

Forum:[Hack Forums](#)

Thread: [CMD keeps popping up then disappearing](#)

Raid7 - December 25, 2017, 2:07 am

i recently been downloading some shit off another site, even tho i scan everything before i download i think im infected as a CMD keeps popping up and disappearing, and i've looked into registry keys a couple of days ago and found some weird asian/chinese keys that didn't make any sense?

Adwcleaner and junkwareremoval tool seem to find nothing

jammy47 - December 25, 2017, 6:13 am

first use a vmware to sniff traffic of your computer and see where the data is going and block ips using your hosts file if ips are malicious. You can use flypaper to get the program to be in a suspended state and investigate the parent id of that process. Most times, those are just .bat files trying to invoke other process, so by putting that process in a suspended state you can may be dump that process and find some info. As far as i know flypaper wont allow any process to exit. If that doesnt help, you can google for some other program to stop termination of program.

ALso process explorer should let you know if any other process has been invoked.

Btw have you noticed any other signs or behaviour patterns?

You can try scanning your pc in safe mode. Pretty effective!

Super - December 25, 2017, 5:58 pm

Please follow the instructions here to run FRST:

<https://hackforums.net/showthread.php?tid=5769954&pid=56388000#pid56388000>

Once you've done that, upload your FRST.txt and Addition.txt logs and share the links with us here.

?

Dynamo

LogitechCamMan - December 27, 2017, 2:40 pm

Run a full scan using Malware bytes, then use this <https://usa.kaspersky.com/downloads/tdsskiller> , un-install any programs you don't use. check task manager to disable any programs you see run on start up that you don't know.

AsSaSs@iN - December 27, 2017, 8:12 pm

Hey sorry for the delay...

I'm AsSaSs@iN, I'm a member of the HackForums Malware Removal Team (MRT) and will be assisting you throughout this thread. Before we start just take a second to read through these few requests - these are to ensure we can help you quickly and safely: Only use this thread for help. Please don't create multiple threads, accounts, PM me or post on other forums - if you do just let me know.

Only follow my guidance.

Don't run tools I haven't asked you to run. If you do just let me know so I can take that into consideration when viewing logs.

DO NOT install any other software while we are attempting to clean your machine. It can get quite confusing especially if you are downloading questionable tools.

[color=#ffcc33]Please be prompt in responding.

I'll do my best to do so. If >48hrs has passed, please either PM me or ask "Are you there, I still need help" in this thread.

Please stick with me until I give you the 'All Clean'. I'll help you cleanup quickly and offer some tips to make you more secure and get your system running faster.

Your malware related tools will be removed. I don't support the tools often distributed on these forums. Scanners will generally remove these - I take no responsibility for any malicious software that is lost.

I (nor does the forum) support pirated software.

If you don't understand something, don't be afraid to ask - I'm here to help. ?

You'll notice the logs are pretty big and you won't be able to post a reply containing it all. Please use ONLY either: <https://hastebin.com> - here you can upload the .txt file directly. <- I prefer this.

<http://pasted.co/> - here you can set a password if you wish to protect your data. Just PM me the password.

And paste the link to the logs in your reply. Post each log separately (each with a separate link). If you're a new member and can't paste links you can fool the forums system by removing the beginning of the link.

e.g.If you can't post this: <https://hastebin.com/raw/epaduvuyic>

Post: I used hastebin, here is the ending /raw/epaduvuyic

If I request you to post an image please use a service like <https://imgur.com>

Let's get to it! (p.s. Call me assass for short!)

Please go here and following my first post through. Post the logs in this thread, NOT in a new thread.

Raid7 - December 28, 2017, 3:35 am

Thank you for your help, here are the logs!

FRST => <https://hastebin.com/raw/fuyejifepi>

Addition => <https://hastebin.com/raw/eriwatutop>

Super - December 28, 2017, 10:59 am

Hmm, it doesn't appear that you have any active malware on your system. I found something else that might help you:

You might wanna try this:

<http://www.tomshardware.com/faq/id-3426393/fix-hourly-cmd-window-pop-appearing.html>

Some other information that could help us:

- How often do you get these popups?
- Do you get these popups at startup?

Update: I think I found the problem.

It appears that OP is using a pirated copy of windows that calls a license activation patch task every once in a while. This is probably what is causing the CMD popups.

Code Task: {4C1BB8D6-63EF-4292-A8AE-A9496C77D56A} -

System32\Tasks\R@1n-KMS\Office15ProPlus => wmic [Argument = path SoftwareLicensingProduct where (ID="b322da9c-a2e2-4058-9e4e-f59a6970bd69") call Activate]

Task: {B127C20B-51A8-4DAB-BD49-D8BE4B5F2A0B} -

System32\Tasks\R@1n-KMS\Windows64Professional => wmic [Argument = path SoftwareLicensingProduct where (ID="2de67392-b7a7-462a-b1ca-108dd189f588") call Activate]

Reference: [Pirated windows 10 backround proces called KMS-R@1n](#)

?

Dynamo

AsSaSs@iN - December 28, 2017, 8:34 pm

Hi Raid,

Quote:S2 KMS-R@1n; C:\Windows\KMS-R@1n.exe [X]

It appears you may be running an illegitimate version of Windows. Unfortunately as a result, I can no longer help you. Even if you are infected, illegitimate versions of Windows have many flaws in their security and reinfection is imminent after cleaning.

I encourage you to purchase Windows either in-store or online and in the future I will be happy to help.

Based on your logs it looks like the CMD boxes are a result of it's attempt to activate as pointed out by Dynamo...

Raid7 - December 29, 2017, 2:15 am

alright, thanks for your analysis guys much appreciated!

have good holiday :)

Barhkk - December 29, 2017, 2:22 am

You could have just downloaded ESET.

Raid7 - December 29, 2017, 3:14 am

(Dec 29, 2017 03:22 AM)Barhkk Wrote: [\[CITE\]](#) You could have just downloaded ESET. exactly because ESET catches all malware and encrypted FUD malware, im so dumb

Super - December 29, 2017, 4:51 pm

Hey OP, sorry we couldn't be of more assistance. If you want I can make you a fixlist to remove the patch tasks so you won't get popups, but that might make Windows start fussing up about license keys.

Either way, take care ?

Dynamo

--

By the way, your avatar is dope.

Raid7 - December 30, 2017, 2:47 am

(Dec 29, 2017 05:51 PM)Dynamo Wrote: [\[CITE\]](#) Hey OP, sorry we couldn't be of more assistance. If you want I can make you a fixlist to remove the patch tasks so you won't get popups, but that might make Windows start fussing up about license keys.

Either way, take care ?

Dynamo

--

By the way, your avatar is dope.

Yes please do, i bought a new PC and apparently the guy sold me it with a pirated windows copy lol (typical arabian sotres lol)

Leo Mikaelson - December 30, 2017, 3:00 am

Try using this:

<http://www.herdprotect.com/>

It works great. When i installed windows, I installed 8 first to get free upgrade to 10. Not sure if this works anymore though.