

## Forum:[Hack Forums](#)

Thread: [RAT on my PC, survived windows reset, any help?](#)

**Flaws.** - October 29, 2021, 4:42 am

Holla,

I've somehow managed to get infected with a RAT on one of my machines, the guys just moving my mouse about and keeps trying to go to different websites. Its pretty funny. But, this gets mad now because whatever RAT it is, I reset windows (But kept files), and the RAT is still there and hes still fucking around on my machine.

Oh, and ESET and Malwarebytes both cant detect anything.

Anything anyone can do to help?

**Allelujah** - October 29, 2021, 8:02 am

What OS are you on? If there's an upgrade, like from macOS 10.14.6 to 11.6 you may have better chances of finding the RAT after upgrading. You could also try completely erasing everything as much as that sucks. If you have a back up you may be able to pull files from that rather than restoring everything.

**Bastille** - October 29, 2021, 1:52 pm

Hi buddy,

Could you save your files and try a full reinstall ?

**spyglass** - October 29, 2021, 2:01 pm

(Oct 29, 2021 04:42 AM)Flaws. Wrote: [\[CITE\]](#) Holla,

I reset windows (But kept files), and the RAT is still there and hes still fugging around on my machine.

Oh, and ESET and Malwarebytes both cant detect anything.

Anything anyone can do to help?

Hi Flaws.,

This is your problem... (But kept files)

When you do a reinstall make sure to also format the drive you are installing windows on.

**Sigma** - October 29, 2021, 3:04 pm

(Oct 29, 2021 01:52 PM)Yseurk Wrote: [\[CITE\]](#) Hi buddy,

Could you save your files and try a full reinstall ?

This would solve your issue.

I would love to see an FRST scan as well if you can provide that.

**tripac** - October 29, 2021, 3:17 pm

Im not expert at this but try running TRON script <https://github.com/bmrf/tron>

**Flaws.** - October 30, 2021, 3:15 am

(Oct 29, 2021 03:04 PM)Sigma Wrote: [\[CITE\]](#) This would solve your issue.

I would love to see an FRST scan as well if you can provide that.

Link me to whatever you want me to run or do on the machine and ill happily do it for you, really keen to see what it is

(Oct 29, 2021 08:02 AM)Allelujah Wrote: [\[CITE\]](#) What OS are you on? If there's an upgrade, like from macOS 10.14.6 to 11.6 you may have better chances of finding the RAT after upgrading. You could also try completely erasing everything as much as that sucks. If you have a back up you may be able to pull files from that rather than restoring everything.

I'm running windows 10, latest build, cant upgrade to 11 sadly for the stupid reason of it not supporting an i7 6700k

(Oct 29, 2021 01:52 PM)Yseurk Wrote: [\[CITE\]](#) Hi buddy,

Could you save your files and try a full reinstall ?

I can indeed, but first i think ill get scans out of the way and get some data on what it is

(Oct 29, 2021 02:01 PM)spyglass Wrote: [\[CITE\]](#) Hi Flaws.,

This is your problem... (But kept files)

When you do a reinstall make sure to also format the drive you are installing windows on.

Clear and understood buddy, will do

**Sigma** - October 30, 2021, 6:04 am

(Oct 30, 2021 03:15 AM)Flaws. Wrote: [\[CITE\]](#) Link me to whatever you want me to run or do on the machine and ill happily do it for you, really keen to see what it is

I'm running windows 10, latest build, cant upgrade to 11 sadly for the stupid reason of it not supporting an i7 6700k

I can indeed, but first i think ill get scans out of the way and get some data on what it is

Clear and understood buddy, will do

<https://www.bleepingcomputer.com/download/farbar-recovery-scan-tool/>

**Flaws.** - October 30, 2021, 6:41 am

(Oct 30, 2021 06:04 AM)Sigma Wrote: [\[CITE\]](#)

<https://www.bleepingcomputer.com/download/farbar-recovery-scan-tool/>

Understood, will run it on Monday

**Jinu** - October 30, 2021, 1:17 pm

A fresh install without old files will resolve your problems very easily.

**Maadcat** - October 30, 2021, 1:49 pm

Clean install and do not keep your files (restore), format HDD. Best, if you can, have OS install file in

a boot usb key and format by zero your HD and (only after) boot with the key. Sometimes, malware can have trace on bios.

Is possible your file is corrupted too, to be sure, dont save. But you can first try with save and you will see...

