Forum:Hack Forums

Thread: Suspected RAT infection

dota123 - *August 11, 2026, 10:06 am*

Hi everyone,

I need some help checking if my PC might be infected with a RAT or some other malware.

I've been worried about this for about two months. I check my PC for malware almost every day, but so far I haven't found any clear proof that there is actually an infection.

I would really appreciate it if someone experienced with malware could look at my diagnostic logs and tell me if anything looks suspicious.

I'm mainly looking for signs of a RAT, suspicious processes, startup entries, scheduled tasks, services, or anything else that could indicate malware.

I don't want to keep checking and reinstalling Windows over and over if there isn't any real evidence of an infection.

I'm happy to provide any logs you need and follow your instructions.

Thanks for your help!

5chn4pp - *August 11, 2026, 10:14 am*

Please do the following if you want me to check your device.

Please download Farbar Recovery Scan Tool (FRST) and save it to your Desktop.

Note: Most modern systems are 64-bit. If you're unsure, download the 64-bit version first. If it won't run, try the 32-bit version instead.

1. Right-click the downloaded file and select Run as administrator.
2. When the tool opens, click Yes to accept the disclaimer.
3. Click the Scan button and wait for it to finish.
4. Two logs will be created on your Desktop: FRST.txt and Addition.txt.
5. Open each log, copy its contents, and paste them into Pastebin. Share both Pastebin links in your next reply.

DramaKing - *August 11, 2026, 10:52 am*

2 months is a long time for malware to remain undetected? Do you have some explanation as to why you think this?

Binance - *August 11, 2026, 10:58 am*

(Aug 11, 2026 10:52 AM)DramaKing Wrote: *[CITE]* 2 months is a long time for malware to remain undetected? Do you have some explanation as to why you think this?
it's alex buckland again

DramaKing - *August 11, 2026, 11:24 am*

(Aug 11, 2026 10:58 AM)Binance Wrote: [CITE] it's alex buckland again
Then reports of his suicide are false.

dota123 - *August 11, 2026, 1:48 pm*
(Aug 11, 2026 10:52 AM)DramaKing Wrote: [CITE] 2 months is a long time for malware to remain undetected? Do you have some explanation as to why you think this?

It sounds silly, but for a long time now, some people from Discord have been mentioning things I did on my computer—things they couldn't possibly have known about.

Sorry, you cannot post links, videos, or images until you've made more than 50 total posts or have upgraded.

5chn4pp - *August 11, 2026, 2:04 pm*
(Aug 11, 2026 01:48 PM)dota123 Wrote: [CITE] Sorry, you cannot post links, videos, or images until you've made more than 50 total posts or have upgraded.
You can post it like this:

pastebin.com/testing123

dota123 - *August 11, 2026, 2:08 pm*
pastebin.com/29f79uxf

pastebin.com/PQNgL8sG

5chn4pp - *August 11, 2026, 2:56 pm*
(Aug 11, 2026 02:08 PM)dota123 Wrote: [CITE] pastebin.com/29f79uxf

pastebin.com/PQNgL8sG
These logs are a bit tricky, because while they don't show any obvious infection by malware, they do show usage of 3rd-party Windows patches, which could in theory be malicious.

For example, you are running ExplorerPatcher, which uses a DXGI proxy in-between system processes. Technically, this could enable someone to essentially monitor everything on your device.

Another thing is that you downloaded a tool called SimpleUnlocker. This tool had a modified version of process hacker where 15 KB of base64 data was added at the end of the .exe. I did not completely analyze it fully, since it would take me some time to do that.

My suggestion here is that you do not utilize any of these tools and only stick to a stock version of Windows 11. Then only use well-known apps from trusted sites.

Let me know if you intend to factory reset your device like you have done before, that's probably the fastest method, or we can do a manual malware removal from the current installation.

DramaKing - *August 11, 2026, 3:19 pm*
(Aug 11, 2026 01:48 PM)dota123 Wrote: [CITE] It sounds silly, but for a long time now, some people from Discord have been mentioning things I did on my computer—things they couldn't possibly have known about.
I've heard this story too many times before. Are there kids running around on Discord committing stupid computer crimes? Sure. But a RAT would get detected, and there are too many mental ailments that can cause people to imagine just this. Could be paranoid schizophrenia. One member was certain that his fully wiped PC with a fresh Windows install was hacked and that a certain

person online was spying on him through everything he owned with an electronic circuit. He also posted about blowing his mind on drugs.

dota123 - *August 11, 2026, 3:40 pm*

(Aug 11, 2026 02:56 PM)5chn4pp Wrote: [CITE] These logs are a bit tricky, because while they don't show any obvious infection by malware, they do show usage of 3rd-party Windows patches, which could in theory be malicious.

