

Forum:[Hack Forums](#)

Thread: [Got ratted from a hack pack and it keeps reinstalling](#)

lukasv456 - May 9, 2015, 8:27 am

So i downloaded a hack pack off the site and i was just going through the programs to see what each one does since im new here, and then i noticed when i opened task manager it showed a running app called "Internet Explorer (32bit)" but the icon was some lightning thing and when i click on it and made a little drop down that showed Form1 lol :D, so then i got curious and ran dark comet rat remover and DC Keylogger and Winwork.exe keep popping up and wont get removed..

Knautschtabak - May 9, 2015, 8:41 am

Please read through the points below to ensure this process moves as quickly and efficiently as possible. Ensure you read through my instructions thoroughly, and carry out each step in the order specified.

Please do not run any tools or take any steps other than those I provide for you. Independent efforts may make matters worse, and will affect my ability in providing the best set of instructions for you.

Please backup important files before proceeding with my instructions. Malware removal can be unpredictable at times.

If you come across any issues whilst following my instructions, please stop and inform me of the issue in as much detail as possible. Please do not hesitate to ask before proceeding.

I will notify you when I believe your computer is free of malware. Please bear in mind, absence of symptoms does not necessarily correlate to absence of malware, so please wait until the "All Clean".

Step 1: Farbar Recovery Scan Tool (FRST) ScanPlease download [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.

Upon completion, click OK, then OK on the Addition.txt pop up screen.

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 \(32 bit\)](#)/[RogueKiller \(64 bit\)](#) and save the file to your Desktop.

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

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.

lukasv456 - May 9, 2015, 2:14 pm

Addition: pastebin.com/wMJJBuA3

FRST: pastebin.com/wU3QHks1

(May 9, 2015 08:41 AM)Knautschtabak Wrote: [\[CITE\]](#) Please read through the points below to ensure this process moves as quickly and efficiently as possible. Posted above, thank you for trying to help

(May 9, 2015 02:14 PM)lukasv456 Wrote: [\[CITE\]](#) Addition: pastebin.com/wMJJBuA3

FRST: pastebin.com/wU3QHks1

Posted above, thank you for trying to help

Roguekiller: pastebin.com/zxheHs2d

Knautschtabak - May 10, 2015, 12:08 pm

Yes, you have a RAT.

Question: Do you use Darkcomet?

Backdoor warning: We can remove the visible infection signs, but due to the nature of this type of malware, no one can guarantee the trustworthiness of your computer. If you want to use it for anything important like online-banking, reformat and install of your operating system is the safest option.

Note: Please change any of your passwords from a non-infected computer.

Step 1: Roguekiller Fix

Follow the same steps you did on RogueKiller, but after the Scan is finish go through each tab to find and check the following entries.

After you have checked all the entries, click on Delete and finally Report and paste the log to <http://pastebin.com/>

```
Code [Suspicious.Path\VT.Backdoor:Win32\Fynloski.A] WinWork.exe(5296) --
C:\Users\Lucas\AppData\Local\Temp\Path_58044\WinWork.exe[-]VT(16) -> Killed [TermProc]
[Suspicious.Path\Proc.Injector\VT.Backdoor:Win32\Fynloski.A] WinWork.exe(5740) --
C:\Users\Lucas\AppData\Local\Temp\Path_8107\WinWork.exe[-]VT(16) -> Killed [TermProc]
[Rans.Gendarm] (X64)
HKEY_USERS\S-1-5-21-1223581141-2463725323-2735195162-1002\Software\Microsoft\Windows\
CurrentVersion\Run | update : C:\Users\Lucas\AppData\Local\Temp\WinApp\RCE.exe [-] -> Found
[Rans.Gendarm] (X86)
HKEY_USERS\S-1-5-21-1223581141-2463725323-2735195162-1002\Software\Microsoft\Windows\
CurrentVersion\Run | update : C:\Users\Lucas\AppData\Local\Temp\WinApp\RCE.exe [-] -> Found
[PUM.SecurityCenter] (X86) HKEY_LOCAL_MACHINE\Software\Microsoft\Security Center |
AntiVirusDisableNotify : 0 -> Found
[PUM.SecurityCenter] (X86) HKEY_LOCAL_MACHINE\Software\Microsoft\Security Center |
UpdatesDisableNotify : 1 -> Found
```

