

Forum:[Hack Forums](#)

Thread: [Possibly infected](#)

SIM-3487621 - April 6, 2020, 8:04 am

My dumbass ran a program which probably infected me. Any suggestions on how to find the virus if there actually is one?

Bastille - April 6, 2020, 8:07 am

Check the running processes in the taskmanager, run Malwarebytes

SIM-3487621 - April 6, 2020, 8:09 am

(Apr 6, 2020 08:07 AM)Yseurk Wrote: [\[CITE\]](#) Check the running processes in the taskmanager, run MalwarebytesI've already done both. Processes look pretty normal to me and Malwarebytes found nothing.

Bastille - April 6, 2020, 8:14 am

(Apr 6, 2020 08:09 AM)InfamousalGT Wrote: [\[CITE\]](#) I've already done both. Processes look pretty normal to me and Malwarebytes found nothing.

I would say everything seems fine so

Avoid weird programs for the future

Have a nice day buddy

Knautschtabak - April 6, 2020, 10:59 pm

You already know the culprit that may have cause an infection. So what you can do is upload said program to a scanner service like Virustotal. Check which AV engine detects it. Use one of those engines to scan your system. The chance getting rid of the infection (if there is any by that file) is higher that way.

SIM-3487621 - April 7, 2020, 12:28 am

(Apr 6, 2020 10:59 PM)Knautschtabak Wrote: [\[CITE\]](#) You already know the culprit that may have cause an infection. So what you can do is upload said program to a scanner service like Virustotal. Check which AV engine detects it. Use one of those engines to scan your system. The chance getting rid of the infection (if there is any by that file) is higher that way.[Virus Total scan](#)

[Virus total scan of some kind of program it opened](#)

Its a open source rat. Anything suspicious in there?

Bastille - April 7, 2020, 3:48 am

You intentionally ran a malware on your computer and then you come here to ask help ?

You are looking for help in the white hat section while you are attempting for black hat activities ?!!

May your computer die because of your stupidity

Astonished - April 7, 2020, 8:49 am

Looks to me like you actually are infected and that you may have malicious files on your system but maybe not. This is what happens when you executed whatever it was

<https://imgur.com/a/MubO6EX>

Might want to double check your system friend unless you are aware that these things have happened

P.s > depends who you downloaded limeRat from. If its from nyancats' github page then its clean, if you downloaded from someone else it is most definitely NOT. I dont see why this has created a firewall exclusion or what its for so I doubt you have the legitimate version

SIM-3487621 - April 7, 2020, 9:04 am

(Apr 7, 2020 03:48 AM)Yseurk Wrote: [\[CITE\]](#) You intentionally ran a malware on your computer and then you come here to ask help ?

You are looking for help in the white hat section while you are attempting for black hat activities ?!!

May your computer die because of your stupidityHow do you know this was intended for blackhat activities? Think before you post something

(Apr 7, 2020 08:49 AM)killmenow Wrote: [\[CITE\]](#) Looks to me like you actually are infected and that you may have malicious files on your system but maybe not. This is what happens when you executed whatever it was

<https://imgur.com/a/MubO6EX>

Might want to double check your system friend unless you are aware that these things have happened

P.s > depends who you downloaded limeRat from. If its from nyancats' github page then its clean, if you downloaded from someone else it is most definitely NOT. I dont see why this has created a firewall exclusion or what its for so I doubt you have the legitimate versionI did download it from nyan cats github page and did click on a button to add an exclusion to my firewall.

Astonished - April 7, 2020, 5:30 pm

(Apr 7, 2020 09:04 AM)InfamousalGT Wrote: [\[CITE\]](#) How do you know this was intended for blackhat activities? Think before you post something

I did download it from nyan cats github page and did click on a button to add an exclusion to my firewall.

Then you're all good, nyan cat is a reputable member and creator of tools. All most all are widely used by script kiddies and people learning to create their own tools. You're all good

Luffy-_- - April 8, 2020, 2:35 pm

I'm not an expert or something but i have a small suggestion for you, i don't know if [Bastille](#) agree with me , everytime you download a suspicious file try to run it on a virtual machine first

Bastille - April 8, 2020, 2:38 pm

(Apr 8, 2020 02:35 PM)Luffy-_- Wrote: [\[CITE\]](#) I'm not an expert or something but i have a small suggestion for you, i don't know if [Bastille](#) agree with me , everytime you download a suspicious file try to run it on a virtual machine first

Thanks to mention me on a white hat thread, however I'm not gonna help OP

Always useful to read the previous posts on a thread, please check above

Knautschtabak - April 8, 2020, 11:19 pm

(Apr 7, 2020 12:28 AM)InfamousalGT Wrote: [\[CITE\]](#) [Virus Total scan](#)

[Virus total scan of some kind of program it opened](#)

Its a open source rat. Anything suspicious in there?

Well, you can weaken security of your system by running it, even if there is no backdoor in the code.

For this one the install locations depend on the settings:

--> installation routine is here:

https://github.com/NYAN-x-CAT/Lime-RAT/blob/master/Project/Client/C_Installation.vb

--> default settings for the client:

https://github.com/NYAN-x-CAT/Lime-RAT/blob/master/Project/Client/C_Settings.vb

The default path of the malware in DEBUG mode is %TEMP%\Lime\Client.exe. Depending on what your settings were, you need to delete the file, then run [Sysinternals Autoruns](#) to remove the run entry (Software\Microsoft\Windows\CurrentVersion\Run\) or the task that references that file. The task is named LimeRAT-Admin no matter the settings.

SIM-3487621 - April 9, 2020, 12:10 am

(Apr 8, 2020 02:35 PM)Luffy-_- Wrote: [\[CITE\]](#) I'm not an expert or something but i have a small suggestion for you, i don't know if [Bastille](#) agree with me , everytime you download a suspicious file try to run it on a virtual machine firstThanks for your suggestion

(Apr 8, 2020 11:19 PM)Knautschtabak Wrote: [\[CITE\]](#) Well, you can weaken security of your system by running it, even if there is no backdoor in the code.

For this one the install locations depend on the settings:

--> installation routine is here:

https://github.com/NYAN-x-CAT/Lime-RAT/blob/master/Project/Client/C_Installation.vb

--> default settings for the client:

https://github.com/NYAN-x-CAT/Lime-RAT/blob/master/Project/Client/C_Settings.vb

The default path of the malware in DEBUG mode is %TEMP%\Lime\Client.exe. Depending on what your settings were, you need to delete the file, then run [Sysinternals Autoruns](#) to remove the run entry (Software\Microsoft\Windows\CurrentVersion\Run\) or the task that references that file. The task is named LimeRAT-Admin no matter the settings.I found no file called "Client.exe" in the path you gave me and i had no task named "LimeRAT-Admin". So im guessing im good? Thanks for your help

Knautschtabak - April 9, 2020, 1:03 am

That's because this is the default path in DEBUG mode. The file you ran likely used something else.

Please download [Sysinternals Autoruns](#). Doubleclick autoruns.exe. Wait for a while until it has read everything. Click "File" -> "Save..." then choose "Save as type: Text (*.txt)" and choose a location where you find it again.

Open the Autoruns log file and copy and paste the text file contents to pastebin.com. Click on "Create a new paste" then copy the link here.

\$hady - April 18, 2020, 5:05 pm

If you think you're infected, boot your computer into safe mode & try to run your anti-virus. Your computer has trouble detecting/removing malware when the file is in use, so safe mode makes your computer use only the necessary things to run your PC. This way if you are indeed infected your anti-virus will be able to catch it and safely remove it.