

Forum:[Hack Forums](#)

Thread: [This person is viewing what i type on youtube, and possibly everything i type.](#)

CheeChee - October 11, 2010, 11:01 am

There should be no RAT, i just formatted.

The person is likely on my network.

The person says he got through using my telephone connection.

This person is my cousin's friend btw.

The person has access to my ports. How is he doing this?

Like when i type something into the search box of youtube or facebook, then can see exactly what i type which goes to their cellphone.

Could anyone tell me how they are doing this?

By the way, they can change the ads, profile photos, and videos around, and pause my videos on youtube and facebook. I'm not kidding - everytime i refresh the page, saying something, they reply like that with a message for example in the ads and what not.

The Hellblazer - October 11, 2010, 11:20 am

Umm man...I think you got RAT'ed ...Please submit an HJT log, and visit the White Hat section. They will fix your problem 100% !

Excalibur - October 11, 2010, 11:21 am

you probably got ratted by a driveby or thru a vulnerable open network...

post Hijackthis log in whithat section and look up on network security

flAmingw0rm - October 11, 2010, 11:23 am

What is your Operating System? There are exploits which can download and execute a file on your computer just by knowing your IP.

Grumpy - October 11, 2010, 11:24 am

Get a post made in the Whitehat Help Section. Looks like you've been infected through a driveby.

The Janitor - October 11, 2010, 11:25 am

Hey there,

I will help you fixing your problem, if i am not able to, i will call someone who is more experienced,

Before doing anything please begin with this:

Are you having any of these symptoms?Unexplainable deletion of files.

Unexplainable editing of files.

CD Tray opening and closing, though not provoked.

Webcam randomly turning on.

Keylogging.

Cursor moving freely.

Blocked access to particular sites (usually security-based websites).

Random messages appearing.

Unknown files/documents being created.

Slow Internet speeds.

Unresponsive components (monitors being disabled).

Passwords being changed.

HOSTS File being changed.

Please post,

Also please do the following:Open CMD As administrator

Type Netstat-b

Look for any Unknown Connections

If any found look what program uses them

If not sure post a screenshot by uploading it on www.imageshack.us

Also, it could be that you are on the same network, you can possibly be more-secured by doing the following:Download [Comodo Firewall](#)

Install, Update

Look for any Outgoing connections, If unsafe Firewall will block

After doing this do the following:Boot into safe mode by restarting your Computer and continiously pressing f8

When entering the boot Menu, navigate to Safe Mode with Networking with the arrow keys.

Dont be affraid when you see a list of files being named, this is normal

After being in safe mode with networking

Download [Malwarebytes Anti-Malware](#) , Install it, update, and run a full scan, This might take over 3 hours.

Delete any infections found

Scan your computer with an Up-To-Date Anti virus, if you don't have one, i suggest one of these : [Avira Antivir](#) Or [Avast Antivirus](#)

-

Update, Run a full scan delete any infections found,

Now to triple check it, please download and install [Eset Online-Scanner](#)

Delete any infections found.

After this, your PC Should be clean,

If you encounter any problems after this, Please run an Optional scan with: [SuperAntiSpyware](#)

Update it, run a full scan delete any infections found.

If you still are encountering troubles, please post and i will help you further.

kind regards

Gtaclck

Likealot - October 11, 2010, 12:27 pm

Sorry the other account is locked out or something.

Windows 7 is my operating system. @ above post, thanks but i tried this before, they are somehow connecting to me directly. They are most likely administrating my network or something like that because sometimes they restrict my access to some sites.

Hano - October 11, 2010, 12:28 pm

(Oct 11, 2010 12:27 PM)Likealot Wrote: [\[CITE\]](#) Sorry the other account is locked out or something.

Windows 7 is my operating system. @ above post, thanks but i tried this before, they are somehow connecting to me directly. They are most likely administrating my network or something like that because sometimes they restrict my access to some sites. Then it was not by ip. Probably some Drive-by site.

MikeMz - October 11, 2010, 12:55 pm

You're on a Rat. Submit a HiJackThis log at the White Hat help section.

Dr. A. NonyMouse - October 11, 2010, 1:00 pm

Perhaps if someone could get physical access to the PC then they could add a small chip to it so no matter how many times you reformat or delete it it will reinstall itself.

Fetus Flipper - October 11, 2010, 1:29 pm

Check if you have a port that is open. If you do, he could be exploiting you through it.

Braco Asshole - October 11, 2010, 2:21 pm

Maybe you are rat'd. Submit a HiJackThis log i am 1000% sure that the problem will be fixed if you do it.

playgrounds - October 11, 2010, 2:27 pm

I mean Jeez , Haven't You guys Said submit enough already ,

as you know you should Download Trend micro Hijackthis And Run a scan and post your log in the white hat Section

Then Wait For a HJT member To Server You.