Step 2: Farbar Recovery Scan Tool (FRST) ScriptPress 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:

CloseProcesses:

C:\Users\Lucas\AppData\Local\Temp\Path_58044

C:\Users\Lucas\AppData\Local\Temp\Path_8107

Folder: C:\Users\Lucas\AppData\Local\Temp

HKU\S-1-5-21-1223581141-2463725323-2735195162-1002\...\Run: [Spotify Web Helper] => [X]

HKU\S-1-5-21-1223581141-2463725323-2735195162-1002\...\Run: [AdobeBridge] => [X]

HKU\S-1-5-21-1223581141-2463725323-2735195162-1002\...\Run: [Xvid] => [X]

HKU\S-1-5-21-1223581141-2463725323-2735195162-1002\...\Run: [CCleaner Monitoring] => [X]

HKU\S-1-5-21-1223581141-2463725323-2735195162-1002\...\Run: [Spotify] => [X]

HKU\S-1-5-21-1223581141-2463725323-2735195162-1002\...\Run: [Steam] => [X]

HKU\S-1-5-21-1223581141-2463725323-2735195162-1002\...\Run: [update] => [X]

HKU\S-1-5-21-1223581141-2463725323-2735195162-1002\...\Policies\system: [EnableLUA] 0

HKU\S-1-5-21-1223581141-2463725323-2735195162-1002\...\MountPoints2:

{46b497a4-b5dc-11e3-8275-d43d7eed4b4e} - "E:\Setup\src\Autorun.exe"

AppInit_DLLs-x32: ?? E?? => "?? E??" File Not Found

S3 X6va017; \??\C:\Windows\SysWOW64\Drivers\X6va017 [X]

S3 X6va021; \??\C:\Windows\SysWOW64\Drivers\X6va021 [X]

S3 X6va022; \??\C:\Windows\SysWOW64\Drivers\X6va022 [X]

S3 X6va025; \??\C:\Windows\SysWOW64\Drivers\X6va025 [X]

S3 X6va026; \??\C:\Windows\SysWOW64\Drivers\X6va026 [X]

S3 X6va027; \??\C:\Windows\SysWOW64\Drivers\X6va027 [X]

S3 X6va028; \??\C:\Windows\SysWOW64\Drivers\X6va028 [X]

R3 X6va029; \??\C:\Windows\SysWOW64\Drivers\X6va029 [X]

C:\Users\Lucas\Downloads\ComboFix.exe

File: C:\Users\Lucas\AppData\Local\LumaEmu

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.

lukasv456 - May 10, 2015, 1:14 pm

(May 10, 2015 12:08 PM)Knautschtabak Wrote: [\[CITE\]](#) [*]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.

[/LIST]

fixlog: pastebin.com/ymfLsar1

Knautschtabak - May 10, 2015, 11:23 pm

Step 1: Malwarebytes Anti-Malware (MBAM) Please download the [Malwarebytes Anti-Malware](#) setup file to your Desktop.

Open mbam-setup.x.x.xxxx.exe (x represents the version #) and follow the prompts to install the programme.

Open Malwarebytes Anti-Malware and click Update Now.

Once updated, click the Settings tab, followed by Detection and Protection and tick Scan for rootkits .

Click the Scan tab, ensure Threat Scan is selected and click Start Scan.

Note: You may see the following message, "Could not load DDA driver". Click Yes, allow your PC to reboot and continue afterwards.

If threats are detected, click Remove Selected. If you are prompted to reboot, click Yes.

Upon completion of the scan (or after the reboot), click the History tab.

Click Application Logs and double-click the Scan Log.

Click Copy to Clipboard and paste the pastebin.com link for the log in your next reply.

