

Forum:[Hack Forums](#)

Thread: [Keylogged, Paypal Hacked, Steam Hacked, and Skype banned for Security.](#)

Berry Fusion - November 3, 2014, 5:50 pm

So I have three separate accounts, three separate usernames, three separate passwords. All three hacked within the hour when I ate dinner. I lost 140\$ on Paypal, I'm busy recovering my Steam, and unlocking my Skype. I just sent a ticket about the money on Paypal, but as of now my main concern is getting rid of whatever virus or whatever this is. I never gave anyone these passwords, and they are good passwords (Multiple words, capitalization, and numbers.) That leads me to believe I am keylogged, I need help badly fixing this, please. ?

Orochimaru - November 3, 2014, 5:51 pm

You may have been RATED, do you have any antivirus?

Check your %appdata% and temp folder for random .exe files.

Open task manager and click processes and search up all the ones that are running, if one is an exe and a name you don't recognize, chances are it's also using a lot of CPU then that may be a virus. Right click it and click view file location and then end the process and delete the file. Though it may have persistence and a rootkit setup, get a free trial for an antivirus, until you can also refer to my guide for more help:

<https://hackforums.net/showthread.php?tid=3472081>

Use <http://virustotal.com> to check the files on your PC and next time scan anything that you may not be sure is legitimate on that website.

Good Luck

Aura - November 3, 2014, 5:56 pm

Unfortunately OP the MRT is currently full and don't take new logs. Would you like someone to come over Teamviewer to see if you're infected, or would you like to be redirected to malware removal forums that offers the same kind of professional assistance as the MRT does ?

BLURRYF?CE - November 3, 2014, 5:57 pm

(Nov 3, 2014 06:51 PM)Orochimaru Wrote: [\[CITE\]](#) You may have been RATED, do you have any antivirus?

Check your %appdata% and temp folder for random .exe files.

Open task manager and click processes and search up all the ones that are running, if one is an exe and a name you don't recognize, chances are it's also using a lot of CPU then that may be a virus. Right click it and click view file location and then end the process and delete the file. Though it may have persistence and a rootkit setup, get a free trial for an antivirus, until you can also refer to my guide for more help:

<https://hackforums.net/showthread.php?tid=3472081>

Use <http://virustotal.com> to check the files on your PC and next time scan anything that you may not be sure is legitimate on that website.

Good LuckYeah, pretty much checking your startups in msconfig should do the trick, could also download the [DarkComet RAT Remover](#) in case you got ratted by a wannabe hacker.

Canonsx130 - November 3, 2014, 6:51 pm

(Nov 3, 2014 06:57 PM)vurezo Wrote: [\[CITE\]](#) Yeah, pretty much checking your startups in msconfig should do the trick, could also download the [DarkComet RAT Remover](#) in case you got ratted by a wannabe hacker.

Unfortunately the remover works only on plain server files. Any crypting/modification to the original file will render this remover useless.

Berry Fusion - November 4, 2014, 1:35 pm

(Nov 3, 2014 06:51 PM)Orochimaru Wrote: [\[CITE\]](#) You may have been RATED, do you have any antivirus?

Check your %appdata% and temp folder for random .exe files.

Open task manager and click processes and search up all the ones that are running, if one is an exe and a name you don't recognize, chances are it's also using a lot of CPU then that may be a virus. Right click it and click view file location and then end the process and delete the file. Though it may have persistence and a rootkit setup, get a free trial for an antivirus, until you can also refer to my guide for more help:

<https://hackforums.net/showthread.php?tid=3472081>

Use <http://virustotal.com> to check the files on your PC and next time scan anything that you may not be sure is legitimate on that website.

Good Luck

This did the trick I think, hopefully it doesn't comeback, I'll let you know if it does. Thanks to everyone for the help, I really really appreciate it ?

Aura - November 4, 2014, 2:24 pm

(Nov 4, 2014 02:35 PM)KillerTrooper Wrote: [\[CITE\]](#) This did the trick I think, hopefully it doesn't comeback, I'll let you know if it does. Thanks to everyone for the help, I really really appreciate it ?

This tutorial only covers a small part of malware removal, I still strongly suggest you to get checked at GeeksToGo or BleepingComputer for a complete check-up.

BLURRYF?CE - November 4, 2014, 3:04 pm

(Nov 4, 2014 03:24 PM)Aur? Wrote: [\[CITE\]](#) This tutorial only covers a small part of malware removal, I still strongly suggest you to get checked at GeeksToGo or BleepingComputer for a complete check-up.Or even better, do a clean install!

Aura - November 4, 2014, 3:05 pm

(Nov 4, 2014 04:04 PM)vurezo Wrote: [\[CITE\]](#) Or even better, do a clean install!

Fak u vurezo, I don't want that kind of stuff in this section ?

hashe - November 4, 2014, 3:08 pm

dont use windows use linux u never been hacked :)

Aura - November 4, 2014, 3:12 pm

(Nov 4, 2014 04:08 PM)korsa Wrote: [\[CITE\]](#) dont use windows use linux u never been hacked :)

You don't know anything about hacking, computer protection, *nix nor anything else that is computing related don't you ?

whitewoolyhat - November 9, 2014, 10:12 am

@Aura no need to be mean to him - just because you are a boss at being a white hat xD :D Can you add me on skype or PM me sometime with yours? I am really interested in getting into network security later on in life.

Aura - November 9, 2014, 11:08 am

(Nov 9, 2014 11:12 AM)whitewoolyhat Wrote: [\[CITE\]](#) @Aura no need to be mean to him - just because you are a boss at being a white hat xD :D Can you add me on skype or PM me sometime with yours? I am really interested in getting into network security later on in life.

