect\bin\SPVC32Loader.dll => File Not
Found
C:\PROGRA~2\SearchProtect
SearchScopes: HKLM - DefaultScope {6772D856-7B10-4F42-B248-6E3CA2234828} URL =
<http://start.funmoods.com/results.php?f=4&q={searchTerms}&a=adknlg&chnl=adknlg&cd=2XzutAtN2Y1L1Qzu0B0CyByBtAyB0CzyyE0BtAtByBtCyCzztN0D0TzutBtDtCtBtDyCtBtB&cr=353172034>
SearchScopes: HKLM - {0633EE93-D776-472f-A0FF-E1416B8B2E3A} URL =
SearchScopes: HKLM - {6772D856-7B10-4F42-B248-6E3CA2234828} URL =
<http://start.funmoods.com/results.php?f=4&q={searchTerms}&a=adknlg&chnl=adknlg&cd=2XzutAtN2Y1L1Qzu0B0CyByBtAyB0CzyyE0BtAtByBtCyCzztN0D0TzutBtDtCtBtDyCtBtB&cr=353172034>
SearchScopes: HKLM-x32 - Backup.Old.DefaultScope
{6772D856-7B10-4F42-B248-6E3CA2234828}
SearchScopes: HKLM-x32 - {6772D856-7B10-4F42-B248-6E3CA2234828} URL =
<http://start.funmoods.com/results.php?f=4&q={searchTerms}&a=adknlg&chnl=adknlg&cd=2XzutAtN2Y1L1Qzu0B0CyByBtAyB0CzyyE0BtAtByBtCyCzztN0D0TzutBtDtCtBtDyCtBtB&cr=353172034>
SearchScopes: HKLM-x32 - {B67F2F94-D2D3-4AA3-B635-596A1CCC2A9F} URL =
\${SEARCH_URL}{searchTerms}
SearchScopes: HKCU - ToolbarSearchProviderProgress
{96bd48dd-741b-41ae-ac4a-aff96ba00f7e}
SearchScopes: HKCU - Backup.Old.DefaultScope {3BD44F0E-0596-4008-AEE0-45D47E3A8F0E}
SearchScopes: HKCU - {3A5C6A67-996C-467E-922A-8DF25457CACD} URL =
http://search.yahoo.com/search?fr=chr-greentree_ie&ei=utf-8&ilc=12&type=994519&p={searchTerms}
SearchScopes: HKCU - {6D60EA88-0DEE-4856-A7BB-273023E26127} URL =
<http://search.conduit.com/ResultsExt.aspx?q={searchTerms}&SearchSource=4&ctid=CT3291325&CUI=UN55997799115209119&UM=2>
SearchScopes: HKCU - {792F6E16-F6D1-7BD8-2E71-0C43A274B17C} URL =
<http://blekko.com/?source=c3348dd4&tbp=rbox&toolbarid=blekkotb&u=20120311B0BD4E1E85FE06421635BC76&q={searchTerms}>
SearchScopes: HKCU - {B67F2F94-D2D3-4AA3-B635-596A1CCC2A9F} URL =
<http://searchab.com/?aff=7&uid=d6692694-f60f-11e1-a11f-90f84214bc20&q={searchTerms}>
SearchScopes: HKCU - {D1F9CF21-29F8-4EBE-8A32-EDA4E5A98123} URL =
http://websearch.ask.com/custom/java/redirect?client=ie&tb=ORJ&o=100000030&src=kw&q={searchTerms}&locale=&apn_ptnrs=TV&apn_dtid=OSJ000
SearchScopes: HKCU - {DECA3892-BA8F-44b8-A993-A466AD694AE4} URL =
<http://search.yahoo.com/search?p={searchTerms}&fr=mkg028>
BHO-x32: TubeSaver - {7566cf60-3934-4ab3-be8e-40ed8df460d8} - C:\Program Files
(x86)\TubeSaver\133.dll No File
C:\Program Files (x86)\TubeSaver
FF SearchEngineOrder.1: Privitize VPN
FF SearchPlugin:
C:\Users\Conjon\AppData\Roaming\Mozilla\Firefox\Profiles\d2p1unez.default\searchplugins\ AOL-search.xml
FF SearchPlugin:

C:\Users\Conjon\AppData\Roaming\Mozilla\Firefox\Profiles\d2p1unez.default\searchplugins\bing-zu
go.xml
FF SearchPlugin: C:\Program Files (x86)\mozilla firefox\searchplugins\blekkotb.xml
FF Extension: ipFuck -
C:\Users\Conjon\AppData\Roaming\Mozilla\Firefox\Profiles\d2p1unez.default\Extensions\ipfuck@p4
ul.info.xpi [2013-12-22]

C:\Users\Conjon\AppData\Roaming\Mozilla\Firefox\Profiles\d2p1unez.default\Extensions\ipfuck@p4
ul.info.xpi
FF Extension: Define Ext - C:\Program Files (x86)\Mozilla Firefox\extensions\gystqfr@ylgga.com
[2013-09-30]
C:\Program Files (x86)\Mozilla Firefox\extensions\gystqfr@ylgga.com
FF HKCU\...\Firefox\Extensions: [{be02ceb4-b136-48a3-ab6b-bbe9484a93a8}] - C:\Program Files
(x86)\TubeSaver\133.xpi
CHR HKLM-x32\...\Chrome\Extension: [ojcdnngpmbenohhjlickdajclhbcaada] - C:\Program Files
(x86)\TubeSaver\133.crx [2011-07-01]
C:\Users\Conjon\AppData\Local\Google\Chrome\User
Data\Default\Extensions\lhpbbgjabfbiiabnpgajodepdclnfpn
C:\Users\Conjon\AppData\Local\Google\Chrome\User
Data\Default\Extensions\kbihjialmcplbhlockodgnilgoobfhap
C:\Users\Conjon\AppData\Local\Google\Chrome\User
Data\Default\Extensions\ibndcjiiebigejgnpddfipmbpndlmigig
C:\Users\Conjon\AppData\Local\Google\Chrome\User
Data\Default\Extensions\hnfaaffckpbebgoppomggmnaadjcabpne
C:\Users\Conjon\AppData\Local\Google\Chrome\User
Data\Default\Extensions\fbloaifakjebojlekmngngddkmdfdnfp
C:\Users\Conjon\AppData\Local\Google\Chrome\User
Data\Default\Extensions\dllpdkfbbinindpblacdckjaffjdmj
C:\Users\Conjon\AppData\Local\Google\Chrome\User
Data\Default\Extensions\cfmmgffogijfjfmhamonfknlgjbhmcddco
C:\Users\Conjon\AppData\Local\Google\Chrome\User
Data\Default\Extensions\bjgmbpodpcgmnpfjmigcckcjfldicnd
C:\Users\Conjon\AppData\Local\Google\Chrome\User
Data\Default\Extensions\ajopnjidmegmdimjlfnijceegpefgped
S2 vToolbarUpdater17.3.0; C:\Program Files (x86)\Common Files\AVG Secure
Search\vToolbarUpdater\17.3.0\ToolbarUpdater.exe [X]
2014-02-16 12:57 - 2014-02-16 12:57 - 000000___ () C:\Users\Conjon\Downloads\null.inneffective
2014-02-16 12:25 - 2014-02-16 12:25 - 00002411___ ()
C:\Users\Conjon\Desktop\RKreport[0]_S_02162014_122517.txt
2014-02-16 00:54 - 2014-02-16 22:52 - 000000___D () C:\Users\Conjon\Desktop\RK_Quarantine
2014-02-16 00:24 - 2014-02-16 00:24 - 000000___D () C:\Users\Conjon\Desktop\rkill
2014-02-16 00:19 - 2014-02-16 00:54 - 00001934___ () C:\Users\Conjon\Desktop\RKkill.txt
2014-02-16 00:19 - 2014-02-16 00:19 - 01038584___ (Bleeping Computer, LLC)
C:\Users\Conjon\Desktop\rkill64.com
2014-02-16 00:17 - 2013-11-20 20:55 - 01898232___ (Bleeping Computer, LLC)
C:\Users\Conjon\Desktop\rkill.com
2014-02-15 19:16 - 2014-02-15 19:16 - 00003812___ () C:\Windows\System32\Tasks\Security
Center Update - 3588189980
2014-02-15 19:15 - 2014-02-16 23:10 - 000000___D () C:\Users\Conjon\AppData\Roaming\Byeavg
2014-02-15 19:15 - 2014-02-16 00:00 - 00000802___ () C:\Windows\Tasks\Security Center
Update - 3588189980.job
2014-02-15 16:04 - 2014-02-15 16:04 - 00448512___ (OldTimer Tools)
C:\Users\Conjon\Downloads\TFC.exe