Step 2: FRST

Do another scan with FRST and post a fresh FRST.txt and Addition.txt

lukasv456 - May 11, 2015, 12:05 pm

MBAM : pastebin.com/a2jpnTTN

FRST: pastebin.com/rMGxZnSN

ADDITION: pastebin.com/pKU27aFk

Knautschtabak - May 11, 2015, 12:58 pm

Quote:C:\Users\Lucas\Desktop\Tools and stuff\Tools\DarkCometRAT531

I suspect this is yours. If you need it, just get it back from MBAM quarantine.

Empty your recycle bin. It is full of infected files.

You snipped the first lines in your last FRST fix. We need to do these again.

Also there is an issue with a Unicode entry. Open the FRST.txt on your machine, copy the line that looks like this:

```
Code AppInit_DLLs-x32: ?? E?? => "?? E??" File Not Found
```

And add this line after CloseProcesses: to the following FRST script. FRST is able to read Unicode, but I cannot really copy it properly for you.

Farbar Recovery Scan Tool (FRST) ScriptPress 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:

CloseProcesses:

C:\Users\Lucas\AppData\Local\Temp\Path_58044

C:\Users\Lucas\AppData\Local\Temp\Path_8107

Folder: C:\Users\Lucas\AppData\Local\Qc1n6SRAYs2IKsFWMS

Folder: C:\Users\Lucas\AppData\Local\Temp

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.

lukasv456 - May 11, 2015, 7:29 pm

(May 11, 2015 12:58 PM)Knautschtabak Wrote: [\[CITE\]](#) [*]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.

[/LIST]

fixlog.txt: pastebin.com/s2fvzXEt

Grim - May 11, 2015, 7:30 pm

i would never recommend downloading those packs. a lot of those files are usually outdated and probably have malware of some kind.

Knautschtabak - May 11, 2015, 7:44 pm

Give me a fresh FRST.txt and Addition.txt, please.

lukasv456 - May 12, 2015, 11:41 am

(May 11, 2015 07:30 PM)?Sith Lord Wrote: [\[CITE\]](#) i would never recommend downloading those packs. a lot of those files are usually outdated and probably have malware of some kind.

Yea i learned that now :D,i just deleted all of it and am just downloading fresh new releases :P

FRST: pastebin.com/hKusu7dz

addition: pastebin.com/X9hWezKs

(May 11, 2015 07:44 PM)Knautschtabak Wrote: [\[CITE\]](#) Give me a fresh FRST.txt and Addition.txt, please.

Ta-da , thanks for the help

NukeHV - May 12, 2015, 11:49 am

You should start reading my malware guide [Here](#), It tells you everything about the newest malware's out there and how you protect against those threats.

Knautschtabak - May 12, 2015, 11:59 am

Please navigate to the following folder and delete it:

C:\Users\Lucas\AppData\Local\Qc1n6SRAyS2IKsFWMS

Empty your recycle bin after that.

We got rid of the RAT, but the trovi search in your browser makes me suspicious. We will do some adware cleaning too.

Junkware Removal Tool (JRT)Please download [Junkware Removal Tool](#) and save the file to your Desktop.

Create a System Restore Point. For instructions, please refer to the following [link](#) (W8) | [link](#) (W7) | [link](#) (Vista).

Temporarily disable your anti-virus software. For instructions, please refer to the following [link](#).

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

Follow the prompts and allow the scan to run uninterrupted.

Upon completion, a log (JRT.txt) will open on your desktop.

Re-enable your anti-virus software

Copy the contents of JRT.txt to pastebin.com and paste the link in your next reply.

AdwCleanerPlease download [AdwCleaner](#) and save the file to your Desktop.

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

Follow the prompts.

Click Scan.

Upon completion, click Report. A log (AdwCleaner[R0].txt) will open. Briefly check the log for anything you know to be legitimate.

Ensure anything you know to be legitimate does not have a checkmark, and click Clean.

Follow the prompts and allow your computer to reboot.

After rebooting, a log (AdwCleaner[S0].txt) will open. Copy the contents of the log to pastebin.com and paste the links in your next reply.

