

Forum:[Hack Forums](#)

Thread: [\[URGENT\] Check up required, potentially ratted \[WILL PAY\]](#)

Unident - November 26, 2018, 1:46 pm

So I believe I may be infected, I've been experiencing weird mouse malfunctions such as release of click without releasing, example of this would be

Code I click scrollbar & whilst scrolling up my mouse no longer becomes active on that element and instead of scrolling the bar, the mouse just moves up the screen
or another example would be

Code I click & hold a form to move it, but whilst moving it my mouse no longer becomes activate within that form and just moves the mouse instead of the form

I've also been experiencing screen blackouts that last milliseconds & most recently I was browsing facebook, when a ton of old message chat boxes popped up from years ago? It could potentially be a facebook bugging out, but I've never experienced that before and these messages weren't in anyway active for the past year..

I don't know how I would be infected though as I haven't downloaded anything out of the ordinary, the only thing I've downloaded which may have lead to potential infection is virtual box, which I then use to run remmina and connect remotely to a virtual private server (which could be infected) however, they would then have to not only escape remote desktop to infect the host, but also escape virtualbox to infect the main host..

I understand there's potential 0days which may lead to infections through open ports etc, but as far as I'm aware everything I run is uptodate and isn't publicly vulnerable.

Would appreciate any guidance/support & the correct route to take for a check up.

When I formatted previously, I used windows 10 " Reset this PC " & the " Remove everything & reinstall OS " option.

Tilcayo - November 26, 2018, 2:03 pm

(Nov 26, 2018 02:46 PM)Unident Wrote: [\[CITE\]](#) I've also been experiencing screen blackouts that last milliseconds & most recently I was browsing facebook, when a ton of old message chat boxes popped up from years ago? It could potentially be a facebook bugging out, but I've never experienced that before and these messages weren't in anyway active for the past year..

Have you checked recent device logins on facebook? Go to settings, then security and login, then you should see a section called "where you're logged in"

which lists all devices and specific locations where your facebook has been logged in from, if you notice anything unusual like some random login location that you don't recognise or maybe even another country, then it's very likely someones logged into your facebook account! If you do see this, hover your mouse over the location and it will show you the IP address of the person that logged in. Hope that helps! ?

Edit: If you find an IP, google it, get all the information you can on that IP so you know whether its a VPN IP or someones home internet, it might even tell you the VPN name.

Unident - November 26, 2018, 2:13 pm

(Nov 26, 2018 03:03 PM)Flexyy Wrote: [\[CITE\]](#) Have you checked recent device logins on facebook? Go to settings, then security and login, then you should see a section called "where you're logged in"

which lists all devices and specific locations where your facebook has been logged in from, if you notice anything unusual like some random login location that you don't recognise or maybe even another country, then it's very likely someones logged into your facebook account! If you do see this, hover your mouse over the location and it will show you the IP address of the person that logged in. Hope that helps! ?

Edit: If you find an IP, google it, get all the information you can on that IP so you know whether its a VPN IP or someones home internet, it might even tell you the VPN name.

Yes I done that as soon as I noticed message boxs were popping up, but the only connected device was my own.. So then I logged in via another device and opened multiple chat boxs to see if it effected my other session, but it didn't the message boxs I opened on the other device didn't open on the regular device. So it would have had to been through the current device I'm using..

Tilcayo - November 26, 2018, 2:20 pm

(Nov 26, 2018 03:13 PM)Unident Wrote: [\[CITE\]](#) Yes I done that as soon as I noticed message boxs were popping up, but the only connected device was my own.. So then I logged in via another device and opened multiple chat boxs to see if it effected my other session, but it didn't the message boxs I opened on the other device didn't open on the regular device. So it would have had to been through the current device I'm using..

Do you leave your facebook logged in while you're afk for long hours? You could be infected, do you have an AV? Worth maybe installing Eset and using the month trial for a scan just to check.

