

# Forum:[Hack Forums](#)

Thread: [Persistence Defender Detections](#)

**squidward1337** - July 10, 2022, 8:10 am

Hello,

Im currently writing a crypter in c#.

It is FUD by now in 99% of the crypts.

But my persistence method is detected as Trojan by Defender: Win32/Bearfoos.B!ml or Behavior:Win32/Persistence.A!ml.

If i don't include persistence it is fud.

Im dropping a Powershell script which is copying the .exe into a folder and adds an entry to Run Registry KEY and than deletes itself.

During runtime it is undetected and executes.

But Defender later catches it with both detections above and also catches the copied file as soon as a restart is done.

Does anyone know a good persistence method (that does NOT require admin)?

Or someone knows what I can do to prevent these detections?

Harmless programmes also add themselves to Run Key so I dont understand why it is detected.

Dropping to Startup folder has same detections btw.

Thanks for help

**Frost Crypt** - July 10, 2022, 10:00 am

why are you dropping the powershell script, you could execute powershell commands directly from c# without any drop including your registry key.

That could be the reason of the detection.

**squidward1337** - July 10, 2022, 10:41 am

(Jul 10, 2022 10:00 AM)Nano Shield Wrote: [\[CITE\]](#) why are you dropping the powershell script, you could execute powershell commands directly from c# without any drop including your registry key. That could be the reason of the detection.

First i did not and executed everything in Executable. Tried it with PS Scripts to have another process execute the persistence to avoid having Assembly.Load and Persistence in the same file. Thought that could be the cause of the detection. So same result with doing it in executable.

Thanks shatter. This may help!

**?BADMAN?** - July 11, 2022, 3:38 pm

(Jul 10, 2022 10:06 AM)shatter Wrote: [\[CITE\]](#) <https://github.com/mandiant/SharPersist>  
Most of these require admin , also they are detected.

I have seen lot of persistence methods recently which also require admin but they are probably not detected by wd (havent tested all of them).

What i personally use is some variant of dll proxy load for programs that already use startup.

**?BADMAN?** - July 11, 2022, 5:18 pm

(Jul 11, 2022 03:57 PM)shatter Wrote: [\[CITE\]](#) here's an idea

execute in memory!

It doesnt matter, you will get flagged after system reboot even if success to pass your file to startup at first execution.

Task scheduler , Registries and Services are monitored.