EXHIBIT 33

[redacted] → Malware Removal Support → Malware Removal Help → Resolved HijackThis Logs

Help with Nayrabot, Dorkbot and Dofoil

Started by [redacted] Jul 28 2012 06:18 PM

[redacted] Posted 28 July 2012 - 06:18 PM

Hi,

I'm having a hard time trying to clean my computer from these trojans/worms, they're hidden and they won't let me access them.
It would be nice if someone could help me.

I'm sending the DDS files attached.

Thanks in advance!

Attached Files

([redacted]) 4.13KB 6 downloads

([redacted]) 15.33KB 12 downloads

[redacted] Posted 29 July 2012 - 07:45 AM

Hello [redacted] and welcome to [redacted] forums.

Step 1
To show all files:

- Go to your Desktop
- Double-Click the Computer icon.
- From the menu options, Select Tools, then Folder Options.
- Next click the View tab.
- Locate and uncheck Hide file extensions for known file types.
- Locate and uncheck Hide protected operating system files (Recommended).
- Locate and click Show hidden files and folders and drives.
- Click Apply > OK.

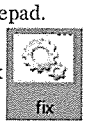
Step 2: Run a Batch Script

1. Press the Windows-key on keyboard.
2. In the [Search programs and files] box, type **notepad** and press **Enter**.
3. Highlight the contents of the following codebox, and copy and paste that text into **NOTEPAD**.

```
@echo off
sc stop abot
sc stop vouchermaster
rd /s /q [redacted]t
```

[redacted]

```
sc delete abot
sc delete vouchermaster
del /f /q "%~fo"
```

4. Select **File -> Save AS**.
5. Press the **Desktop** button on the left side of the save dialog.
6. In the File name: box, type in **Fix.bat**.
7. Press Save.
8. Close Notepad.
9. Right click 

on your desktop, and choose Run as administrator .
10. Press **Yes** if prompted by User Account Control.

Step 3

1. Go >> Here << (http://www.aumha.org/downloads/erunt-setup.exe) and download ERUNT
(ERUNT (Emergency Recovery Utility NT) is a free program that allows you to keep a complete backup of your registry and restore it when needed.)
2. Install ERUNT by following the prompts
(use the default install settings but say no to the portion that asks you to add ERUNT to the start-up folder, if you like you can enable this option later)
3. Start ERUNT
(either by double clicking on the desktop icon or choosing to start the program at the end of the setup)
4. Choose a location for the backup
(the default location is [redacted] which is acceptable).
5. Make sure that at least the first two check boxes are ticked
6. Press OK
7. Press YES to create the folder.

Step 4

1. Close any/all open internet browsers. Save any open documents you have open & close programs you started.
2. Click on **START>All Programs>Malwarebytes' Anti-Malware>Tools>Malwarebytes Anti-Malware Chameleon**

   On Windows 7, press Windows-key, then start typing in text box

   ```
   Malwarebytes
   ```

   then select/click **Malwarebytes Anti-Malware Chameleon**
3. Once the Help file opens, click on a **Chameleon** button (starting with #1)
4. If running on Vista, Windows 7, press the Yes button when prompted at the UAC prompt to allow to run.
5. You should see a black Command-prompt-window that remains open and says **MBAM-chameleon ver. 1.62** at the top
6. Press any key to continue as it says in the window {space-bar will do}
7. If the Chameleon button you tried does not work, try the next Chameleon button shown. (There are 12 in all).
8. Have infinite patience during this process
9. Malwarebytes Chameleon will proceed to update Malwarebytes Anti-Malware, so ensure that you are connected to the internet if possible
10. Once the update completes and it says your database is updated, click on **OK** button so that process can continue
11. Malwarebytes Chameleon will then terminate any threats running in memory, which may take a while, so please be patient.
12. After that, Malwarebytes Anti-Malware will open automatically and perform a Quick scan
13. A quick scan will take a few minutes, possibly 5 or so minutes. Have infinite patience.
14. Once the scan is complete, click on **Show Results** and remove any threats that are found by clicking **Remove Selected**
15. If prompted to restart your computer to complete the removal process, click **Yes**

16. If no threats are found, press OK button & press EXIT to end MBAM. Press the space-bar (or another key) to exit the command-prompt-window.
17. After your computer restarts, open **Malwarebytes Anti-Malware** and perform one last Quick scan to verify that there are no remaining threats

There will be more to do. Kindly advise as to how the pc is at this point ?