2014-02-15 15:47 - 2014-02-15 15:47 - 01166132___ () C:\Users\Conjon\Downloads\AdwCleaner (1).exe
2014-02-15 15:47 - 2014-02-15 15:47 - 01037530___ (Thisisu) C:\Users\Conjon\Downloads\JRT (1).exe
2014-02-15 15:41 - 2014-02-16 23:10 - 000000___D () C:\AdwCleaner
2014-02-15 15:41 - 2014-02-15 15:41 - 01166132___ ()
C:\Users\Conjon\Downloads\AdwCleaner.exe
2014-02-15 15:40 - 2014-02-15 15:40 - 01037530___ (Thisisu) C:\Users\Conjon\Desktop\JRT.exe
2014-02-09 22:56 - 2014-02-09 22:56 - 01854976___ ()
C:\Users\Conjon\Downloads\721019190.pokedex (1).exe
2014-02-09 22:54 - 2014-02-09 22:54 - 01854976___ ()
C:\Users\Conjon\Downloads\721019190.pokedex.exe
2014-02-09 17:16 - 2014-02-15 20:00 - 000000___SHD () C:\Users\Conjon\O178W183c
2014-02-09 17:05 - 2014-02-15 19:52 - 000000___SHD () C:\Users\Conjon\Q719W341f
2014-02-09 17:02 - 2014-02-09 17:02 - 0000001___SH () C:\Users\Conjon\B209T414I.SM2
2014-02-09 16:57 - 2014-02-15 19:52 - 000000___D () C:\Users\Conjon\E945G635u
2014-02-09 10:14 - 2014-02-09 10:14 - 00858284___ ()
C:\Users\Conjon\Downloads\mytv4-0.1.0.crx
2014-02-08 20:30 - 2014-02-08 20:30 - 000000___D ()
C:\Users\Conjon\AppData\Local\F62D595E-F00F-4DAC-839D-BDA813250E1A}
2014-01-21 21:14 - 2014-01-21 21:14 - 000000___D ()
C:\Users\Conjon\AppData\Local\{301BDBA7-9A9F-45E1-8109-3581F5BDFE3A}
2014-02-18 10:28 - 2013-06-28 18:49 - 00000416___ () C:\Windows\Tasks\PC Optimizer Pro64 startups.job
2014-02-16 23:10 - 2013-12-28 14:42 - 000000___D ()
C:\Users\Conjon\AppData\Local\Gvhumedia
2014-02-15 19:53 - 2011-10-23 15:36 - 000000___HD () C:\Windupdt
2014-02-15 15:38 - 2014-01-11 18:22 - 000000___D () C:\Program Files (x86)\AVG SafeGuard toolbar
2014-02-14 13:07 - 2011-07-25 14:24 - 00000404___H () C:\Windows\Tasks\Norton Security Scan for Conjon.job
C:\Users\Conjon\AppData\Roaming\RSBuddy Login.ini
C:\Users\Conjon\Adobe Photoshop CS6 Extended.exe
C:\Users\Conjon\cache.dat
C:\Users\Conjon\jagex_cl_oldschool_LIVE.dat
C:\Users\Conjon\jagex_cl_runescape_LIVE.dat
C:\Users\Conjon\jagex_cl_runescape_LIVE1.dat
C:\Users\Conjon\jagex_cl_runescape_LIVE2.dat
C:\Users\Conjon\jagex_runescape_preferences.dat
C:\Users\Conjon\jagex_runescape_preferences2.dat
C:\Users\Conjon\jagex__preferences3.dat
C:\Users\Conjon\matrix_cl_matrix_LIVE.dat
C:\Users\Conjon\random.dat
C:\Users\Connor\jagex_cl_runescape_LIVE.dat
C:\Users\Public\AlexaNSISPlugin.59284.dll
C:\Users\Conjon\AppData\Local\Temp\hiiim.exe
AlternateDataStreams: C:\Users\Conjon\Downloads\RE how are you.eml:OECustomProperty
MSCONFIG\startupfolder: C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup\McAfee Security Scan Plus.Ink => C:\Windows\pss\McAfee Security Scan Plus.Ink.CommonStartup
MSCONFIG\startupfolder: C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup\Start Activity Monitor Utility.Ink => C:\Windows\pss\Start Activity Monitor Utility.Ink.CommonStartup

