

Forum:[Hack Forums](#)

Thread: [Friend used sketchy stuff](#)

Kaxon - April 14, 2018, 12:04 pm

My friend used a few sketchy applications and found himself with permission errors and bitcoin miners detected in Malwarebytes. I am hoping to see if there is anything more that Malwarebytes couldn't detect as well as fix any problems he may still have.

I have made him run r-kill and frst. Here are his logs:

FRST.txt: <https://pastebin.com/EmRZSg65>

Addition.txt: <https://pastebin.com/Z1U8JNN3>

dragonking - April 16, 2018, 12:03 pm

If he has valuable or sensitive information on his machine, he should run his PC in safe mode with no networking, backup all important files to an external HDD, and the reinstall his OS. This is to ensure data integrity. If this isn't an option let me know and I can give you a few other tips that may help.

Kaxon - April 16, 2018, 12:35 pm

(Apr 16, 2018 12:03 PM)dragonking Wrote: [\[CITE\]](#) If he has valuable or sensitive information on his machine, he should run his PC in safe mode with no networking, backup all important files to an external HDD, and the reinstall his OS. This is to ensure data integrity. If this isn't an option let me know and I can give you a few other tips that may help.

The sticky thread said I shouldn't listen to people saying to reinstall OS. And you have only 14 rep so I think I'll pass on that idea for now. Thanks anyway.

dragonking - April 16, 2018, 12:45 pm

Haha ok dude. You do you.

SecurityCult - April 18, 2018, 8:43 am

Well if you haven't been able to manually remove it you should really consider what Dragonking has said.

Boot into safemode with no networking back everything up that's important to him and reinstall OS unless you want to live with 100% CPU usage from a miner.

If its a rootkit then you'll have even more fun trying to remove it manually.