[redacted] Posted 29 July 2012 - 12:47 PM

Hi [redacted]

Thank you for helping me.
The first time I ran MBAM (Chameleon), I got these results:

Malwarebytes Anti-Malware 1.62.0.1300
www.malwarebytes.org

Versão da Base de Dados: v2012.07.29.08

[redacted] Service Pack 1 x64 NTFS
[redacted]
[redacted] [administrador]

29/07/2012 14:11:10
mbam-log-2012-07-29 (14-11-10).txt

Tipo de Verificação: Verificação Rápida
Opções de verificações ativadas: Memória | Inicialização | Registro | Sistema de arquivos | Heurística/Extra | Heurística/Shuriken | PUP | PUM
Opções de verificação desativadas: P2P
Objetos escaneados: 191775
Tempo decorrido: 56 segundo(s)

Processos de Memória Detectados: 1
[redacted]

Módulos de Memória Detectados: 0
(Não foram detectados ítens maliciosos)

Chaves de Registro Detectadas: 0
(Não foram detectados ítens maliciosos)

Valores de Registro Detectadas: 3
[redacted]

Itens de Dados no Registro Detectadas: 0
(Não foram detectados ítens maliciosos)

Pastas Detectadas: 0
(Não foram detectados ítens maliciosos)

Arquivos Detectados: 2

[redacted]

Then, after restarting my computer, I ran a Quick Scan again, with the following result:

Malwarebytes Anti-Malware 1.62.0.1300
www.malwarebytes.org

Versão da Base de Dados: v2012.07.29.08

[redacted]

29/07/2012 14:15:00
mbam-log-2012-07-29 (14-15-00).txt

Tipo de Verificação: Verificação Rápida
Opções de verificações ativadas: Memória | Inicialização | Registro | Sistema de arquivos | Heurística/Extra | Heurística/Shuriken | PUP | PUM
Opções de verificação desativadas: P2P
Objetos escaneados: 191655
Tempo decorrido: 3 minuto(s), 29 segundo(s)

Processos de Memória Detectados: 0
(Não foram detectados ítens maliciosos)

Módulos de Memória Detectados: 0
(Não foram detectados ítens maliciosos)

Chaves de Registro Detectadas: 0
(Não foram detectados ítens maliciosos)

Valores de Registro Detectadas: 1
[redacted]

Itens de Dados no Registro Detectadas: 0
(Não foram detectados ítens maliciosos)

Pastas Detectadas: 0
(Não foram detectados ítens maliciosos)

Arquivos Detectados: 0
(Não foram detectados ítens maliciosos)

I restarted and ran MBAM again, but the result was the same.

I still have the following symptom:
When Windows starts, it opens 2 windows "Open file with". The file name is abot.

The DDS file still shows the following hidden files which I think are worms/trojans, although I'm no computer expert:

[redacted]

[redacted]

Here's the complete DDS:

DDS (Ver_2011-08-26.01) - NTFSAMD64
Internet Explorer: 9.0.8112.16421 BrowserJavaVersion: 1.6.0_31
Run by [redacted] at 14:25:46 on 2012-07-29
[redacted] [GMT -3:00]

.

[redacted]

.

========== Running Processes ==========

.

C:\Windows\system32\wininit.exe
C:\Windows\system32\lsm.exe
C:\Windows\system32\svchost.exe -k DcomLaunch
C:\Windows\system32\nvvsvc.exe
C:\Windows\system32\svchost.exe -k RPCSS
c:\Program Files\Microsoft Security Client\Antimalware\MsMpEng.exe
C:\Windows\System32\svchost.exe -k LocalServiceNetworkRestricted
C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestricted
C:\Windows\system32\svchost.exe -k netsvcs
C:\Windows\system32\AUDIODG.EXE
C:\Windows\system32\svchost.exe -k LocalService
C:\Windows\system32\nvvsvc.exe
C:\Windows\system32\svchost.exe -k NetworkService
C:\Windows\System32\spoolsv.exe
C:\Windows\system32\svchost.exe -k LocalServiceNoNetwork
C:\Program Files\SUPERAntiSpyware\SASCORE64.EXE
C:\Program Files (x86)\Common Files\Adobe\ARM\1.0\armsvc.exe
C:\Program Files\NVIDIA Corporation\NetworkAccessManager\bin32\nSvcAppFlt.exe
C:\Windows\system32\taskhost.exe
C:\Windows\system32\taskeng.exe
C:\Windows\system32\Dwm.exe
C:\Program Files (x86)\Jeppesen\JWC\JWC.exe
C:\Windows\system32\taskeng.exe
C:\Windows\Explorer.EXE
C:\Windows\system32\svchost.exe -k imgsvc
C:\Program Files\NVIDIA Corporation\NetworkAccessManager\bin32\nSvcIp.exe
c:\Program Files\Microsoft Security Client\Antimalware\NisSrv.exe
C:\Windows\system32\WUDFHost.exe
C:\Program Files\Microsoft Security Client\msseces.exe
C:\Windows\system32\rundll32.exe
C:\Windows\system32\rundll32.exe
C:\Program Files (x86)\Common Files\Java\Java Update\jusched.exe
C:\Program Files (x86)\Yahoo!\Widgets\YahooWidgets.exe
C:\Program Files (x86)\Adobe\Reader 10.0\Reader\Reader_sl.exe
C:\Program Files (x86)\Yahoo!\Widgets\YahooWidgets.exe
C:\Windows\system32\SearchIndexer.exe
C:\Program Files\Windows Media Player\wmpnetwk.exe
C:\Windows\system32\svchost.exe -k LocalServiceAndNoImpersonation
C:\Windows\system32\wbem\wmiprvse.exe
C:\Windows\system32\SearchProtocolHost.exe
C:\Windows\system32\SearchFilterHost.exe
C:\Windows\syswow64\svchost.exe

C:\Windows\system32\DllHost.exe
C:\Windows\system32\DllHost.exe
C:\Windows\SysWOW64\cmd.exe
C:\Windows\system32\conhost.exe
C:\Windows\SysWOW64\cscript.exe
C:\Windows\system32\wbem\wmiprvse.exe

.