For example, you are running ExplorerPatcher, which uses a DXGI proxy in-between system processes. Technically, this could enable someone to essentially monitor everything on your device.

Another thing is that you downloaded a tool called SimpleUnlocker. This tool had a modified version of process hacker where 15 KB of base64 data was added at the end of the .exe. I did not completely analyze it fully, since it would take me some time to do that.

My suggestion here is that you do not utilize any of these tools and only stick to a stock version of Windows 11. Then only use well-known apps from trusted sites.

Let me know if you intend to factory reset your device like you have done before, that's probably the fastest method, or we can do a manual malware removal from the current installation.
Thank you for reviewing the logs.

I have already uninstalled ExplorerPatcher and I will not use these types of third-party Windows patches or tools going forward. I also understand your concerns regarding SimpleUnlocker.

I would prefer to proceed with manual malware removal from the current Windows installation, rather than factory resetting the device again.

Please guide me through the manual removal process and let me know what you would like me to check or remove next.

Thank you for your help.

(Aug 11, 2026 03:19 PM)DramaKing Wrote: [CITE] I've heard this story too many times before. Are there kids running around on Discord committing stupid computer crimes? Sure. But a RAT would get detected, and there are too many mental ailments that can cause people to imagine just this. Could be paranoid schizophrenia. One member was certain that his fully wiped PC with a fresh Windows install was hacked and that a certain person online was spying on him through everything he owned with an electronic circuit. He also posted about blowing his mind on drugs.

I just thought maybe he created a custom-made RAT that's impossible to detect.

5chn4pp - *August 11, 2026, 3:57 pm*

(Aug 11, 2026 03:40 PM)dota123 Wrote: [CITE] Thank you for reviewing the logs.

I have already uninstalled ExplorerPatcher and I will not use these types of third-party Windows patches or tools going forward. I also understand your concerns regarding SimpleUnlocker.

I would prefer to proceed with manual malware removal from the current Windows installation, rather than factory resetting the device again.

Please guide me through the manual removal process and let me know what you would like me to check or remove next.

Thank you for your help.
The next step for manual malware removal is to also fetch the logs from the other tools already ran.

Please share the following:

C:\Users\User\Desktop\eset.txt
C:\Users\User\Desktop\Fixlog.txt

And any logs/reports under the following folders:

C:\ProgramData\HitmanPro\Logs
C:\AdwCleaner\Logs

Also please tell me if Malwarebytes or Kaspersky had any detections when you ran those tools.

If Malwarebytes or Kaspersky detected anything, it should be viewable in the applications.

And please do a clean FRST scan, and share the new FRST.txt and Addition.txt logs.

Please note I will only respond in about 16 hours, due to me needing sleep now.

DramaKing - *August 11, 2026, 6:38 pm*

(Aug 11, 2026 03:40 PM)dota123 Wrote: [CITE] I just thought maybe he created a custom-made RAT that's impossible to detect.
Some malware is more difficult to analyze, but everything gets analyzed if it hits enough systems.

(Aug 11, 2026 03:40 PM)dota123 Wrote: [CITE] Thank you for reviewing the logs.

I have already uninstalled ExplorerPatcher and I will not use these types of third-party Windows patches or tools going forward. I also understand your concerns regarding SimpleUnlocker.

I would prefer to proceed with manual malware removal from the current Windows installation, rather than factory resetting the device again.

Please guide me through the manual removal process and let me know what you would like me to check or remove next.

Thank you for your help.
Let's be clear. No malware was found. Just a couple of apps that are a little sketchy. These do not fit with the Discord social engineering scenario.

dota123 - *August 12, 2026, 4:08 am*

Hello,

I completed the requested scans and fixes.

"ESET.txt" (Click to View)
Scan completed successfully.
Files scanned: 461867
Detections: 1
Cleaned files: 1

Detection:

C:\Users\User\Desktop\simpleunlocker_release\othersoftware\ProcessHacker\x64\kprocesshacker.sys
Detection: Win64/VulnDriver.ProcessHacker.A (potentially unsafe application)
Action: cleaned by deleting

"Fixlog.txt - summary" (Click to View)
Farbar Recovery Scan Tool fix completed successfully.