MSCORECONFIG\startupreg: Goepuwvuugimr => C:\Users\Conjon\AppData\Roaming\Byevig\dynop.exe
 Task: C:\Windows\Tasks\Security Center Update - 3588189980.job =>
 C:\Users\Conjon\AppData\Roaming\Byevig\dynop.exe
 Task: C:\Windows\Tasks\PC Optimizer Pro64 startups.job => C:\Program Files\PC Optimizer
 Pro\StartApps.exe <==== ATTENTION
 Task: C:\Windows\Tasks\Norton Security Scan for Conjon.job =>
 C:\PROGRA~2\NORTON~2\Engine\351~1.6\Nss.exe
 Task: {BDD1DD8E-AA1C-4616-8B18-D11B38D62C0E} -
 System32\Tasks\RealUpgradeLogonTaskS-1-5-21-49055449-2376379733-193483228-1001 =>
 C:\Program Files (x86)\Real\RealUpgrade\RealUpgrade.exe
 Task: {C115E300-F75A-414B-AC4B-31585DD85AEA} -
 System32\Tasks\RealUpgradeScheduledTaskS-1-5-21-49055449-2376379733-193483228-1001 =>
 C:\Program Files (x86)\Real\RealUpgrade\RealUpgrade.exe
 Task: {C706AA55-8001-4237-9F1E-095BA3F041A7} - \TubeSaver Update No Task File
 Task: {7E02CECC-56C0-4400-8E95-222C148ADAF3} - System32\Tasks\PC Optimizer Pro64
 startups => C:\Program Files\PC Optimizer Pro\StartApps.exe <==== ATTENTION
 Task: {9B5F344B-2D5A-46F4-B9C4-612C923B422E} - System32\Tasks\Norton Security Scan for
 Conjon => C:\Program Files (x86)\Norton Security Scan\Engine\3.5.1.6\Nss.exe [2012-10-03]
 (Symantec Corporation)
 Task: {531FBA95-302F-49CC-A020-16FE72FA11CF} - System32\Tasks\Security Center Update -
 3588189980 => C:\Users\Conjon\AppData\Roaming\Byevig\dynop.exe [2013-12-21] (JenMeramkul
 S.O.L.) <==== ATTENTION
 Task: {21A83543-7C62-49FE-B218-3BD6401E734D} -
 System32\Tasks\ReclaimerResumeInstall_Conjon =>
 C:\Users\Conjon\AppData\Roaming\Real\Update\UpgradeHelper\RealPlayer\10.30\agent\rnupgage
 nt.exe [2013-01-23] (RealNetworks, Inc.)
 Task: {2900CC26-1582-45ED-BE4E-4D6832E29146} - System32\Tasks\BackgroundContainer
 Startup Task => Rundll32.exe
 "C:\Users\Conjon\AppData\Local\Conduit\BackgroundContainer\BackgroundContainer.dll",DllRun

Ensure the file is in the same location as FRST (which is the desktop).

Click the Fix button.

A prompt will let you know the operation has been completed. Click OK.

It will produce a log at the desktop once done.

Copy and paste the content of the log into your next reply.

Step 2

Double-click FRST.exe to run it.

Close all other windows and allow it to run without interruptions.

Run the file. Windows Vista and Windows 7 users should run it as an administrator.

Click Yes to continue.

Wait for its initial task to finish as it is backing up the registry.

Tick the following: Addition

Drivers MD5

Click Scan and wait for it to finish.

It will notify you twice for each log that will pop-up. Click OK for each prompt.

Two log files will be saved on your desktop: FRST.txt

Addition.txt

Copy and paste the contents of both logs into your next reply.

Step 3

Please download Malwarebytes Anti-Rootkit ['here'](#).

Double-click mbar-*.exe to extract the application to your desktop. If a prompt greets you with a warning, click No.

Once the program has loaded, select Next and press Update.

Wait for it to finish downloading. Press Next once done.

Ensure all options are checked. Press the Scan button. If infections are found upon completion of the scan, make sure the Create Restore Point box is checked. Press Cleanup after.