Network Security is more of -Hyperion's domain if you ask me, not mine. Even Goodies is good at that.

datguy.dev - November 9, 2014, 12:46 pm

(Nov 4, 2014 04:04 PM)vurezo Wrote: [\[CITE\]](#) Or even better, do a clean install!

I agree with that. I wouldn't touch that 'repaired' install with a 10 ft pole after this.

The poor guy just got a bunch of his accounts stolen and his money is in jeopardy. How would you feel if the correction had a fault and this reoccurred?

Aura - November 9, 2014, 4:23 pm

(Nov 9, 2014 01:46 PM)datguy.dev Wrote: [\[CITE\]](#) I agree with that. I wouldn't touch that 'repaired' install with a 10 ft pole after this.

The poor guy just got a bunch of his accounts stolen and his money is in jeopardy. How would you feel if the correction had a fault and this reoccurred?

You mean, if the person that was assisting him in the malware removal process would leave leftovers ? I don't think I've ever seen that happen from someone that has been assisted by the MRT, or on GTG, BC, etc.

datguy.dev - November 9, 2014, 7:45 pm

(Nov 9, 2014 05:23 PM)Aur? Wrote: [\[CITE\]](#) You mean, if the person that was assisting him in the malware removal process would leave leftovers ? I don't think I've ever seen that happen from someone that has been assisted by the MRT, or on GTG, BC, etc.

You said that. ?

I mean, your wrong if you don't consider that their maybe underlying consequences for continuing to use a once compromised drive or install. And I wouldn't want to be that support person or the victim when if it was to happen.

If it was my drive, it would be scrap given the severity of this.

Aura - November 9, 2014, 8:15 pm

(Nov 9, 2014 08:45 PM)datguy.dev Wrote: [\[CITE\]](#) You said that. ?

I mean, your wrong if you don't consider that their maybe underlying consequences for continuing to use a once compromised drive or install. And I wouldn't want to be that support person or the victim when if it was to happen.

If it was my drive, it would be scrap given the severity of this.

These malware removal experts knows their limits and the limits of malware removal as well. If they feel like the malware cannot be removed (like Sality) or that there's still a doubt that its present on the system, they'll warn the user about it and strongly suggest a reinstallation.

datguy.dev - November 9, 2014, 8:37 pm

(Nov 9, 2014 09:15 PM)Aur? Wrote: [\[CITE\]](#) These malware removal experts knows their limits and the limits of malware removal as well. If they feel like the malware cannot be removed (like Sality) or that there's still a doubt that its present on the system, they'll warn the user about it and strongly suggest a reinstallation.

You can go through the steps. But your either 100% certain, or your not at all.

Bet the OP is 100%? I'm not.

Aura - November 10, 2014, 4:06 am

(Nov 9, 2014 09:37 PM)datguy.dev Wrote: [\[CITE\]](#) You can go through the steps. But your either 100% certain, or your not at all.

Bet the OP is 100%? I'm not.

You're* by the way (caught you a few times already).

How do you know ? The OP didn't attempt anything right now to remove the malware if he's infected, so we can't know.

SIM-1984933 - November 10, 2014, 1:21 pm

Lets me Ask you a question.

1.Do you Hit Save Password when you log into a Website like Gmail,Yahoo,ect?

What you can do for possible keyloggers,rats

Open Wireshark and use a filter and use SMTP Or FTP
that's one of many things

Domanate - November 10, 2014, 1:26 pm

Hello! ?

Seems like you have had a rough time, Well that is easy to fix :) The best way I can see you fixing the Security issue, is to wipe your windows and re-install your drivers and change all your passwords, the sooner the better! :) That should stop it, next time. Ensure you are using a good antivirus and do not open anything that is not trusted by a company or user. Security is one of the nations biggest joke, but like I said just have someone wipe windows, also i wouldn't use the same hardrive, it may be infected. Just purchase a new hardrive from amazon, 1 TBs are 50\$ each. I hope this helped you.

I wish you the best of luck!

-Domanate ?

Karnaugh - November 10, 2014, 1:27 pm

Do you want me to help you get the PP money back? I can give them a call (;

Domanate - November 10, 2014, 1:29 pm

(Nov 10, 2014 02:27 PM)Kura Wrote: [\[CITE\]](#) Do you want me to help you get the PP money back? I can give them a call (;

Brother, Violence over the phone will not do anything, any information gathered on the person should be reported to a higher power, police, ect.

That is really nice though to offer ;3 Your a good guy :3 ?

Some offices of the police may be able to figure out who messed with your computer, Hardrive defraging, ect.

Karnaugh - November 10, 2014, 1:31 pm

(Nov 10, 2014 02:29 PM)Domanate Wrote: [\[CITE\]](#) Brother, Violence over the phone will not do anything, any information gathered on the person should be reported to a higher power, police, ect.

That is really nice though to offer ;3 Your a good guy :3 ?

Some offices of the police may be able to figure out who messed with your computer, Hardrive defraging, ect.

What the fuck are you talking about? I am talking about calling PP, you think I'm gonna threat them? -.-

Domanate - November 10, 2014, 4:31 pm

(Nov 10, 2014 02:31 PM)Kura Wrote: [\[CITE\]](#) What the fuck are you talking about? I am talking about calling PP, you think I'm gonna threat them? -.-

No bro that was a miss understanding ?

Aura - November 10, 2014, 8:53 pm

OP, can we have any updates on your current situation?