- Processes closed successfully.
- Restore point created successfully.
- npcap_wifi service/driver was removed.
- Microsoft Edge automatic startup entry was removed.
- Edge policy entries and stale registry entries were removed.
- Stale firewall rules were removed.
- WMI repository was verified as consistent.
- Performance counters were successfully rebuilt.
- DISM RestoreHealth completed successfully.
- SFC completed successfully and reported:
  "Windows Resource Protection found corrupt files and successfully repaired them."
- Windows Update components were reset.
- Network stack and Windows Firewall were reset.
- Temporary files and caches were cleaned.
- Approximately 5.1 GB of temporary data was removed.

The full Fixlog.txt is available if needed.

Regarding the ESET detection: this was the Process Hacker driver located inside my old SimpleUnlocker folder. I understand this was flagged as potentially unsafe.

Please let me know if you need the complete Fixlog.txt or any additional logs/reports.

5chn4pp - *August 12, 2026, 6:56 am*
(Aug 12, 2026 04:08 AM)dota123 Wrote: *[CITE]* Hello,

I completed the requested scans and fixes.

"ESET.txt" (Click to View)
Scan completed successfully.
Files scanned: 461867
Detections: 1
Cleaned files: 1

Detection:

C:\Users\User\Desktop\simpleunlocker_release\othersoftware\ProcessHacker\x64\kprocesshacker.sys
Detection: Win64/VulnDriver.ProcessHacker.A (potentially unsafe application)
Action: cleaned by deleting

"Fixlog.txt - summary" (Click to View)
Farbar Recovery Scan Tool fix completed successfully.

- Processes closed successfully.
- Restore point created successfully.
- npcap_wifi service/driver was removed.
- Microsoft Edge automatic startup entry was removed.
- Edge policy entries and stale registry entries were removed.
- Stale firewall rules were removed.
- WMI repository was verified as consistent.
- Performance counters were successfully rebuilt.
- DISM RestoreHealth completed successfully.
- SFC completed successfully and reported:
  "Windows Resource Protection found corrupt files and successfully repaired them."
- Windows Update components were reset.
- Network stack and Windows Firewall were reset.
- Temporary files and caches were cleaned.
- Approximately 5.1 GB of temporary data was removed.

The full Fixlog.txt is available if needed.

Regarding the ESET detection: this was the Process Hacker driver located inside my old SimpleUnlocker folder. I understand this was flagged as potentially unsafe.

Please let me know if you need the complete Fixlog.txt or any additional logs/reports.
That looks like a large fixlog, please provide the full fixlog.txt.

Also, where did you get it from? Fixlists are supposed to be individualized for each device. Did someone create it for your specific device?

dota123 - *August 12, 2026, 7:00 am*
(Aug 12, 2026 06:56 AM)5chn4pp Wrote: *[CITE]* That looks like a large fixlog, please provide the full fixlog.txt.

Also, where did you get it from? Fixlists are supposed to be individualized for each device. Did someone create it for your specific device?
Just to clarify, I received this Fixlog.txt from another malware-removal forum, where a specialist provided the FIXLIST specifically for my computer. I did not create the fixlist myself or use a generic script.

the full Fixlog.txt as requested.

pastebin.com/wa2ZfCA5

5chn4pp - *August 12, 2026, 4:11 pm*
(Aug 12, 2026 07:00 AM)dota123 Wrote: *[CITE]* Just to clarify, I received this Fixlog.txt from another malware-removal forum, where a specialist provided the FIXLIST specifically for my computer. I did not create the fixlist myself or use a generic script.

the full Fixlog.txt as requested.

pastebin.com/wa2ZfCA5
I looked over the other thread on that forum, and the removal process has essentially already been ran and concluded over there.

We generally use the same removal process, and since you have already been provided fixlists and ran other scans, there is nothing much left to do.

If you have any questions, I would be happy to answer them.

dota123 - *August 14, 2026, 2:40 pm*
(Aug 12, 2026 04:11 PM)5chn4pp Wrote: [CITE] I looked over the other thread on that forum, and the removal process has essentially already been ran and concluded over there.

We generally use the same removal process, and since you have already been provided fixlists and ran other scans, there is nothing much left to do.

If you have any questions, I would be happy to answer them.
One more concern: about two hours before someone sent me a video, I had watched that exact video myself. This has happened several times before with things I had recently watched or listened to. Could this indicate unauthorized access or a RAT, or is there another technical explanation?