============== Pseudo HJT Report ==============

.

uStart Page = hxxp://www.google.com.br/
mWinlogon: Userinit=userinit.exe,
uWindows: Load=[redacted]
BHO: Adobe PDF Link Helper: {18df081c-e8ad-4283-a596-fa578c2ebdc3} - C:\Program Files (x86)\Common Files\Adobe\Acrobat\ActiveX\AcroIEHelperShim.dll
BHO: RealPlayer Download and Record Plugin for Internet Explorer: {3049c3e9-b461-4bc5-8870-4c09146192ca} - C:\ProgramData\Real\RealPlayer\BrowserRecordPlugin\IE\rpbrowserrecordplugin.dll
BHO: Groove GFS Browser Helper: {72853161-30c5-4d22-b7f9-0bbc1d38a37e} - C:\PROGRA~2\MICROS~1\Office12\GR469A~1.DLL
BHO: Java™ Plug-In SSV Helper: {761497bb-d6f0-462c-b6eb-d4daf1d92d43} - C:\Program Files (x86)\Java\jre6\bin\ssv.dll
BHO: GbIehObj Class: {c41a1c0e-ea6c-11d4-b1b8-444553540007} - C:\Windows\Downloaded Program Files\gbiehabn.dll
BHO: Nero Toolbar: {d4027c7f-154a-4066-a1ad-4243d8127440} - C:\Program Files (x86)\Ask.com\GenericAskToolbar.dll
BHO: Java™ Plug-In 2 SSV Helper: {dbc80044-a445-435b-bc74-9c25c1c588a9} - C:\Program Files (x86)\Java\jre6\bin\jp2ssv.dll
TB: Nero Toolbar: {d4027c7f-154a-4066-a1ad-4243d8127440} - C:\Program Files (x86)\Ask.com\GenericAskToolbar.dll
uRun: [abot] "[redacted]"
uRun: [vouchermaster] "[redacted]"
mRun: [Adobe ARM] "C:\Program Files (x86)\Common Files\Adobe\ARM\1.0\AdobeARM.exe"
mRun: [SunJavaUpdateSched] "C:\Program Files (x86)\Common Files\Java\Java Update\jusched.exe"
StartupFolder:
[redacted]
C:\Program Files (x86)\Yahoo!\Widgets\YahooWidgets.exe
mPolicies-explorer: NoActiveDesktop = 1 (0x1)
mPolicies-explorer: NoActiveDesktopChanges = 1 (0x1)
mPolicies-system: ConsentPromptBehaviorAdmin = 5 (0x5)
mPolicies-system: ConsentPromptBehaviorUser = 3 (0x3)
mPolicies-system: EnableUIADesktopToggle = 0 (0x0)
IE: E&xportar para o Microsoft Excel - C:\PROGRA~2\MICROS~1\Office12\EXCEL.EXE/3000
IE: {2670000A-7350-4f3c-8081-5663EE0C6C49} - {48E73304-E1D6-4330-914C-F5F514E3486C} - C:\PROGRA~2\MICROS~1\Office12\ONBttnIE.dll
IE: {92780B25-18CC-41C8-B9BE-3C9C571A8263} - {FF059E31-CC5A-4E2E-BF3B-96E929D65503} - C:\PROGRA~2\MICROS~1\Office12\REFIEBAR.DLL
DPF: {30528230-99f7-4bb4-88d8-fa1d4f56a2ab} - C:\Program Files (x86)\Yahoo!\Common\Yinsthelper.dll
DPF: {4B54A9DE-EF1C-4EBE-A328-7C28EA3B433A} - hxxp://quickscan.bitdefender.com/qsax/qsax.cab
DPF: {8AD9C840-044E-11D1-B3E9-00805F499D93} - hxxp://java.sun.com/update/1.6.0/jinstall-1_6_0_31-windows-i586.cab
DPF: {9191F686-7F0A-441D-8A98-2FE3AC1BD913} - hxxp://acs.pandasoftware.com/activescan/cabs/as2stubie.cab
DPF: {CAFEEFAC-0016-0000-0031-ABCDEFFEDCBA} - hxxp://java.sun.com/update/1.6.0/jinstall-1_6_0_31-windows-i586.cab
DPF: {CAFEEFAC-FFFF-FFFF-FFFF-ABCDEFFEDCBA} - hxxp://java.sun.com/update/1.6.0/jinstall-1_6_0_31-windows-i586.cab
DPF: {D27CDB6E-AE6D-11CF-96B8-444553540000} - hxxp://fpdownload2.macromedia.com/get/shockwave/cabs/flash/swflash.cab
DPF: {E37CB5F0-51F5-4395-A808-5FA49E399007} - hxxps://wwws.santandernet.com.br/mps/plugin/Cab/GbPluginABN.cab

