

Forum: [Hack Forums](#)

Thread: [RATTED](#)

Asag - May 15, 2016, 6:38 pm

So today i paid \$140 for 1.5k loads via paypal. Didnt realize exiled means another form of banned as i rarely get on HF. ANYWAYS long story short he sent me a file saying it was a "file size editor" so the stupidity in me clicked it. Didn't load but realized when i looked to find it, it was gone/melted without me doing anything. I soon realized i have been ratted. So as soon as that happened i have changed my PWs to most of my shit, restored to the farthest restore point. Deleted all my users on my computer and made a new one. Nothing has happened so far but i am afraid to type in any pw on anything because i dont want my personal info stolen. Idk if the RAT is still there, could someone help please to see if i am still infected? Thanks so much in advance.

jakeoh - May 15, 2016, 6:48 pm

If you want to be sure you've gotten rid of it just do a fresh format of your harddrive and reinstall windows.

Asag - May 15, 2016, 7:00 pm

(May 15, 2016 06:48 PM)jakeoh Wrote: [\[CITE\]](#) If you want to be sure you've gotten rid of it just do a fresh format of your harddrive and reinstall windows.

I went to factory reset my computer but i need a windows install disk which i do not have sadly.

?Ñåzg?! - May 15, 2016, 8:07 pm

don't bother factory ressetting your computer for such a small thing just wait until a more knowledgeable member can assist you, and if possible change your passwords on another computer which isn't infected

if you want to check if your still ratted you could view network activity with TCP view
<https://technet.microsoft.com/en-us/sysinternals/tcpview.aspx>

this isn't a fool proof solution the rat could have a rootkit installed or it could be using less network activity then normal

and this was a HF member who did this?

can you also send me the download link to the file that he sent you (send it to me in PM)

Asag - May 15, 2016, 8:18 pm

(May 15, 2016 08:07 PM)?Ñåzg?! Wrote: [\[CITE\]](#) don't bother factory ressetting your computer for such a small thing just wait until a more knowledgeable member can assist you, and if possible change your passwords on another computer which isn't infected

only change passwords that you have typed on your current infected computer (a keylogger probbaly would have recorded them all)

if your infected computer has any passwords saved in your browser then you should change all those passwords as well as they might be compromised

can you also send me the download link to the file that he sent you (send it to me in PM)

I changed all my passwords via my Phone. Would you mind pming me your skype as i cant PM anyone because of my posts. Need 25 to PM people

NiceMe.Me - May 15, 2016, 8:53 pm

(May 15, 2016 07:00 PM)UniversalChillz Wrote: [\[CITE\]](#) I went to factory reset my computer but i need a windows install disk which i do not have sadly.

Go on another computer and get a windows 10 usb made (with the media creation tool)

<https://www.microsoft.com/en-us/software-download/windows10/>

Asag - May 15, 2016, 9:01 pm

(May 15, 2016 08:53 PM)NiceMe.Me Wrote: [\[CITE\]](#) Go on another computer and get a windows 10 usb made (with the media creation tool)

Thanks ill give this a go, just got help from naz and by the sounds of it im not ratted but i am not entirely sure and a little eerie. Ill still take suggestions if anyone has any. Thanks

?Ñâzg?! - May 15, 2016, 9:23 pm

(May 15, 2016 09:01 PM)UniversalChillz Wrote: [\[CITE\]](#) Thanks ill give this a go, just got help from naz and by the sounds of it im not ratted but i am not entirely sure and a little eerie. Ill still take suggestions if anyone has any. Thanks

yeah I analysed the malware in my virtual machine

I told the OP what process the malware made including network activity so that he can recognize if it's running on his PC

if anyone want's to take a look at the malware you can PM me I can send you a link (should make it easier to use farbar recovery or OTL)

here are some screenshots of the malware in startup

Spoiler [\(Click to View\)](#)

screenshot of the malware process

Spoiler [\(Click to View\)](#)

the member who infected him was

<https://hackforums.net/member.php?action=profile&uid=3080855>

here is a virustotal sample

<https://www.virustotal.com/en/file/0dc9be57efa39c98380bc483c2e7656baa6929b8a7bfc5686f71f5521ba60aaa/analysis/1463386059/>

here is a static and dynamic analysis (not as accurate as I wanted it to be)

<https://malwr.com/analysis/M2I2MGViZDRIOTQxNGE4NWlzMjYzZmY2E0NGQ/>

Will Grigg - May 15, 2016, 9:26 pm

Just have a look at all apps and .exe files that is running on your PC. If you find something that shouldnt be running then try to remove it. Or you could simply download ESET and do a scan on your PC. Most of the crypters on HF gets detected by ESET after 2-3 days of what i heard.

Asag - May 15, 2016, 9:32 pm

(May 15, 2016 09:26 PM)Greta Del Torres Wrote: [\[CITE\]](#) Just have a look at all apps and .exe files that is running on your PC. If you find something that shouldnt be running then try to remove it. Or you could simply download ESET and do a scan on your PC. Most of the crypters on HF gets

detected by ESET after 2-3 days of what i heard.

Ran ESET after along with some other programs but i had to pay to delete all the threats detected. Ran process hacker and tried looking for CasPol and RegAsm since thats what naz had me look for. Didnt find anything. So i hope everything is all good.