DramaKing - *August 14, 2026, 2:56 pm*
(Aug 14, 2026 02:40 PM)dota123 Wrote: [CITE] One more concern: about two hours before someone sent me a video, I had watched that exact video myself. This has happened several times before with things I had recently watched or listened to. Could this indicate unauthorized access or a RAT, or is there another technical explanation?
Cybercriminals rarely taunt their victims.

dota123 - *August 14, 2026, 3:02 pm*
(Aug 14, 2026 02:56 PM)DramaKing Wrote: [CITE] Cybercriminals rarely taunt their victims.
Yeah, but they're school kids, and I know one of them in real life

DramaKing - *August 14, 2026, 3:05 pm*
(Aug 14, 2026 03:02 PM)dota123 Wrote: [CITE] Yeah, but they're school kids, and I know one of them in real life
It could be some viral video, and this person sent it by coincidence. You didn't download anything from them, right?

dota123 - *August 14, 2026, 3:08 pm*
(Aug 14, 2026 03:05 PM)DramaKing Wrote: [CITE] It could be some viral video, and this person sent it by coincidence. You didn't download anything from them, right?
That’s the thing, I don't think I downloaded anything, and I never turn off Windows Defender; I’d expect it to have blocked a RAT installation, though I can't be certain. The video is indeed popular, but he’d never sent it before—yet today, the very day I watched it, he decided to send it. Could he have created a custom RAT? One that’s impossible for antivirus software or FRST to detect?

(Aug 14, 2026 03:08 PM)dota123 Wrote: [CITE] That’s the thing, I don't think I downloaded anything, and I never turn off Windows Defender; I’d expect it to have blocked a RAT installation, though I can't be certain. The video is indeed popular, but he’d never sent it before—yet today, the very day I watched it, he decided to send it. Could he have created a custom RAT? One that’s impossible for antivirus software or FRST to detect?

I even reinstalled Windows twice.

DramaKing - *August 14, 2026, 5:40 pm*

(Aug 14, 2026 03:08 PM)dota123 Wrote: [CITE] That’s the thing, I don't think I downloaded anything, and I never turn off Windows Defender; I’d expect it to have blocked a RAT installation, though I can't be certain. The video is indeed popular, but he’d never sent it before—yet today, the very day I watched it, he decided to send it. Could he have created a custom RAT? One that’s impossible for antivirus software or FRST to detect?

Well, FRST doesn't really detect malware. It offers visibility for someone to spot anything suspicious. If you didn't interact with this person directly, the coincidence is just enormous. Or the person would have had to do a ton of work to target you anonymously.

Again, there's no clear sign of actual malware, just your feeling of being hacked. Feelings lie. Mind games are easier for peevish jerks to play than deploying a RAT.

5chn4pp - *August 14, 2026, 6:11 pm*

(Aug 14, 2026 02:40 PM)dota123 Wrote: [CITE] One more concern: about two hours before someone sent me a video, I had watched that exact video myself. This has happened several times before with things I had recently watched or listened to. Could this indicate unauthorized access or a RAT, or is there another technical explanation?

My recommendation is to change passwords for all of your online accounts, if you haven't done it already after the malware removal process.

I would not be worried about your actual computer, but it's possible that they took your session and viewed your YouTube history, for example.

In any case, just follow best practice, change passwords, if you can, setup MFA for your accounts, that is also a good idea.

dota123 - *August 15, 2026, 3:53 am*

If necessary, I can reinstall Windows

DramaKing - *August 15, 2026, 6:21 am*

(Aug 15, 2026 03:53 AM)dota123 Wrote: [CITE] If necessary, I can reinstall Windows

Personally, it's better with Linux, but if you need Windows, just look for the most reasonable explanations to things. Sometimes someone will post something here that I've already seen, but I think nothing of it. Sometimes more than one person will post the same thing.

5chn4pp - *August 15, 2026, 11:39 am*

(Aug 15, 2026 03:53 AM)dota123 Wrote: [CITE] If necessary, I can reinstall Windows

If reinstalling gives you more sleep at night, go for it.

But after that, given my previous advice with the online accounts, I would let it rest at that point.

dota123 - *August 17, 2026, 7:29 am*

(Aug 15, 2026 11:39 AM)5chn4pp Wrote: [CITE] If reinstalling gives you more sleep at night, go for it.

But after that, given my previous advice with the online accounts, I would let it rest at that point.

I reinstalled it I hope everything will be fine.