

Forum:[Hack Forums](#)

Thread: [Just updated my security a bit.](#)

Pharmacist - December 15, 2016, 2:16 pm

So someone backdoored a Visual Studio project that I ran, and got infected by Quasar RAT.

I don't think there was that much damage done, although It got me paranoid enough to get some shit done on my PC.

Here's what I've done so far: Created a VM for all unknown files, period, even images (lol).

Changed my password on all sites I'm registered on.

Installed MalwareBytes Anti-Malware (Premium)

Installed ESET Nod32 Antivirus.

And installed Comodo Firewall.

I've created an encrypted drive using VeraCrypt to store all sensitive files.

I'm thinking about installing DeepFreeze (I think that's the name) and I'm also assuring that this time I set a master password for my browser.

Really sucks getting infected, but it finally made me rethink my security a bit.
Opinions?

aerohack - December 15, 2016, 5:32 pm

I'll built a security setup similar to yours.

I'm in doubt between Kaspersky and Eset.

Pain - December 15, 2016, 5:33 pm

Just curious how did you get infected in the first place?

Sadistic - December 15, 2016, 5:35 pm

Vouch, I was there. There was like 160 infections on one MBAM log

aerohack - December 15, 2016, 5:36 pm

Kaspersky/Eset+ Malwarebytes 3.0 Premium + Zemana Anti-Logger + Comodo.

Pharmacist - December 15, 2016, 6:09 pm

(Dec 15, 2016 06:36 PM)aerohack Wrote: [\[CITE\]](#) Kaspersky/Eset+ Malwarebytes 3.0 Premium + Zemana Anti-Logger + Comodo.

Great recommendation, I didn't have any type of Anti-Keylogging software.

Thank you.

.Astro - December 16, 2016, 11:33 pm

Not sure if any of these programs offer this feature but there are programs out there such as Advanced SystemCare (IOBit I think) that allow you to know when a program has been added to your start up and allows you to cancel the action if you did not allow it.

R?????obert - December 16, 2016, 11:45 pm

Use 2fac for entering your browser

aerohack - December 21, 2016, 11:33 am

(Dec 15, 2016 07:09 PM)Pharmacist Wrote: [\[CITE\]](#) Great recommendation, I didn't have any type of Anti-Keylogging software.

Thank you.

I think about to setup this security combo:

- ESET NOD32 Antivirus + Malwarebytes 3.0 Premium + Grindosoft Anti-Malware + Hitman Pro alert + Zemana AntiLogger Premium + WinPatrol Plus + Comodo Firewall.

But I don't know if 4 Anti-Malwares can cause some kind of conflicts or will this setup will be overkill or all the programs will work well together.

(Dec 15, 2016 07:09 PM)Pharmacist Wrote: [\[CITE\]](#) Great recommendation, I didn't have any type of Anti-Keylogging software.

Thank you.

I think about to setup this security combo:

- ESET NOD32 Antivirus + Malwarebytes 3.0 Premium + Grindosoft Anti-Malware + Hitman Pro alert + Zemana AntiLogger Premium + WinPatrol Plus + Comodo Firewall.

But I don't know if 4 Anti-Malwares can cause some kind of conflicts or will this setup will be overkill or all the programs will work well together.

(Dec 15, 2016 07:09 PM)Pharmacist Wrote: [\[CITE\]](#) Great recommendation, I didn't have any type of Anti-Keylogging software.

Thank you.

I think about to setup this security combo:

- ESET NOD32 Antivirus + Malwarebytes 3.0 Premium + Grindosoft Anti-Malware + Hitman Pro alert + Zemana AntiLogger Premium + WinPatrol Plus + Comodo Firewall.

But I don't know if 4 Anti-Malwares can cause some kind of conflicts or will this setup will be overkill or all the programs will work well together.

EliteTM - December 21, 2016, 2:28 pm

Have you considered securing the browser as well? I'm assuming your running some kind of ad blocker. You'd also want to get an extension like noScript (for Firefox)/ScriptBlock (for Chrome) to stop those annoying popup dialog. If your really paranoid, you'd also keep the browser on a VM. I'd also get a VPN for your router (if you have a router that supports VPNs) so none of your traffic can be logged, make sure you do your research and find a good VPN provider that doesn't log (Private Internet Access I know doesn't log). I honestly don't think you'll need DeepFreeze, it'll become pretty annoying having to freeze and unfreeze the computer if you want to save any changes you made. Also another thing is you don't want to just have your sensitive files backed up on your computer alone, you also want them stored on a NAS (Network Attached Storage) encrypted of course or store them on a second drive/computer. So even if some zero day is able to find some way to bypass all the secure measures you placed, you won't lose the most important thing of them all,

your files.

Canonsx130 - December 21, 2016, 8:39 pm

A special software against keyloggers is not really required if you already have a realtime protection system such as ESET running along with Malwarebytes. Couple more things you can do:

Just make sure all your plugins on your browser is updated. Firefox:

<https://www.mozilla.org/en-US/plugincheck/>

Uninstall stuffs like Java, if you do not use it.

Replace Adobe products like Adobe Reader with something like Foxit Reader which is less prone to vulnerabilities.

Make sure you have 2fa activated on all your accounts.

It is better to avoid several malware protection softwares. You already have a firewall, ESET, and Malwarebytes. The only additional thing I'd suggest is maybe Malwarebytes AntiExploit:

<https://www.malwarebytes.com/antiexploit/> Anything more, I'd call it overkill.