When disinfection is completed, you will be prompted to reboot. Allow it by pressing Yes.

Two logs will be saved inside the mbar folder in your desktop: mbar-log-* (*.txt

system-log.txt

Copy and paste both logs in your next reply.

In your next post, please provide the following:

Farbar Recovery Scan Tool Log(s) FRST Fix Log

FRST.txt

Addition.txt

Malwarebytes Anti-Rootkit Logs

Big Chuck - February 20, 2014, 6:37 pm

Posted these now because rootkit will make me restart comp. Will post those logs upon completion.

Fix Result:

<http://pastebin.com/KYuXkXbF>

FRST Scan:

<http://pastebin.com/0MtAWWCu>

Additon:

<http://pastebin.com/NtadP33x>

System-log

<http://pastebin.com/a5wDyY07>

mbar-log

Malwarebytes Anti-Rootkit BETA 1.07.0.1009

www.malwarebytes.org

Database version: v2014.02.21.09

Windows 7 Service Pack 1 x64 NTFS

Internet Explorer 11.0.9600.16518

Conjon :: CONNOR-PC [administrator]

2/21/2014 10:41:38 AM

mbar-log-2014-02-21 (10-41-38).txt

Scan type: Quick scan

Scan options enabled: Anti-Rootkit | Drivers | MBR | Physical Sectors | Memory | Startup | Registry |

File System | Heuristics/Extra | Heuristics/Shuriken

Scan options disabled:

Objects scanned: 55741

Time elapsed: 46 minute(s), 10 second(s) [aborted]

Memory Processes Detected: 2

C:\Users\Conjon\AppData\Roaming\Byevig\dynop.exe (Trojan.Zbot.FBD) -> 3624 -> Delete on reboot.

C:\Users\Conjon\AppData\Roaming\Byevig\dynop.exe (Trojan.Zbot.FBD) -> 3288 -> Delete on reboot.

Memory Modules Detected: 0
(No malicious items detected)

Registry Keys Detected: 0
(No malicious items detected)

Registry Values Detected: 2
HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\Goepuwvuugimr (Trojan.Zbot.FBD) -> Data: C:\Users\Conjon\AppData\Roaming\Byevig\dynop.exe -> Delete on reboot.
HKCU\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Run\Goepuwvuugimr (Trojan.Zbot.FBD) -> Data: C:\Users\Conjon\AppData\Roaming\Byevig\dynop.exe -> Delete on reboot.

Registry Data Items Detected: 0
(No malicious items detected)

Folders Detected: 0
(No malicious items detected)

Files Detected: 1
C:\Users\Conjon\AppData\Roaming\Byevig\dynop.exe (Trojan.Zbot.FBD) -> Delete on reboot.

Physical Sectors Detected: 0
(No malicious items detected)

(end)

Paradoxum - February 23, 2014, 6:54 am

Step 1

Please download RogueKiller from one of the following links and save it to your desktop.

['32-bit'](#)

['64-bit'](#)

Make sure all other windows are closed and to let it run uninterrupted.

Run the file. Windows Vista and Windows 7 users should run it as an administrator.

Wait for its initial scan to finish. Accept RogueKiller's EULA.

Click Scan. It will say "Scan Finished" once done.

Click Report and copy and paste the contents of the log into your next reply. A log file will be saved on your desktop as well.

Close the program. Click Yes.

Note: If the program is blocked, do not hesitate to try several times. Should you fail (it may happen), rename it to winlogon.exe.

Step 2

Run OTL.exe.

Copy and paste what is inside the quote box below into OTL's Custom Scans & Fixes box at the bottom.

```
Quote:CREATERESTOREPOINT
netsvcs
BASESERVICES
%SYSTEMDRIVE%\*.exe
dir "%systemdrive%\*" /S /A:L /C
/md5start
services.*
explorer.exe
Userinit.exe
svchost.exe
/md5stop
```

Click the button at the top.

A log will pop-up shortly. Post that log.

In your next post, please provide the following:

OTL Log(s)OTL.txt

RogueKiller Log

Big Chuck - February 23, 2014, 7:05 am

Th problem is gone! No more dynop in task manager or anything and comp runs fast. Do you still want these logs? Thanks!

Paradoxum - February 23, 2014, 7:06 am

I am aware. I'll need further scans to ensure nothing is left. ?