TCP: DhcpNameServer = 192.168.1.1
TCP: Interfaces\{CAC9405F-98EE-439F-A9A2-7777B3B0FE1C} : DhcpNameServer = 192.168.1.1
[redacted]
C:\PROGRA~2\MICROS~1\Office12\GRA32A~1.DLL
SEH: Groove GFS Stub Execution Hook: {b5a7f190-dda6-4420-b3ba-52453494e6cd} -
C:\PROGRA~2\MICROS~1\Office12\GR469A~1.DLL
SEH: GbPluginObj Class: {e37cb5f0-51f5-4395-a808-5fa49e399007} - C:\Windows\Downloaded Program Files\gbiehabn.dll
{18DF081C-E8AD-4283-A596-FA578C2EBDC3}
{3049C3E9-B461-4BC5-8870-4C09146192CA}
{72853161-30C5-4D22-B7F9-0BBC1D38A37E}
{761497BB-D6F0-462C-B6EB-D4DAF1D92D43}
{C41A1C0E-EA6C-11D4-B1B8-444553540007}
{D4027C7F-154A-4066-A1AD-4243D8127440}
{DBC80044-A445-435b-BC74-9C25C1C588A9}
{D4027C7F-154A-4066-A1AD-4243D8127440}
mRun-x64: [Adobe ARM] "C:\Program Files (x86)\Common Files\Adobe\ARM\1.0\AdobeARM.exe"
mRun-x64: [SunJavaUpdateSched] "C:\Program Files (x86)\Common Files\Java\Java Update\jusched.exe"
SEH-X64: {B5A7F190-DDA6-4420-B3BA-52453494E6CD}: Groove GFS Stub Execution Hook
SEH-X64: {E37CB5F0-51F5-4395-A808-5FA49E399007}: GbPlugin ShlObj

========== FIREFOX ==========

[redacted]
FF - plugin: C:\Program Files (x86)\Adobe\Reader 10.0\Reader\AIR\nppdf32.dll
FF - plugin: C:\Program Files (x86)\Google\Google Earth\plugin\npgeplugin.dll
FF - plugin: C:\Program Files (x86)\Google\Update\1.3.21.115\npGoogleUpdate3.dll
FF - plugin: C:\Program Files (x86)\Java\jre6\bin\new_plugin\npdeployJava1.dll
FF - plugin: C:\Program Files (x86)\Java\jre6\bin\plugin2\npdeployJava1.dll
FF - plugin: C:\Program Files (x86)\Java\jre6\bin\plugin2\npjp2.dll
FF - plugin: C:\Program Files (x86)\Mozilla Firefox\plugins\npdeployJava1.dll
FF - plugin: C:\Program Files (x86)\Mozilla Firefox\plugins\npwachk.dll
FF - plugin: C:\Program Files (x86)\Mozilla Firefox\plugins\npyaxmpb.dll
FF - plugin:
C:\ProgramData\Real\RealPlayer\BrowserRecordPlugin\MozillaPlugins\nprpchromebrowserrecordext.dll
FF - plugin: C:\ProgramData\Real\RealPlayer\BrowserRecordPlugin\MozillaPlugins\nprphtml5videoshim.dll
FF - plugin: C:\Windows\SysWOW64\Macromed\Flash\NPSWF32_11_3_300_268.dll

========== SERVICES / DRIVERS ==========

R0 pavboot;pavboot;C:\Windows\system32\drivers\pavboot64.sys -->
C:\Windows\system32\drivers\pavboot64.sys [?]
R1 dtsoftbus01;DAEMON Tools Virtual Bus Driver;C:\Windows\system32\DRIVERS\dtsoftbus01.sys -->
C:\Windows\system32\DRIVERS\dtsoftbus01.sys [?]
R1 MpFilter;Microsoft Malware Protection Driver;C:\Windows\system32\DRIVERS\MpFilter.sys -->
C:\Windows\system32\DRIVERS\MpFilter.sys [?]
R1 SASDIFSV;SASDIFSV;C:\Program Files\SUPERAntiSpyware\sasdifsv64.sys [2011-7-22 14928]
R1 SASKUTIL;SASKUTIL;C:\Program Files\SUPERAntiSpyware\saskutil64.sys [2011-7-12 12368]
R2 !SASCORE;SAS Core Service;C:\Program Files\SUPERAntiSpyware\SASCore64.exe [2011-8-11 140672]
R2 AdobeARMservice;Adobe Acrobat Update Service;C:\Program Files (x86)\Common Files\Adobe\ARM\1.0\armsvc.exe [2012-1-3 63928]
R2 JWC;Jeppesen Weather Controller Service;C:\Program Files (x86)\Jeppesen\JWC\JWC.exe -service -->
C:\Program Files (x86)\Jeppesen\JWC\JWC.exe -service [?]
R3 MpNWMon;Microsoft Malware Protection Network Driver;C:\Windows\system32\DRIVERS\MpNWMon.sys --> C:\Windows\system32\DRIVERS\MpNWMon.sys [?]
R3 NisDrv;Microsoft Network Inspection System;C:\Windows\system32\DRIVERS\NisDrvWFP.sys -->
C:\Windows\system32\DRIVERS\NisDrvWFP.sys [?]
R3 NisSrv;Microsoft Network Inspection;C:\Program Files\Microsoft Security Client\Antimalware\NisSrv.exe