-- File and folder backups are made for items removed using this tool. Should a legitimate file or folder be removed (otherwise known as a 'false-positive'), simple steps can be taken to restore the item. Please do not overly concern yourself with the contents of AdwCleaner[R0].txt.

lukasv456 - May 12, 2015, 12:20 pm

(May 12, 2015 11:59 AM)Knautschtabak Wrote: [\[CITE\]](#) [*]Copy the contents of JRT.txt to pastebin.com and paste the link in your next reply.

JRT : pastebin.com/DsN7CeRX

adw : pastebin.com/JdKL2grV

Knautschtabak - May 12, 2015, 12:40 pm

We are almost done. ?

ESET Online Scan

Note: This scan may take a long time to complete. Please do not browse the Internet whilst your Anti-Virus is disabled. Please download [ESET Online Scan](#) and save the file to your Desktop.

Temporarily disable your anti-virus software. For instructions, please refer to the following [link](#).

Double-click esetsmartinstaller_enu.exe to run the programme.

Agree to the EULA by placing a checkmark next to Yes, I accept the Terms of Use. Then click Start.

Agree to the Terms of Use once more and click Start. Allow components to download.

Place a checkmark next to Enable detection of potentially unwanted applications.

Click Advanced settings. Place a checkmark next to: Scan archives

Scan for potentially unsafe applications

Enable Anti-Stealth technology

Ensure Remove found threats is unchecked.

Click Start.

Wait for the scan to finish. Please be patient as this can take some time.

Upon completion, click

[img]http://billy-oneal.com/Canned%20Speeches/speechimages/eset/esetListThreats.png[/img]. If no threats were found, skip the next two bullet points.

Click [img]http://billy-oneal.com/Canned%20Speeches/speechimages/eset/esetExport.png[/img] and save the file to your Desktop, naming it something such as "MyEsetScan".

Push the Back button.

Place a checkmark next to

[img]http://3-ps.googleusercontent.com/x/forums.whatthetech.com/i.imgur.com/xKN1w2nv.png.page speed.ic.JWqlaEgZi7.png[/img] and click

[img]http://1-ps.googleusercontent.com/x/forums.whatthetech.com/i.imgur.com/SzOC1p0.png.pages peed.ce.OWDP45O6oG.png[/img].

Re-enable your anti-virus software.

Copy the contents of the log and paste in your next reply.

lukasv456 - May 12, 2015, 4:50 pm

(May 12, 2015 12:40 PM)Knautschtabak Wrote: [\[CITE\]](#) [*]Copy the contents of the log and paste in your next reply.

[/LIST]

MyEsetScan: pastebin.com/iug1gYrk

Knautschtabak - May 12, 2015, 8:32 pm

The ESET findings are worrisome, especially since some of them are in your appdata temp. Did you run any of these tools that were found while we were cleaning up?

Please provide a fresh FRST.txt and Addition.txt. I want to make sure these entries are not in your startup.

(Michael) - May 12, 2015, 8:42 pm

Bruh you're going through so much shit with all these scans. A simple scan with Norton Power Eraser and MalwareBytes would most likely get rid of everything. Just from my experience. I would think the user above me probably knows more though.

Also, post a community alert against the guy who released the pack. Or tell him to delete it first and to warn all users who've downloaded it to do a scan.

Good luck with removing the RAT.

Knautschtabak - May 13, 2015, 12:01 am

(May 12, 2015 08:42 PM)(Michael) Wrote: [\[CITE\]](#) Bruh you're going through so much shit with all these scans. A simple scan with Norton Power Eraser and MalwareBytes would most likely get rid of everything. Just from my experience. I would think the user above me probably knows more though.

Also, post a community alert against the guy who released the pack. Or tell him to delete it first and to warn all users who've downloaded it to do a scan.

Good luck with removing the RAT.

In a lot of cases this can be enough, but not in this case.

For now I just need to make sure that nothing came back or re-infected. A FRST scan is not really time-consuming, not comparable to a full malware scan with ESET or similar.

lukasv456 - May 13, 2015, 11:25 am

(May 12, 2015 08:32 PM)Knautschtabak Wrote: [\[CITE\]](#) The ESET findings are worrisky, especially since some of them are in your appdata temp. Did you run any of these tools that were found while we were cleaning up?

