

Forum:[Hack Forums](#)

Thread: [What is the quickest way to know if i am in a Botnet :D](#)

SpookyD - May 14, 2020, 8:42 am

I am not the most tech savvy when it comes to this.

Can someone tell me what tools i can run on my PC to check if there are any suspicious connections or files running on my PC?

I am quite sure there are, should i just run an anti virus check? (not really sure that's the way to go)

I must be your slave huh, you don't wanna let me know a way out :P

3xploit - May 14, 2020, 11:36 am

Download Process Hacker and check the network tab. You will see a list of processes that are connected to the internet and also where the connection is going + there are tools like whois lookup included.

Sinistros - May 14, 2020, 11:44 am

(May 14, 2020 08:42 AM)SpookyD Wrote: [\[CITE\]](#) I am not the most tech savvy when it comes to this.

Can someone tell me what tools i can run on my PC to check if there are any suspicious connections or files running on my PC?

I am quite sure there are, should i just run an anti virus check? (not really sure that's the way to go)

I must be your slave huh, you don't wanna let me know a way out :P

I guess if you are a victim of a botnet, the malware has a startup feature if it don't have rootkit feature check registry entries for startup and startup folder.

Feel free to conatct me if you need more help

protecteur6 - May 14, 2020, 12:48 pm

(May 14, 2020 08:42 AM)SpookyD Wrote: [\[CITE\]](#) I am not the most tech savvy when it comes to this.

Can someone tell me what tools i can run on my PC to check if there are any suspicious connections or files running on my PC?

I am quite sure there are, should i just run an anti virus check? (not really sure that's the way to go)

I must be your slave huh, you don't wanna let me know a way out :P

if you think you are infected by a payload tchek download process hacker and see the runing process and close every thing (browsers....) and open process hacker and then look up for name like chrome ore win.exe or Comsurgateor even svchost)

then tchek your start up do windows+r and then type %appdata% and see if there is any suspecious program you dont use delete it ifyou delete it and you restart your computerand you still find it download ccleaner and delte it from there in safe mode on windows and then you will delete it also if you suspect a program right click open folder location and delete it from there if its a miner

do the same and run nod av or advanced system care

if you are looking for best av: is you

if you need help: windows defender and nod are the best for now

SpookyD - May 14, 2020, 3:45 pm

(May 14, 2020 11:36 AM)????? Wrote: [\[CITE\]](#) Download Process Hacker and check the network tab. You will see a list of processes that are connected to the internet and also where the connection is going + there are tools like whois lookup included.

(May 14, 2020 11:44 AM)Sinistros Wrote: [\[CITE\]](#) I guess if you are a victim of a botnet, the malware has a startup feature if it don't have rootkit feature check registry entries for startup and startup folder.

Feel free to contact me if you need more help

Thanks for the answers guys. i am too toasted right now, i am on "READ ONLY" lol

But tomorrow as i wake up i will take the time to finally understand better what is going on on this PC.

(May 14, 2020 12:48 PM)protecteur6 Wrote: [\[CITE\]](#) if you think you are infected by a payload tchek download process hacker and see the running process and close every thing (browsers....) and open process hacker and then look up for name like chrome ore win.exe or Comsurgateor even svchost)

then tchek your start up do windows+r and then type %appdata% and see if there is any suspicious program you dont use delete it if you delete it and you restart your computer and you still find it download ccleaner and delete it from there in safe mode on windows and then you will delete it also if you suspect a program right click open folder location and delete it from there if its a miner do the same and run nod av or advanced system care

if you are looking for best av: is you

if you need help: windows defender and nod are the best for now

Not sure why it left you quote out, and i couldn't edit it in, so Thanks :)

protecteur6 - May 14, 2020, 7:23 pm

(May 14, 2020 03:45 PM)SpookyD Wrote: [\[CITE\]](#) Thanks for the answers guys. i am too toasted right now, i am on "READ ONLY" lol

But tomorrow as i wake up i will take the time to finally understand better what is going on on this PC.

Not sure why it left you quote out, and i couldn't edit it in, so Thanks :)

np :D

VisualSoft - May 15, 2020, 3:57 am

Just check for suspicious start-up options over there and you will be good to go.

SpookyD - May 15, 2020, 3:59 am

(May 15, 2020 03:57 AM)VisualSoft Wrote: [\[CITE\]](#) Just check for suspicious start-up options over there and you will be good to go.

Please explain, what is over there?

I just downloaded process hacker and about to start digging in a little, if there is something i shouldn't miss please shed some light on it :)

VisualSoft - May 15, 2020, 5:01 am

download Autoruns.exe from the internet and check yourself if there is any program in the start-up which you are not aware of?

remove start-up from Autoruns and you are done.

SpookyD - May 15, 2020, 5:05 am

(May 15, 2020 05:01 AM)VisualSoft Wrote: [\[CITE\]](#) download Autoruns.exe from the internet and check yourself if there is any program in the start-up which you are not aware of?

remove start-up from Autoruns and you are done.

Thanks mate, it was nowhere mentioned anywhere else in the thread, so i didn't figure why you thought its obvious i should do that ;)

Teleperformance - May 18, 2020, 5:59 am

Download Pi-Hole and filter out all of the requests going out of your PC, just filter them out by your IP, once you notice some strange traffic post it here so we can try to ping that lucky person ;3