CheeChee - October 11, 2010, 4:19 pm

Spoiler ([Click to View](#))

Logfile of Trend Micro HijackThis v2.0.4
Scan saved at 7:16:32 PM, on 10/11/2010
Platform: Windows 7 (WinNT 6.00.3504)
MSIE: Internet Explorer v9.00 (9.00.7930.16406)
Boot mode: Normal

Running processes:

C:\Windows\system32\taskhost.exe
C:\Windows\system32\Dwm.exe
C:\Windows\Explorer.EXE
C:\Program Files\Agnitum\Outpost Firewall Pro\op_mon.exe
C:\Windows\system32\taskhost.exe
C:\Windows\system32\taskmgr.exe
C:\Program Files\Trend Micro\HiJackThis\HiJackThis.exe
C:\Users\Sujee\AppData\Local\Google\Chrome\Application\chrome.exe
C:\Users\Sujee\AppData\Local\Google\Chrome\Application\chrome.exe
C:\Windows\system32\DllHost.exe

R1 - HKLM\Software\Microsoft\Internet Explorer\Main,Default_Page_URL =
<http://go.microsoft.com/fwlink/?LinkId=69157>

R1 - HKLM\Software\Microsoft\Internet Explorer\Main,Default_Search_URL =
<http://go.microsoft.com/fwlink/?LinkId=54896>

R1 - HKLM\Software\Microsoft\Internet Explorer\Main,Search Page =
<http://go.microsoft.com/fwlink/?LinkId=54896>

R0 - HKLM\Software\Microsoft\Internet Explorer\Main,Start Page =
<http://go.microsoft.com/fwlink/?LinkId=69157>

R0 - HKLM\Software\Microsoft\Internet Explorer\Search,SearchAssistant =

R0 - HKLM\Software\Microsoft\Internet Explorer\Search,CustomizeSearch =

O2 - BHO: Adobe PDF Reader Link Helper - {06849E9F-C8D7-4D59-B87D-784B7D6BE0B3} -
C:\Program Files\Common Files\Adobe\Acrobat\ActiveX\AcroIEHelper.dll

O2 - BHO: Windows Live ID Sign-in Helper - {9030D464-4C02-4ABF-8ECC-5164760863C6} -
C:\Program Files\Common Files\Microsoft Shared\Windows Live\WindowsLiveLogin.dll

O2 - BHO: Google Toolbar Helper - {AA58ED58-01DD-4d91-8333-CF10577473F7} - C:\Program
Files\Google\Google Toolbar\GoogleToolbar_32.dll

O2 - BHO: Adobe PDF Conversion Toolbar Helper - {AE7CD045-E861-484f-8273-0445EE161910}
- C:\Program Files\Adobe\Acrobat 8.0\Acrobat\AcroIEFavClient.dll

O2 - BHO: Google Toolbar Notifier BHO - {AF69DE43-7D58-4638-B6FA-CE66B5AD205D} - C:\Program Files\Google\GoogleToolbarNotifier\5.5.5126.1836\swg.dll

O2 - BHO: Ask Toolbar BHO - {D4027C7F-154A-4066-A1AD-4243D8127440} - C:\Program Files\Ask.com\GenericAskToolbar.dll

O3 - Toolbar: Google Toolbar - {2318C2B1-4965-11d4-9B18-009027A5CD4F} - C:\Program Files\Google\Google Toolbar\GoogleToolbar_32.dll

O3 - Toolbar: Adobe PDF - {47833539-D0C5-4125-9FA8-0819E2EAAAC93} - C:\Program Files\Adobe\Acrobat 8.0\Acrobat\AcroIEFavClient.dll

O3 - Toolbar: Ask Toolbar - {D4027C7F-154A-4066-A1AD-4243D8127440} - C:\Program Files\Ask.com\GenericAskToolbar.dll

O4 - HKLM\..\Run: [OrderReminder] C:\Program Files\Hewlett-Packard\OrderReminder\OrderReminder.exe

O4 - HKLM\..\Run: [Acrobat Assistant 8.0] "C:\Program Files\Adobe\Acrobat 8.0\Acrobat\Acrotray.exe"

O4 - HKLM\..\Run: [igfxtray] C:\Windows\system32\igfxtray.exe

O4 - HKLM\..\Run: [igfxhkcmd] C:\Windows\system32\hkcmd.exe

O4 - HKLM\..\Run: [igfxpers] C:\Windows\system32\igfxpers.exe

O4 - HKLM\..\Run: [VirtualCloneDrive] "C:\Program Files\Elaborate Bytes\VirtualCloneDrive\VCDDaemon.exe" /s

O4 - HKLM\..\Run: [Smapp] C:\Program Files\Analog Devices\SoundMAX\SMTray.exe

O4 - HKLM\..\Run: [DrvLsnr] C:\Program Files\Analog Devices\SoundMAX\DrvLsnr.exe

O4 - HKLM\..\Run: [Malwarebytes' Anti-Malware] "C:\Program Files\Malwarebytes' Anti-Malware\mbamgui.exe" /starttray

O4 - HKLM\..\Run: [OutpostMonitor] "C:\PROGRA~1\Agnitum\OUTPOS~1\op_mon.exe" /tray /noservice

O4 - HKLM\..\Run: [OutpostFeedBack] "C:\Program Files\Agnitum\Outpost Firewall Pro\feedback.exe" /dump:os_startup

