

# Forum:[Hack Forums](#)

Thread: [Accidentally ran demo VBS](#)

**c00lkid66** - August 2, 2019, 6:48 am

Well I'm stupid and accidentally ran [exploitpack/Agent.vbs at master · mr-m0nst3r/exploitpack · GitHub](#) on my own computer. I know it's not that big of a deal since it wasn't set up with a server, but now even though I've removed the file from my \AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup path and removing the key from Computer\HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Run I keep having this popup: <https://i.imgur.com/SHWWeqT.png> which pops back up a few seconds after closing and doesn't stop even though I've restarted my computer. What could be calling this?

**Bastille** - August 2, 2019, 8:11 am

Seems that a program is executed at the boot of you Windows, can you take a look over there ?

- > Type Windows + R
- > Type taskmgr
- > Go to Startup tab

Post a screen of the list of the programs executed at start

**c00lkid66** - August 2, 2019, 8:52 am

(Aug 2, 2019 08:11 AM)Yseurk Wrote: [\[CITE\]](#) Seems that a program is executed at the boot of you Windows, can you take a look over there ?

- > Type Windows + R
- > Type taskmgr
- > Go to Startup tab

Post a screen of the list of the programs executed at start

<https://i.imgur.com/96tX11R.png>

I don't see anything

**Bastille** - August 2, 2019, 8:58 am

(Aug 2, 2019 08:52 AM)c00lkid66 Wrote: [\[CITE\]](#) <https://i.imgur.com/96tX11R.png>

I don't see anything  
Can you try this ?

<https://www.winhelponline.com/blog/cannot-find-script-run-vbs-logon/>

**c00lkid66** - August 2, 2019, 9:21 am

(Aug 2, 2019 08:58 AM)Yseurk Wrote: [\[CITE\]](#) Can you try this ?

<https://www.winhelponline.com/blog/cannot-find-script-run-vbs-logon/>

Just tried and my Userinit is fine. I've also searched for both "Agent.vbs" and "exploitpack.vbs" in the registry and recieved no results

**Bastille** - August 2, 2019, 9:40 am

(Aug 2, 2019 09:21 AM)c00lkid66 Wrote: [\[CITE\]](#) Just tried and my Userinit is fine. I've also searched for both "Agent.vbs" and "exploitpack.vbs" in the registry and recieved no results

Have you run some anti-malware or anti-virus ? Maybe they could help and clean your computer ?

A program is probably calling the script, have you anything weird installed on your computer ? Can you see something in the program's list ?

- > Push Windows Key + R
- > Type "appwiz.cpl"
- > Hit the Enter button

**c00lkid66** - August 2, 2019, 10:16 am

(Aug 2, 2019 09:40 AM)Yseurk Wrote: [\[CITE\]](#) Have you run some anti-malware or anti-virus ? Maybe they could help and clean your computer ?

A program is probably calling the script, have you anything weird installed on your computer ? Can you see something in the program's list ?

- > Push Windows Key + R
- > Type "appwiz.cpl"
- > Hit the Enter button

yeah I already ran it and it didn't pick it up, there are no weird programs and I'm certain it was caused by the linked .vb file

**Aura** - August 2, 2019, 10:45 am

According to the script, there's a Run entry there.

HKLM\Software\Microsoft\Windows\CurrentVersion\Run

**c00lkid66** - August 2, 2019, 1:30 pm

(Aug 2, 2019 10:45 AM)Aura Wrote: [\[CITE\]](#) According to the script, there's a Run entry there.

HKLM\Software\Microsoft\Windows\CurrentVersion\Run

I've already removed that from the registry and restarted a few times yet it's still running at the start.

**Aura** - August 2, 2019, 2:58 pm

Okay cause in your 1st post you said that you removed it from HKCU, not HKLM.

Farbar Recovery Scan Tool (FRST) - Scan mode

Follow the instructions below to download and execute a scan on your system with FRST, and provide the logs in your next reply. Download the right version of FRST for your system: [FRST 32-bit](#)

[FRST 64-bit](#)

Note: Only the right version will run on your system, the other will throw an error message. So if you don't know what your system's version is, simply download both of them, and the one that works is the one you should be using.