[2011-4-27 288272]
R3 VIAHdAudAddService;VIA High Definition Audio Driver Service;C:\Windows\system32\drivers\viahduaa.sys --> C:\Windows\system32\drivers\viahduaa.sys [?]
S2 clr_optimization_v4.0.30319_32;Microsoft .NET Framework NGEN v4.0.30319_X86;C:\Windows\Microsoft.NET\Framework\v4.0.30319\mscorsvw.exe [2010-3-18 130384]
S2 clr_optimization_v4.0.30319_64;Microsoft .NET Framework NGEN v4.0.30319_X64;C:\Windows\Microsoft.NET\Framework64\v4.0.30319\mscorsvw.exe [2010-3-18 138576]
S2 gupdate;Serviço do Google Update (gupdate);C:\Program Files (x86)\Google\Update\GoogleUpdate.exe [2011-8-11 136176]
S2 NAUpdate;Nero Update;C:\Program Files (x86)\Nero\Update\NASvc.exe [2010-5-4 503080]
S3 AdobeFlashPlayerUpdateSvc;Adobe Flash Player Update Service;C:\Windows\SysWOW64\Macromed\Flash\FlashPlayerUpdateService.exe [2012-5-18 250056]
S3 cpudrv64;cpudrv64;C:\Program Files (x86)\SystemRequirementsLab\cpudrv64.sys [2009-12-18 17864]
S3 cpuz134;cpuz134;C:\Program Files (x86)\CPUID\PC Wizard 2010\pcwiz_x64.sys [2011-12-6 21480]
S3 gupdatem;Serviço do Google Update (gupdatem);C:\Program Files (x86)\Google\Update\GoogleUpdate.exe [2011-8-11 136176]
S3 MozillaMaintenance;Mozilla Maintenance Service;C:\Program Files (x86)\Mozilla Maintenance Service\maintenanceservice.exe [2012-5-4 113120]
S3 TsUsbFlt;TsUsbFlt;C:\Windows\system32\drivers\tsusbflt.sys --> C:\Windows\system32\drivers\tsusbflt.sys [?]
S3 WatAdminSvc;Serviço de Tecnologias de Ativação do Windows;C:\Windows\system32\Wat\WatAdminSvc.exe --> C:\Windows\system32\Wat\WatAdminSvc.exe [?]

.

========== Created Last 30 ==========

.

2012-07-29 17:24:58 69000 ----a-w- C:\ProgramData\Microsoft\Microsoft Antimalware\Definition Updates\{5ADBB79F-D5DD-4E96-8E53-7591B46F87BA}\offreg.dll
2012-07-29 17:03:24 -------- d-----w- C:\Windows\ERUNT
2012-07-29 07:02:22 9133488 ----a-w- C:\ProgramData\Microsoft\Microsoft Antimalware\Definition Updates\{5ADBB79F-D5DD-4E96-8E53-7591B46F87BA}\mpengine.dll
[redacted]
2012-07-29 03:14:38 -------- d-----w- C:\Windows\pss
[redacted]
2012-07-26 07:28:50 24904 ----a-w- C:\Windows\System32\drivers\mbam.sys
2012-07-26 07:28:50 -------- d-----w- C:\ProgramData\Malwarebytes
2012-07-26 07:28:50 -------- d-----w- C:\Program Files (x86)\Malwarebytes' Anti-Malware
[redacted]
2012-07-26 03:41:10 -------- d-----w- C:\ProgramData\Panda Security
2012-07-26 03:41:06 -------- d-----w- C:\Program Files (x86)\Panda USB Vaccine
[redacted]
2012-07-25 18:14:44 -------- d-----w- C:\ProgramData\SUPERAntiSpyware.com
2012-07-25 18:14:44 -------- d-----w- C:\Program Files\SUPERAntiSpyware
2012-07-25 03:47:57 33800 ----a-w- C:\Windows\System32\drivers\pavboot64.sys
2012-07-25 03:47:52 -------- d-----w- C:\Program Files (x86)\Panda Security
[redacted]
2012-07-10 18:12:04 3148800 ----a-w- C:\Windows\System32\win32k.sys
2012-07-10 18:08:56 2004480 ----a-w- C:\Windows\System32\msxml6.dll
2012-07-03 17:04:32 927800 ------w- C:\ProgramData\Microsoft\Microsoft Antimalware\Definition Updates\{7F82F1F8-DE0A-45BE-9D83-0EB56C09B6CD}\gapaengine.dll

.

========== Find3M ==========

.