Please provide a fresh FRST.txt and Addition.txt. I want to make sure these entries are not in your startup.

the only thing i have done was just download some fresh stuff off forums like , 2 crypters and njrat, and test ratted myself twice w/ uninstall

(May 13, 2015 12:01 AM)Knautschtabak Wrote: [\[CITE\]](#) In a lot of cases this can be enough, but not in this case.

For now I just need to make sure that nothing came back or re-infected. A FRST scan is not really time-consuming, not comparable to a full malware scan with ESET or similar.

FRST: pastebin.com/FAuvd6dd

addition : pastebin.com/TgQGzfwf

Knautschtabak - May 13, 2015, 11:59 am

That would explain it. I would not test a RAT on the main machine, you don't know if the uninstaller removes everything.

Your logs look good. ?

Just update your Java and maybe get an Antivirus Suite.

DelFixPlease download [DelFix](#) and save the file to your Desktop.

Double-click DelFix.exe to run the programme.

Place a checkmark next to the following items:Remove disinfection tools

Create registry backup

Click the Run button.

-- This will remove the specialised tools we used to disinfect your system. Any leftover logs, files, folders or tools remaining on your Desktop which were not removed can be deleted manually (right-click the file + delete).

--- Malwarebytes Anti-Malware will still be present on your computer. I recommend keeping this programme, updating and scanning with it once a week to maintain security on your computer. If you do not wish to keep this programme on your computer, you can uninstall it by pressing the Windows Key+ r on your keyboard at the same time, typing appwiz.cpl, clicking OK and searching for Malwarebytes.

lukasv456 - May 13, 2015, 12:20 pm

(May 13, 2015 11:59 AM)Knautschtabak Wrote: [\[CITE\]](#) That would explain it. I would not test a RAT on the main machine, you don't know if the uninstaller removes everything.
Your logs look good. ?

Just update your Java and maybe get an Antivirus Suite.

DelFixPlease download [DeFix](#) and save the file to your Desktop.

Double-click DeFix.exe to run the programme.

Place a checkmark next to the following items:Remove disinfection tools

Create registry backup

Click the Run button.

-- This will remove the specialised tools we used to disinfect your system. Any leftover logs, files, folders or tools remaining on your Desktop which were not removed can be deleted manually (right-click the file + delete).

--- Malwarebytes Anti-Malware will still be present on your computer. I recommend keeping this programme, updating and scanning with it once a week to maintain security on your computer. If you do not wish to keep this programme on your computer, you can uninstall it by pressing the Windows Key+ r on your keyboard at the same time, typing appwiz.cpl, clicking OK and searching for Malwarebytes.

Whats a good Antivirus Suite you recommend?
also how do i +rep you?

Knautschtabak - May 13, 2015, 12:33 pm

A good commercial one: Kaspersky

A good free one: Well, I wouldn't use Windows Defender seeing how much they suck at the reputable AV Tests. Avast or AVG are ok.

Quote:also how do i +rep you?

You can't +rep me. You would need to upgrade your account.

Don't worry, though, I do malware removal for free. I need to get my breakfast.

lukasv456 - May 13, 2015, 12:34 pm

(May 13, 2015 12:33 PM)Knautschtabak Wrote: [\[CITE\]](#) A good commercial one: Kaspersky
A good free one: Well, I wouldn't use Windows Defender seeing how much they suck at the
reputable AV Tests. Avast or AVG are ok.

You can't +rep me. You would need to upgrade your account.
Don't worry, though, I do malware removal for free. I need to get my breakfast. Alright, thank you
very much defiantly got a lot of breakfast on this one :P

Knautschtabak - May 13, 2015, 12:41 pm

[img]http://fc06.deviantart.net/fs70/f/2013/054/8/f/garfield_gets_real_gif____derp_derp_derp_derp_by_c0l0ss4l_st1nk3r-d5w146m.gif[/img]