Unident - November 26, 2018, 2:33 pm

(Nov 26, 2018 03:20 PM)Flexyy Wrote: [\[CITE\]](#) Do you leave your facebook logged in while you're afk for long hours? You could be infected, do you have an AV?

I have malwarebytes and windows defender (i know basic), but unfortunately FUD is a regular occurrence this day as crypters are easily purchased, so it's more than likely not going to be detected regardless of what anti virus I use.

But I may not be infected, I may just be experiencing malfunctions and assuming the worst possible scenario, so that's why I'm here so hopefully someone will guide me through the processes of atleast detecting whether I'm infected.

?Apocalypse - November 26, 2018, 2:35 pm

I can take a look vía TV just let me know

Unident - November 26, 2018, 2:43 pm

(Nov 26, 2018 03:35 PM)?Apocalypse Wrote: [\[CITE\]](#) I can take a look vía TV just let me know I'm not looking for direct access to my PC, I'm looking for a individual to step me through the process of detecting the potential infection, similar to how the OFFICIAL white hat team does it.. Which hopefully they respond to be honest.

?Apocalypse - November 26, 2018, 2:44 pm

(Nov 26, 2018 03:43 PM)Unident Wrote: [\[CITE\]](#) I'm not looking for direct access to my PC, I'm looking for a individual to step me through the process of detecting the potential infection, similar to how the OFFICIAL white hat team does it.. Which hopefully they respond to be honest.

It's done via Team Viewer

Tilcayo - November 26, 2018, 2:46 pm

(Nov 26, 2018 03:33 PM)Unident Wrote: [\[CITE\]](#) FUD is a regular occurrence this day as crypters are

easily purchased, so it's more than likely not going to be detected regardless of what anti virus I use. That's true, but the majority of people that buy other peoples software like crypter's are skids, and they don't stay fud for long anyway unless they're private crypters.. its people that crypt the malware themselves you want to be worried about, not the ones that buy them. It's always worth downloading eset or some other big vendor just incase! I wish you the best of luck getting it sorted, i'm sure someone here will take a look.

Unident - November 26, 2018, 2:48 pm

(Nov 26, 2018 03:44 PM)?Apocalypse Wrote: [\[CITE\]](#) It's done via Team Viewer
It's really not, it's done through running programs such as FRST, Rogue Killer, Rkill etc.. and examining the reports.

Check any response from whitehat based individuals.. I'm not new to the scene, unfortunately I know the steps slightly just not the detection route.

(Nov 26, 2018 03:46 PM)Flexyy Wrote: [\[CITE\]](#) That's true, but the majority of people that buy other peoples software like crypter's are skids, and they don't stay fud for long anyway unless they're private crypters.. its people that crypt the malware themselves you want to be worried about, not the ones that buy them. It's always worth downloading eset or some other big vendor just incase! I wish you the best of luck getting it sorted, i'm sure someone here will take a look.

Yeah a lot RATs also push updates though to prevent crypter becoming outdated, so it's a difficult one.. thanks for the input though and yes hopefully someone will be able to help me detect :).

?Apocalypse - November 26, 2018, 2:50 pm

(Nov 26, 2018 03:48 PM)Unident Wrote: [\[CITE\]](#) It's really not, it's done through running programs such as FRST, Rogue Killer, Rkill etc.. and examining the reports.

Check any response from whitehat based individuals.. I'm not new to the scene, unfortunately I know the steps slightly just not the detection route.

Yeah a lot RATs also push updates though to prevent crypter becoming outdated, so it's a difficult one.. thanks for the input though and yes hopefully someone will be able to help me detect :).

Did you post a report somewhere?

Unident - November 26, 2018, 3:25 pm

(Nov 26, 2018 03:50 PM)?Apocalypse Wrote: [\[CITE\]](#) Did you post a report somewhere?

No I'm waiting on someone to guide me through the process as I don't want to just assume I'm doing it correctly.

Unident - December 2, 2018, 1:07 am

bump still need help, would appreciate if any whitehat can spare some time.