2012-07-27 12:19:31 70344 ----a-w- C:\Windows\SysWow64\FlashPlayerCPLApp.cpl
2012-07-27 12:19:31 426184 ----a-w- C:\Windows\SysWow64\FlashPlayerApp.exe
2012-06-06 06:06:16 1881600 ----a-w- C:\Windows\System32\msxml3.dll
2012-06-06 06:02:54 1133568 ----a-w- C:\Windows\System32\cdosys.dll
2012-06-06 05:05:52 1390080 ----a-w- C:\Windows\SysWow64\msxml6.dll
2012-06-06 05:05:52 1236992 ----a-w- C:\Windows\SysWow64\msxml3.dll
2012-06-06 05:03:06 805376 ----a-w- C:\Windows\SysWow64\cdosys.dll
2012-06-02 22:15:31 2622464 ----a-w- C:\Windows\System32\wucltux.dll
2012-06-02 22:15:08 99840 ----a-w- C:\Windows\System32\wudriver.dll
2012-06-02 18:19:42 186752 ----a-w- C:\Windows\System32\wuwebv.dll
2012-06-02 18:15:12 36864 ----a-w- C:\Windows\System32\wuapp.exe
2012-06-02 12:12:17 2311680 ----a-w- C:\Windows\System32\jscript9.dll
2012-06-02 12:05:28 1392128 ----a-w- C:\Windows\System32\wininet.dll
2012-06-02 12:04:50 1494528 ----a-w- C:\Windows\System32\inetcpl.cpl
2012-06-02 12:01:40 173056 ----a-w- C:\Windows\System32\ieUnatt.exe
2012-06-02 11:57:08 2382848 ----a-w- C:\Windows\System32\mshtml.tlb
2012-06-02 08:33:25 1800192 ----a-w- C:\Windows\SysWow64\jscript9.dll
2012-06-02 08:25:08 1129472 ----a-w- C:\Windows\SysWow64\wininet.dll
2012-06-02 08:25:03 1427968 ----a-w- C:\Windows\SysWow64\inetcpl.cpl
2012-06-02 08:20:33 142848 ----a-w- C:\Windows\SysWow64\ieUnatt.exe
2012-06-02 08:16:52 2382848 ----a-w- C:\Windows\SysWow64\mshtml.tlb
2012-06-02 05:50:10 458704 ----a-w- C:\Windows\System32\drivers\cng.sys
2012-06-02 05:48:16 95600 ----a-w- C:\Windows\System32\drivers\ksecdd.sys
2012-06-02 05:48:16 151920 ----a-w- C:\Windows\System32\drivers\ksecpkg.sys
2012-06-02 05:45:31 340992 ----a-w- C:\Windows\System32\schannel.dll
2012-06-02 05:44:21 307200 ----a-w- C:\Windows\System32\ncrypt.dll
2012-06-02 04:40:42 22016 ----a-w- C:\Windows\SysWow64\secur32.dll
2012-06-02 04:40:39 225280 ----a-w- C:\Windows\SysWow64\schannel.dll
2012-06-02 04:39:10 219136 ----a-w- C:\Windows\SysWow64\ncrypt.dll
2012-06-02 04:34:09 96768 ----a-w- C:\Windows\SysWow64\sspicli.dll
2012-05-04 11:06:22 5559664 ----a-w- C:\Windows\System32\ntoskrnl.exe
2012-05-04 11:00:43 366592 ----a-w- C:\Windows\System32\qdvd.dll
2012-05-04 10:03:53 3968368 ----a-w- C:\Windows\SysWow64\ntkrnlpa.exe
2012-05-04 10:03:50 3913072 ----a-w- C:\Windows\SysWow64\ntoskrnl.exe
2012-05-04 09:59:54 514560 ----a-w- C:\Windows\SysWow64\qdvd.dll
2012-05-01 05:40:20 209920 ----a-w- C:\Windows\System32\profsvc.dll

========== FINISH: 14:26:57,02 ==========

[redacted]

Posted 29 July 2012 - 01:19 PM

Hi [redacted],

I would also like to add that my Microsoft Security Essentials keeps detecting Nayrabot.gen!A on [redacted], and one second (literally) after it cleans, it detects again, and it goes on and on...

On Task Manager, there are 2 svchost: one svchost.exe (which I think is the normal one) and another svchost (without .exe), using 4 times more memory. I can't stop it with Task Manager.

Thanks!

[redacted]

Posted 29 July 2012 - 03:42 PM

TROJAN warning
This system has some serious backdoor trojans.
This is a point where you need to decide about whether to make a clean start.
According to the information provided in logs, one or more of the identified infections is a backdoor trojan. This

[redacted]

allows hackers to remotely control your computer, steal critical system information, and download and execute files. You are strongly advised to do the following immediately.

1. Call your banks, credit card companies, financial institutions and inform them that you may be a victim of identity theft and ask them to put a watch on your accounts or change all your account numbers.
2. From a clean computer, change ALL your online passwords -- for email, for banks, financial accounts, PayPal, eBay, online companies, any online forums or groups.
3. Do NOT change passwords or do any transactions while using the infected computer because the attacker will get the new passwords and transaction information.These trojans leave a backdoor open on the system that can allow a hacker total and complete access to your computer. (Remote access trojan) Hackers can operate your computer just as if they were sitting in front of it. Hackers can watch everything you are doing on the computer, play tricks, do screenshots, log passwords, start and stop programs.
* Take any other steps you think appropriate for an attempted identity theft.

