

Forum:[Hack Forums](#)

Thread: [Password changed](#)

TheDFighter - December 8, 2014, 1:41 am

I'm making this thread for a friend, as his only solution to a potential virus is a reformat, and he refuses to go in this forum, because of them name... (he thinks he will get hacked)

So two days ago he was stupid enough to actually download a steam stealer, but luckily he got his items back, and formatted his pc.

The next day he received a facebook message from a stranger, telling him to go on a link. He followed the link, and realised that it was a scam, and closed the site without doing anything on it.

Today a lot of his passwords are changed.

What are the chances he is infected?

Lexica - December 8, 2014, 1:42 am

Could be good depending on the site he visited, it could have been a JDB.

TheDFighter - December 8, 2014, 2:51 am

Seems i'll have to do some cleanup then, could anyone guide me?

Aura - December 8, 2014, 4:04 am

Can you PM me the link he clicked on, just to see if it was really infected with a JDB or other exploit ?

TheDFighter - December 8, 2014, 6:06 am

I would be happy to do so, but i'm not allowed to send pm's atm :/

EDIT: it seems that it was a file, and not a link. He just thought it was a link, since it opened a fake browser window disguised as a fake facebook. The file has been deleted, so i can't report it sorry :/

Aura - December 8, 2014, 10:39 am

(Dec 8, 2014 07:06 AM)TheDFighter Wrote: [\[CITE\]](#) I would be happy to do so, but i'm not allowed to send pm's atm :/

EDIT: it seems that it was a file, and not a link. He just thought it was a link, since it opened a fake browser window disguised as a fake facebook. The file has been deleted, so i can't report it sorry :/
He opened the file right ?

Well, it's hard to tell you friend what to do and ask for real-time report if he doesn't sign up here.

TheDFighter - December 9, 2014, 1:47 am

I decided to use Hyperions tutorial and the Tron script, that hyperion reviewed, on my friends pc, and he should be all clean now. It also seems he was using multiple antiviruses at once, because he thought more=better :x

Aura - December 9, 2014, 4:53 am

(Dec 9, 2014 02:47 AM)TheDFighter Wrote: [\[CITE\]](#) I decided to use Hyperions tutorial and the Tron

script, that hyperion reviewed, on my friends pc, and he should be all clean now. It also seems he was using multiple antiviruses at once, because he thought more=better :x

Doesn't work that way.

Which Antivirus products does he have? I'll tell you which one he should keep.

TheDFighter - December 9, 2014, 5:42 am

He had AVG, Norton and Kaspersky installed. Also some avast error popped up, from an unclean uninstall when we booted first time.

Aura - December 9, 2014, 5:45 am

(Dec 9, 2014 06:42 AM)TheDFighter Wrote: [\[CITE\]](#) He had AVG, Norton and Kaspersky installed. Also some avast error popped up, from an unclean uninstall when we booted first time.

If the Kaspersky licence is still active, uninstall AVG, Norton and avast! (If you don't see it installed, use its clean up tool). Start with that.

TheDFighter - December 9, 2014, 5:57 am

Okay, i removed everything but kaspersky now. There's still a trial license active for kaspersky.

Aura - December 9, 2014, 5:58 am

(Dec 9, 2014 06:57 AM)TheDFighter Wrote: [\[CITE\]](#) Okay, i removed everything but kaspersky now. There's still a trial license active for kaspersky.

Alright. Do you still get the avast! error pop-up on boot or not ?

TheDFighter - December 9, 2014, 6:01 am

No, i don't get the error message anymore

Aura - December 9, 2014, 1:26 pm

(Dec 9, 2014 07:01 AM)TheDFighter Wrote: [\[CITE\]](#) No, i don't get the error message anymore While we're at it, can you tell your friend to follow the instructions here:

[\[BHCPU\] Program/Software advices and recommendations Help Desk](#) by [Aur?](#)

And post the URL to the Pastebin/Privatepaste paste here or there?

TheDFighter - December 9, 2014, 1:29 pm

Yeah i Can do that. I Will have to wait till tommorow though, as it's 10:30 pm here atm

Aura - December 9, 2014, 1:30 pm

(Dec 9, 2014 02:29 PM)TheDFighter Wrote: [\[CITE\]](#) Yeah i Can do that. I Will have to wait till tommorow though, as it's 10:30 pm here atm

All good, I'll be online tomorrow as well.

BlackHat420 - December 10, 2014, 9:28 pm

Hi new to this section I see your the top dog here :D

Well here is my pastebin:

<http://pastebin.com/UaGESaM0>

Is it normal to see so many Microsoft stuff?

And thanks for your help :)

Aura - December 10, 2014, 9:44 pm

(Dec 10, 2014 10:28 PM)BlackHat420 Wrote: [\[CITE\]](#) Hi new to this section I see your the top dog here :D

Well here is my pastebin:

<http://pastebin.com/UaGESaM0>

Is it normal to see so many Microsoft stuff?

And thanks for your help :)

Please post your log in my thread that I linked a few posts above. Do not hijack this one. Thank you.

TheDFighter - December 11, 2014, 10:16 am

Okay, i have the pastebin with the minitoolbox logs, but i can't post links, as i don't have 50 posts, what do? :x

Aura - December 11, 2014, 10:49 am

(Dec 11, 2014 11:16 AM)TheDFighter Wrote: [\[CITE\]](#) Okay, i have the pastebin with the minitoolbox logs, but i can't post links, as i don't have 50 posts, what do? :x

You can post links if you add spaces in it, so it's good. Do it.

TheDFighter - December 11, 2014, 11:09 am

Okay, here's the link then :) [pastebin.com/c7YfnudA](#)