O4 - HKUS\S-1-5-19\..\Run: [Sidebar] %ProgramFiles%\Windows Sidebar\Sidebar.exe /autoRun (User 'LOCAL SERVICE')

O4 - HKUS\S-1-5-19\..\RunOnce: [mctadmin] C:\Windows\System32\mctadmin.exe (User 'LOCAL SERVICE')

O4 - HKUS\S-1-5-20\..\Run: [Sidebar] %ProgramFiles%\Windows Sidebar\Sidebar.exe /autoRun (User 'NETWORK SERVICE')

O4 - HKUS\S-1-5-20\..\RunOnce: [mctadmin] C:\Windows\System32\mctadmin.exe (User 'NETWORK SERVICE')

O9 - Extra button: Research - {92780B25-18CC-41C8-B9BE-3C9C571A8263} - C:\PROGRA~1\MICROS~2\Office12\REFIEBAR.DLL

O9 - Extra button: Encarta Search Bar - {B205A35E-1FC4-4CE3-818B-899DBBB3388C} - C:\Program Files\Common Files\Microsoft Shared\Encarta Search Bar\ENCSBAR.DLL

O9 - Extra button: Messenger - {FB5F1910-F110-11d2-BB9E-00C04F795683} - C:\Program Files\Messenger\MSMSG.S.EXE

O9 - Extra 'Tools' menuitem: Messenger - {FB5F1910-F110-11d2-BB9E-00C04F795683} - C:\Program Files\Messenger\MSMSG.S.EXE

O10 - Unknown file in Winsock LSP: c:\program files\common files\microsoft shared\windows live\wlidnsp.dll

O10 - Unknown file in Winsock LSP: c:\program files\common files\microsoft shared\windows live\wlidnsp.dll

O11 - Options group: [ACCELERATED_GRAPHICS] Accelerated graphics

O16 - DPF: {E2883E8F-472F-4FB0-9522-AC9BF37916A7} - <http://platformdl.adobe.com/NOS/getPlusPlus/1.6/gp.cab>

O20 - Applnit_DLLs: c:\progra~1\agnitum\outpos~1\wl_hook.dll

O23 - Service: Agnitum Client Security Service (acssrv) - Agnitum Ltd. - C:\PROGRA~1\Agnitum\OUTPOS~1\acs.exe

O23 - Service: FLEXnet Licensing Service - Macrovision Europe Ltd. - C:\Program Files\Common Files\Macrovision Shared\FLEXnet Publisher\FNPLicensingService.exe

O23 - Service: Google Update Service (gupdate) (gupdate) - Google Inc. - C:\Program Files\Google\Update\GoogleUpdate.exe

O23 - Service: Google Software Updater (gusvc) - Google - C:\Program Files\Google\Common\Google Updater\GoogleUpdaterService.exe

O23 - Service: MBAMService - Malwarebytes Corporation - C:\Program Files\Malwarebytes' Anti-Malware\mbamservice.exe

O23 - Service: SoundMAX Agent Service (SoundMAX Agent Service (default)) - Analog Devices, Inc. - C:\Program Files\Analog Devices\SoundMAX\SMAgent.exe

--

End of file - 5709 bytes

Someone help me post this in white hat section. I'm having trouble accessing it MY SQL errors.

Epidemic - October 11, 2010, 5:57 pm

1st of All lets get to this:

1. This is the wrong section, should be in the Whitehat section
2. If its your cousins friend why don't you ask him to stop?

Okay now that that's out of the way lets move on.

Boot into 'Safe Mode With Networking' by restarting your PC And continiously pressing F8 and selecting it from the menu.

Download [MalwareBytes Anti-Malware](#)

Update it and run a FULL scan (Not a Quick scan): it may take over 3 hours, please let it run unhindered.

Delete any infections found.

Scan your PC With [ESET Online Scanner](#). Make sure 'Remove found threads' has been checked.

After that is done, please do this:

Please run a free online scan with ESET Online Scanner by downloading it from ['here'](#) and save it to your Desktop. Please ensure that you're logged into an Administrator account before running the scanner. The ESET Online Scanner will not work if you're on a limited account.

Double-click esetsmartinstaller_enu.exe to execute the program.

Check the box next to 'YES, I accept the Terms of Use'. Press 'Start'.

If this is your first time installing the scanner, allow the ActiveX Control to install.

Database download may take some time.

On the next page, ensure the box next to 'Remove found threads' has been checked. Also ensure that the box next to 'Scan unwanted applications' is checked. Proceed by clicking on 'Start'. The ESET Online Scanner will update the Virus Signature Database and begin the scan.

Please allow it to complete successfully and ensure that any current downloads are stopped.

Once the scan's completed, please open 'Notepad' by navigating to 'Start', then 'Run', and type in 'Notepad'. Open the file located at 'C:\Program Files\ESET\ESET Online Scanner\log.txt'.

Please Copy & Paste this log into your next reply.

Press 'Finish'.

Make sure this is moved to the White hat section. For further inspection.