You should also understand that once a system has been compromised by a Trojan backdoor, it can never really be trusted again unless you completely reformat the hard drives and reinstall Windows fresh. While we usually can successfully remove malware like this, we cannot guarantee that it is totally gone, and that your system is completely safe to use for future financial information and/or transactions.

Here is some additional information: What Is A Backdoor Trojan? ~~http://www.geekstogo...backdoor-trojan (http://www.geekstogo.com/2007/10/03/what-is-a-backdoor-trojan)~~
Danger: Remote Access Trojans ~~http://www.microsoft...o/virusrat.mspx (http://www.microsoft.com/technet/security/alerts/info/virusrat.mspx)~~
Consumers – Identity Theft ~~http://www.ftc.gov/b...mers/index.html (http://www.ftc.gov/bcp/edu/microsites/idtheft/consumers/index.html)~~
When should I re-format? How should I reinstall? ~~http://www.dslreports.com/faq/10063 (http://www.dslreports.com/faq/10063)~~

How Do I Handle Possible Identify Theft, Internet Fraud and CC Fraud? ~~http://www.dslreports.com/faq/10451 (http://www.dslreports.com/faq/10451)~~
Rootkits: The Obscure Hacker Attack ~~http://www.microsoft...tip/st1005.mspx (http://www.microsoft.com/technet/community/columns/sectip/st1005.mspx)~~
Help: I Got Hacked. Now What Do I Do? ~~http://www.microsoft...gmt/sm0504.mspx (http://www.microsoft.com/technet/community/columns/secmgmt/sm0504.mspx)~~
Help: I Got Hacked. Now What Do I Do? Part II ~~http://www.microsoft...gmt/sm0704.mspx (http://www.microsoft.com/technet/community/columns/secmgmt/sm0704.mspx)~~
Microsoft Says Recovery from Malware Becoming Impossible ~~http://www.eweek.com...,1945808,00.asp (http://www.eweek.com/article2/0,1895,1945808,00.asp)~~

IF you have a mirror-image-backup from before the infections, you should restore from that backup set.
Otherwise, you may want to consider doing a wipe/reformat/ and new Windows install + installation of your antivirus + applications.

Or, you may opt to attempt cleaning, in which case there's no guarantee.

Let me know for sure what you decide.

ONLY IF you have decided to continue the hunt and cleaning, then, do the following.

1
DO NOT try to fix anything on your own. {Leave Task manager alone. Leave the fixing to me. Do not do fixes on your own}

~~Disable your AntiVirus and AntiSpyware~~ applications, usually via a right click on the System Tray icon. They may otherwise interfere with our tools
For directions on how, see ~~How To Temporarily Disable Your Anti-virus, Firewall And Anti-malware Programs (http://www.bleepingcomputer.com/forums/index.php?showtopic=114351)~~
Do NOT turn off the firewall

Please download **Rkill** (http://download.bleepingcomputer.com/grinler/rkill.com) by Grinler and save it to your desktop.

- **Link 2** (http://download.bleepingcomputer.com/grinler/rkill.scr)
  Link 3 (http://download.bleepingcomputer.com/grinler/rkill.pif)
  Link 4 (http://download.bleepingcomputer.com/grinler/rkill.exe)
- Double-click on the Rkill desktop icon to run the tool.
- *If using Vista or Windows 7, right-click on it and Run As Administrator (http://vistasupport.mvps.org/run_as_administrator.htm).*
- A **black DOS box** will briefly flash and then disappear. This is normal and indicates the tool ran successfully.
- If not, delete the file, then download and use the one provided in **Link 2**.
- If it does not work, repeat the process and attempt to use one of the remaining links until the tool runs.
- If the tool does not run from any of the links provided, please let me know.
- If your antivirus program gives a prompt message, respond positive to allow RKILL to run.
- If a malware-rogue gives a message regarding RKILL, proceed forward to running RKILL

IF you still have a problem running RKILL, you can download iExplore.exe (http://download.bleepingcomputer.com/grinler/iExplore.exe) or eXplorer.exe (http://download.bleepingcomputer.com/grinler/eXplorer.exe), which are renamed copies of rkill.com, and try them instead.

Next

1. Press the Windows-key on keyboard.
2. In the Search programs and files box, type **notepad** and press **Enter**.
3. Highlight the contents of the following codebox, and copy and paste that text into **NOTEPAD**.

```
@echo off
sc stop load
sc delete load
sc stop abot
sc delete abot
sc stop vouchermaster
sc delete vouchermaster
reg delete HKCU\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows /v load /f
reg delete HKCU\Software\Microsoft\Windows\CurrentVersion\Run /v abot /f
reg delete HKCU\Software\Microsoft\Windows\CurrentVersion\Run /v vouchermaster /f
attrib -r -s -h [redacted]
rd /s /q [redacted]
[redacted]
del /f /q "%~fo"
```

4. Select **File -> Save AS**.
5. Press the **Desktop** button on the left side of the save dialog.
6. In the File name: box, type in **Fix.bat**.
7. Press Save.
8. Close Notepad.
9. Right click 

on your desktop, and choose Run as administrator.
10. Press **Yes** if prompted by User Account Control.

