

Forum: [Hack Forums](#)

Thread: [\[Infected\] Server Based Virus / Maleware](#)

Acsriot - June 15, 2015, 7:42 am

Hey all. I have a heavily infected system at my workplace. The system is a isolated setup, with no outside internet access. LAN only.

Symptom : Random IE Windows popping up, but theres no internet access so I can't see where it is navigating to

Symptom : Windows Task Scheduler has 1-3 tasks that automatically re populated calling a .exe file in System32 or temp

Symptom : Random Crashes, lock ups forcing a restart

I have tried Hijack this, and Maleware bytes. Going to try Glasswire to see what the files are trying to communicate with.

I'll post Hijack logs and M&B Logs in a few minutes

--- Riot

MXHNDFYSYS.exe is starting every restart

Logfile of Trend Micro HijackThis v2.0.5

Scan saved at 8:09:32 AM, on 6/15/2015

Platform: Windows 7 SP1 (WinNT 6.00.3505)

MSIE: Internet Explorer v10.0 (10.00.9200.16686)

Boot mode: Normal

Running processes:

C:\windows\system32\taskhost.exe

C:\windows\system32\Dwm.exe

C:\windows\Explorer.EXE

C:\Program Files\Harris\MediaBase Pro\Notify.exe

C:\windows\system32\conhost.exe

C:\Program Files\Harris\MediaBase Pro\Admin.exe

C:\Program Files\Harris\NMG\nmg.exe

C:\windows\system32\SearchFilterHost.exe

C:\windows\system32\mmc.exe

E:\HijackThis.exe

R1 - HKCU\Software\Microsoft\Internet Explorer\Main,Search Page =

<http://go.microsoft.com/fwlink/?LinkId=54896>

R0 - HKCU\Software\Microsoft\Internet Explorer\Main,Start Page =

<http://go.microsoft.com/fwlink/?LinkId=69157>

R1 - HKLM\Software\Microsoft\Internet Explorer\Main,Default_Page_URL =

<http://go.microsoft.com/fwlink/p/?LinkId=255141>

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/p/?LinkId=255141>

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

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

R0 - HKCU\Software\Microsoft\Internet Explorer\Toolbar,LinksFolderName =

O4 - HKLM\..\Run: [nwiz] C:\Program Files\NVIDIA Corporation\nview\nwiz.exe /installquiet

O4 - HKLM\..\Run: [Adobe ARM] "C:\Program Files\Common

Files\Adobe\ARM\1.0\AdobeARM.exe"

O4 - HKCU\..\Run: [cmba] "C:\Users\Administrator\AppData\Roaming\Microsoft\Hndfy\hndfy.exe"

O4 - HKCU\..\Run: [Notify] "C:\Users\Administrator\AppData\Roaming\Microsoft\Hndfy\hndfy.exe" /c

C:\Program Files\Harris\MediaBase Pro\Notify.exe -con /autostart

O4 - HKCU\..\Run: [bmyu] "C:\Users\Administrator\AppData\Roaming\Microsoft\Hndfy\hndfy.exe"

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

O11 - Options group: [ACCELERATED_GRAPHICS] Accelerated graphics

O16 - DPF: {D27CDB6E-AE6D-11CF-96B8-444553540000} (Shockwave Flash Object) -

<http://fpdownload2.macromedia.com/get/flashplayer/current/swflash.cab>

O23 - Service: Adobe Acrobat Update Service (AdobeARMservice) - Adobe Systems Incorporated - C:\Program Files\Common Files\Adobe\ARM\1.0\armsvc.exe

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

O23 - Service: NVIDIA Performance Driver Service - Unknown owner - C:\Program Files\NVIDIA Corporation\Performance Drivers\nvPDsvc.exe

O23 - Service: NVIDIA Display Driver Service (nvsvc) - NVIDIA Corporation - C:\Windows\system32\nvsvc.exe

O23 - Service: NVIDIA Stereoscopic 3D Driver Service (Stereo Service) - NVIDIA Corporation - C:\Program Files\NVIDIA Corporation\3D Vision\nvSCPAPISvr.exe

--

End of file - 3019 bytes

darkorbisupper - June 15, 2015, 8:34 am

HI ;)

I need to help you ;)

Pls download : Farbars Recovery Tool from the Website : <http://www.bleepingcomputer.com/download/farbar-recovery-scan-tool/>

Post the Log here or send me a private message (better)

Acsriot - June 15, 2015, 8:34 am

Edit : I have just Identified the threat as the JSAgent Trojan, Best removal strategy ?

darkorbisupper - June 15, 2015, 8:39 am

Make a boot time scan and delete all viruses

YekiM - June 15, 2015, 4:16 pm

(Jun 15, 2015 08:34 AM)Acsriot Wrote: [\[CITE\]](#) Edit : I have just Identified the threat as the JSAgent Trojan, Best removal strategy ?

Hi, unfortunately I cannot give you advice for I am in training, and you will need to wait for a malware removal specialist. However, I can get you started and reduce the amount of time taken to solve this problem.