Move the executable (FRST.exe or FRST64.exe) on your Desktop

Right-click on the executable and select Run as Administrator (for Windows Vista, 7, 8, 8.1 and 10

users)

Accept the disclaimer by clicking on Yes, and FRST will then do a back-up of your Registry which should take a few seconds

Make sure the Addition.txt box is checked

Click on the Scan button

On completion, two message box will open, saying that the results were saved to FRST.txt and Addition.txt, then open two Notepad files

Copy and paste the content of both FRST.txt and Addition.txt in your next reply

**Bastille** - August 2, 2019, 4:27 pm

Aura is here with his FRST skills, nothing more to do there

**c00lkid66** - August 2, 2019, 6:38 pm

(Aug 2, 2019 02:58 PM)Aura Wrote: [CITE](#) Okay cause in your 1st post you said that you removed it from HKCU, not HKLM.

Farbar Recovery Scan Tool (FRST) - Scan mode

Follow the instructions below to download and execute a scan on your system with FRST, and provide the logs in your next reply. Download the right version of FRST for your system: [FRST 32-bit](#)

[FRST 64-bit](#)

Note: Only the right version will run on your system, the other will throw an error message. So if you don't know what your system's version is, simply download both of them, and the one that works is the one you should be using.

Move the executable (FRST.exe or FRST64.exe) on your Desktop

Right-click on the executable and select Run as Administrator (for Windows Vista, 7, 8, 8.1 and 10 users)

Accept the disclaimer by clicking on Yes, and FRST will then do a back-up of your Registry which should take a few seconds

Make sure the Addition.txt box is checked

Click on the Scan button

On completion, two message box will open, saying that the results were saved to FRST.txt and Addition.txt, then open two Notepad files

Copy and paste the content of both FRST.txt and Addition.txt in your next reply

<https://pastebin.com/raw/haEZQyG8>

**Bastille** - August 3, 2019, 8:41 am

Seems there is a scheduled task here :

Task: {061C0EDD-9B50-4EEC-B328-1AEDBE829749} - System32\Tasks\Exploit Pack - Agent => C:\Users\noah\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\exploitpack.vbs (which is trying to execute the vbs, which one you deleted)

By the way there is the following, not sure this tool is legit :

(PC-Doctor, Inc. -> PC-Doctor, Inc.) C:\Program Files\Dell\SupportAssistAgent\PCDr\SupportAssist\6.0.7033.2285\DSAPI.exe  
(PC-Doctor, Inc. -> PC-Doctor, Inc.) C:\Program Files\Dell\SupportAssistAgent\PCDr\SupportAssist\6.0.7033.2285\pcdrwi.exe

Can you confirm that master Aura ? ?

**c00lkid66** - August 3, 2019, 3:21 pm

(Aug 3, 2019 08:41 AM)Yseurk Wrote: [\[CITE\]](#) Seems there is a scheduled task here :

Task: {061C0EDD-9B50-4EEC-B328-1AEDBE829749} - System32\Tasks\Exploit Pack - Agent => C:\Users\noah\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\exploitpack.vbs (which is trying to execute the vbs, which one you deleted)

By the way there is the following, not sure this tool is legit :

(PC-Doctor, Inc. -> PC-Doctor, Inc.) C:\Program Files\Dell\SupportAssistAgent\PCDr\SupportAssist\6.0.7033.2285\DSAPI.exe  
(PC-Doctor, Inc. -> PC-Doctor, Inc.) C:\Program Files\Dell\SupportAssistAgent\PCDr\SupportAssist\6.0.7033.2285\pcdrwi.exe

Can you confirm that master Aura ? ?

Thanks, that fixed it :)

**Bastille** - August 4, 2019, 2:50 am

(Aug 3, 2019 03:21 PM)c00lkid66 Wrote: [\[CITE\]](#) Thanks, that fixed it :)

Your welcome bro ! ?

However, if you ask for help for something else, and a person ask you to run FRST, only trust high reputation / post members, like Aura.

Normally (I don't know how to to that now), when you give the report, then the helper give you a script to execute. If this person is dishonest, he can cause some damages to your computer.

See you later on HF take care about you and your computer ?

**c00lkid66** - August 4, 2019, 9:47 am

(Aug 2, 2019 06:38 PM)c00lkid66 Wrote: [\[CITE\]](#) url removed