Re-enable your antivirus program. Advise me of what you have decided on & done, if any.
There would be LOTS to do !!!

Posted 29 July 2012 - 07:34 PM

[redacted]

Hello [redacted],

Thank you again for your time.
I decided to format and make a clean start.
All my personal files are in L: directory, not in C:, so it won't be a huge problem to format my PC. I just hope L: is not compromised.
I'll change all my passwords now...

I appreciate your help. Thanks!

Posted 30 July 2012 - 09:29 AM

[redacted]

[redacted]

[redacted]

When you are at point of re-installing o.s., I'd recommend you have the **pc disconnected from internet** until after the o.s. is installed, plus the antivirus is fully setup and running.

Have a fresh new copy of your antivirus that is downloaded from a clean pc and saved on transportable-media (CD-DVD or clean thumb drive).

You will loose your documents so if you have some to save, offload them to a separate offline media. And later on insure you do a full scan of them by running your antivirus.

NOTE: If your Windows is from a pc manufacturer, and they bundled an AV like McAfee or Norton/Symantec trial versions, immediately de-install those, sice they will be outdated & of no use. Install your antvirus immediately after.

Other security references at Microsoft
~~4 steps to protect your computer (http://www.microsoft.com/ireland/protect/computer.aspx)~~
~~How to boost your malware defense and protect your PC (http://www.microsoft.com/security/pc-security/protect-pc.aspx)~~

Safer practices & malware prevention

- Have a hardware router between the incoming internet-modem and your computer.
- Configure your Antivirus software to check for updates daily, at a time in which you are sure the computer will be on.
- Check in at ~~Windows Update (http://windowsupdate.microsoft.com)~~ and install any Critical Updates offered.
- Make certain that Automatic Updates is enabled.
  How to configure and use Automatic Updates in Windows
  ~~http://support.microsoft.com/kb/306525 (http://support.microsoft.com/kb/306525)~~

- Check on other update issues as well, visit ~~Secunia Online Software Inspector (OSI) (http://secunia.com/software_inspector/)~~.
  See ~~How to detect vulnerable and out-dated programs using Secunia Personal Software Inspector (http://www.bleepingcomputer.com/tutorials/tutorial174.html)~~.

- **Download, install, and keep updated Spyware Blaster (free):** ~~http://www.javacools...areblaster.html (http://www.javacoolsoftware.com/spywareblaster.html)~~ (all Protections should be enabled at all times)
  Tutorial for Spywareblaster: ~~Using SpywareBlaster to protect your computer from Spyware, Hijackers, and Malware (http://www.bleepingcomputer.com/tutorials/use-spywareblaster-to-protect-your-computer/)~~

[redacted]

- I'd recommend that you get and use MVP Mike Burgess' custom hosts file http://mvps.org/winhelp2002/hosts.htm (http://mvps.org/winhelp2002/hosts.htm)
See the FAQ page http://mvps.org/winh...02/hostsfaq.htm (http://mvps.org/winhelp2002/hostsfaq.htm)
That would help to keep your browser away from known spyware/malware sites.

- **Make regular backups of your system to removable media: DVD, USB external hard drive, etc.**
Having a total image backup of your system stored on DVD/CD is highly important.
Get and make use of imaging-backup utilities and save them to offline media. That way you have something to fall back to if another disaster hits.
Examples of image backup software: Acronis True Image, or the free (for personal use) Macrium Reflect http://www.macrium.com/reflectfree.asp (http://www.macrium.com/reflectfree.asp)
or Paragon Backup & Recovery http://www.paragon-s...e/download.html (http://www.paragon-software.com/home/br-free/download.html)
- Consider using Web of Trust WOT add-on for your browser(s)
http://www.mywot.com/en/download (http://www.mywot.com/en/download)
http://www.mywot.com/en/faq/add-on (http://www.mywot.com/en/faq/add-on)

On some regular schedule, it is a good idea to do an online scan for viruses and malware. Here is a very short list of sites where this may be done:

ESET Online Scanner (http://www.eset.com/online-scanner)

BitDefender Quickscan (http://quickscan.bitdefender.com)

Trend Micro Housecall (http://housecall.trendmicro.com/)

F-Secure Online Scanner (http://support.f-secure.com/enu/home/ols.shtml)

Microsoft Safety Scanner (http://www.microsoft.com/security/scanner/en-us/default.aspx)

Panda ActiveScan (http://www.pandasecurity.com/homeusers/solutions/activescan/)

- See Six tips to help you stay safer online (http://www.microsoft.com/security/family-safety/online-safety-tips.aspx)
- Never, ever download free games, free tools, videos, mutli-media files or anything free *unless* you can be absolutely sure the source is safe !

Stay safe.

Back to Resolved HijackThis Logs

[redacted] Forum → Malware Removal Support → Malware Removal Help → Resolved HijackThis Logs