**Flaws.** - November 1, 2021, 4:54 am

So, I've just done a full reset with a windows USB, didn't choose to save any files what so ever, the cunt is still here moving my mouse around and typing random shit.

Luckily I have managed to get FRST scans of both before the reset, and after. Will be uploading shortly

**Sigma** - November 1, 2021, 6:09 am

(Nov 1, 2021 04:54 AM)Flaws. Wrote: [\[CITE\]](#) So, I've just done a full reset with a windows USB, didn't choose to save any files what so ever, the cunt is still here moving my mouse around and typing random shit.

Luckily I have managed to get FRST scans of both before the reset, and after. Will be uploading shortly

That is strange, a full reset should have easily done the trick because it deletes all system files and restores them. Yes, let me check those ASAP!

**Flaws.** - November 1, 2021, 1:18 pm

(Nov 1, 2021 12:08 PM)lasski Wrote: [\[CITE\]](#) You should try disconnecting from internet so he won't be able to acces to your PC. just a small tips so he won't be able to mess with you anymore. That is what i have been doing my guy

(Nov 1, 2021 06:09 AM)Sigma Wrote: [\[CITE\]](#) That is strange, a full reset should have easily done the trick because it deletes all system files and restores them. Yes, let me check those ASAP!  
Here you go dude

<http://www.filedropper.com/scans>

I've included scans before and after the reset also

**Cyber Rick** - November 1, 2021, 1:20 pm

You obviously didn't remove all files and fully reset windows. If you did, then it would be a fresh install of windows and wouldn't have malware on it...

The only chance of that happening is if you did do a full reset but put the RAT back on ur PC from lets say a backup of your files.

**Flaws.** - November 1, 2021, 1:24 pm

(Nov 1, 2021 01:20 PM)SIM-4395330 Wrote: [\[CITE\]](#) You obviously didn't remove all files and fully reset windows. If you did, then it would be a fresh install of windows and wouldn't have malware on it...

The only chance of that happening is if you did do a full reset but put the RAT back on ur PC from lets say a backup of your files.

My good friend, have you ever heard of a rootkit?

**Cyber Rick** - November 1, 2021, 2:11 pm

(Nov 1, 2021 01:24 PM)Flaws. Wrote: [\[CITE\]](#) My good friend, have you ever heard of a rootkit? Obviously I know more about rootkits than you...use Google before you spew verbal diarrhea in a quote to me.

Google: "will a rootkit survive a full reformat"

Answer: "Certainly the only way to be 100% sure that a rootkit no longer exists on a machine is to reformat the hard drives and reinstall the OS."

If a proper OS reinstall was done and the hard drives were reformatted to remove all the files properly (which windows reinstall does on its own if done properly) then it is IMPOSSIBLE for there to still be a RAT on the computer unless there is a new exploit where you can somehow embed the RAT onto hardware such as the RAM stick, which again would be virtually impossible.

Source of my information: I have my masters in networking and IT security + Using basic Googleing skills which anyone in IT should have...

I find it unbelievable that someone who downloaded and ran a RAT on his computer is trying to tell me how viruses work....

**Edge of Nowhere** - November 1, 2021, 2:17 pm

(Nov 1, 2021 02:11 PM)SIM-4395330 Wrote: [\[CITE\]](#) Obviously I know more about rootkits than you...use Google before you spew verbal diarrhea in a quote to me.

Google: "will a rootkit survive a full reformat"

Answer: "Certainly the only way to be 100% sure that a rootkit no longer exists on a machine is to reformat the hard drives and reinstall the OS."

If a proper OS reinstall was done and the hard drives were reformatted to remove all the files properly (which windows reinstall does on its own if done properly) then it is IMPOSSIBLE for there to still be a RAT on the computer unless there is a new exploit where you can somehow embed the RAT onto hardware such as the RAM stick, which again would be virtually impossible.

Source of my information: I have my masters in networking and IT security + Using basic Googleing skills which anyone in IT should have...

I find it unbelievable that someone who downloaded and ran a RAT on his computer is trying to tell me how viruses work....

Depends on the format method, the standard windows format doesn't really format. It just writes on a certain part of the drive.

That means, sure rootkits are gone, but a bootkit will not.

That's why you always run a tool like Darik's Boot and Nuke. Basically writes random data on the entire drive and makes sure the MBR is cleared as well.

P.S. Don't shit on people for trying to learn. You started somewhere at some point in time.