Before we start please note the following: Analysis and research take some time, so please be patient. If your helper doesn't respond for more than 24 hours, PM them.

Please follow their instructions exactly as they are posted and do not run any tools on your own.

Stay with them to the very end, the absence of symptoms doesn't mean that your machine is fully operational.

They can't foresee everything, so if anything unexpected happens, please stop and inform them.

If you have any questions, please don't hesitate to ask your helper.

Category: Discovery

Step 1: Farbar Recovery Scan Tool (FRST) ScanDownload [Farbar Recovery Scan Tool \(x32\)](#) or [Farbar Recovery Scan Tool \(x64\)](#) and save the file to your Desktop

Note: Download and run the version compatible with your system (32 or 64-bit). Download both if you're unsure; only one will run

Right-Click FRST.exe or FRST64.exe and select Run as Administrator

Click Yes to the disclaimer.

Ensure the Addition.txt box is checked.

Click the Scan button and let the program run.

When it has finished, it will alert you in separate pop-ups that both FRST.txt and addition.txt has been saved to the desktop. Go ahead and press Ok

Two logs (FRST.txt & Addition.txt) will now be open on your Desktop. Copy the contents of both logs and paste them to [pastebin.com](#). Post the link here.

Step #2: RogueKillerDownload [RogueKiller \(x64\)](#) and save the file to your Desktop.

Close any running programs.

Right-Click RogueKiller.exe and select Run as administrator to run the program.

Allow the Prescan to complete. Upon completion, a window will open. Click Accept.

A browser window may open. Close the browser window.

Click . Upon completion, click .

Close the program. Do not fix anything!

A log (RKreport.txt) will be open. Copy the contents of the log to pastebin.com, click Submit and paste the link to it in your next reply.

In your next reply:FRST.txt

Addition.txt

RKreport.txt

Cheese - June 15, 2015, 7:13 pm

(Jun 15, 2015 08:34 AM)darkorbitssupper Wrote: [\[CITE\]](#) HI ;)

I need to help you ;)

Pls download : Farbars Recovery Tool from the Website : <http://www.bleepingcomputer.com/download/farbar-recovery-scan-tool/>

Post the Log here or send me a private message (better)

Please don't take advice from this guy, he tried to spread his RAT here... He is also not experienced and will most likely leave your system in a worse condition then it already was.

Knautschtabak - June 15, 2015, 11:50 pm

(Jun 15, 2015 08:34 AM)Acsriot Wrote: [\[CITE\]](#) Edit : I have just Identified the threat as the JSAgent Trojan, Best removal strategy ?JSAgent Trojan is a generic detection name for any JavaScript based trojan. This is no real identification, it can mean almost everything.

Run FRST if you want to get help (see instructions above by YekiM). HJT is outdated and not sufficient anymore to deal with the threats today.

Acsriot - June 16, 2015, 10:29 am

+1 YekiM

Doing all of that now.

<https://www.dropbox.com/s/sgk3nmxwoft1olz/FRST.txt?dl=0>

<https://www.dropbox.com/s/a44ig82rornizw7/Addition.txt?dl=0>

https://www.dropbox.com/s/27z525h4f5ac9mz/RKreport_SCN_06162015_124012.log?dl=0

I ran a Avast Bootscan on this machine, its listed as "Clean" , but keep in mind this is inside a closed network, all the machines will usually get the virus's / random ass DLL files back in a few hours

-- Riot

Knautschtabak - June 17, 2015, 1:03 am

Acsriot, please disconnect every infected machine from the network or they will reinfect each other. You can put them back when they are clean.

The machine you made the logs from looks clean, there are just malicious startup entries left, whose files are missing.

Farbar Recovery Scan Tool (FRST) Script Press the Windows Key + r on your keyboard at the same time. Type Notepad and click OK.

Copy the entire contents of the codebox below and paste into the Notepad document.

Code start

CreateRestorePoint:

Startup: C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Start

Menu\Programs\Startup\zodokge.lnk [2015-05-13]

ShortcutTarget: zodokge.lnk -> C:\Users\Admin\AppData\Roaming\Microsoft\Zodokge\zodokge.exe

(No File)

Startup: C:\Users\Ingest_2\AppData\Roaming\Microsoft\Windows\Start

Menu\Programs\Startup\avyzey.lnk [2015-05-13]

ShortcutTarget: avyzey.lnk -> C:\Users\Ingest_2\AppData\Roaming\Microsoft\Avyzey\avyzey.exe

(No File)

EmptyTemp:

end

Click File, Save As and type fixlist.txt as the File Name.

Important: The file must be saved in the same location as FRST.exe.

NOTICE: This script is intended for use on this particular machine. Do not use this script on any other machine; doing so may cause damage to your Operating System. Right-Click FRST.exe and select Run as administrator to run the program.

Click Fix.

A log (Fixlog.txt) will open on your desktop. Copy the contents of the log to pastebin.com and paste the link to it in your next reply.