**Cyber Rick** - November 1, 2021, 2:56 pm

(Nov 1, 2021 02:17 PM)Machiavelli Wrote: [\[CITE\]](#) Depends on the format method, the standard windows format doesn't really format. It just writes on a certain part of the drive.

That means, sure rootkits are gone, but a bootkit will not.

That's why you always run a tool like Darik's Boot and Nuke. Basically writes random data on the entire drive and makes sure the MBR is cleared as well.

P.S. Don't shit on people for trying to learn. You started somewhere at some point in time.

I have no problem with people learning but when someone tries to be a smartass and correct me with incorrect information, that's when I get annoyed....especially when they are the person having the issue and asking for help in the first place.

In regards to what you are saying, Windows has two options. "Quick Format and Full Format". If you choose quick format, then yes you are correct in that a bootkit could potentially still be there, however choosing the "Full Format" option, does in fact fully format the drive (at least to my understanding) which is why it takes MUCH longer than quick format.

It still isn't a bad idea to use tools to rewrite data over it multiple times but in my opinion, is usually overkill for this scenario.

**Edge of Nowhere** - November 1, 2021, 3:22 pm

(Nov 1, 2021 02:56 PM)SIM-4395330 Wrote: [\[CITE\]](#) I have no problem with people learning but when someone tries to be a smartass and correct me with incorrect information, that's when I get annoyed....especially when they are the person having the issue and asking for help in the first place.

In regards to what you are saying, Windows has two options. "Quick Format and Full Format". If you choose quick format, then yes you are correct in that a bootkit could potentially still be there, however choosing the "Full Format" option, does in fact fully format the drive (at least to my understanding) which is why it takes MUCH longer than quick format.

It still isn't a bad idea to use tools to rewrite data over it multiple times but in my opinion, is usually overkill for this scenario.

May be overkill, but, you never know what people can find on your drive. 4-5 formats later, most people don't remember what they had.

Anyways, off topic now. Sorry about that, I sometimes get caught up in the discussion. haha

**Trojan** - November 2, 2021, 1:39 am

The malware is still in your files don't transfer your files in a fresh install LMAO just get your important things and do a clean install and boom malware is gone.

**Flaws.** - November 2, 2021, 2:13 am

(Nov 1, 2021 02:56 PM)SIM-4395330 Wrote: [\[CITE\]](#) I have no problem with people learning but when someone tries to be a smartass and correct me with incorrect information, that's when I get annoyed....especially when they are the person having the issue and asking for help in the first place.

In regards to what you are saying, Windows has two options. "Quick Format and Full Format". If you choose quick format, then yes you are correct in that a bootkit could potentially still be there, however choosing the "Full Format" option, does in fact fully format the drive (at least to my understanding) which is why it takes MUCH longer than quick format.

It still isn't a bad idea to use tools to rewrite data over it multiple times but in my opinion, is usually overkill for this scenario.

Lmao man I remember when I used to be a little prick too, I've been out of this for time and just come back for a bit of help, love that you and your butt buddy also both neg repped me simply for replying too you, actually hilarious :')

(Nov 1, 2021 02:17 PM)Machiavelli Wrote: [\[CITE\]](#) Depends on the format method, the standard windows format doesn't really format. It just writes on a certain part of the drive.  
That means, sure rootkits are gone, but a bootkit will not.

That's why you always run a tool like Darik's Boot and Nuke. Basically writes random data on the entire drive and makes sure the MBR is cleared as well.

P.S. Don't shit on people for trying to learn. You started somewhere at some point in time.

Cheers for the heads up on Dariks boot and nuke, will do that now champ

**Sigma** - November 3, 2021, 5:24 am

(Nov 2, 2021 02:13 AM)Flaws. Wrote: [\[CITE\]](#) Lmao man I remember when I used to be a little prick too, I've been out of this for time and just come back for a bit of help, love that you and your butt buddy also both neg repped me simply for replying too you, actually hilarious :')

Cheers for the heads up on Dariks boot and nuke, will do that now champ

I still would like to see those FRST logs, I can help you get that removed or at least pinpoint it.

**Flaws.** - November 3, 2021, 5:27 am

(Nov 3, 2021 05:24 AM)Sigma Wrote: [\[CITE\]](#) I still would like to see those FRST logs, I can help you get that removed or at least pinpoint it.

Much appreciated mate, all worked out now though

Have a good day!