What is a registry run key?

A registry run key is a Windows registry location whose entries Windows executes automatically at logon or boot, such as `HKCU\Software\Microsoft\Windows\CurrentVersion\Run`. Attackers add a value pointing at their payload, so it relaunches every time the user logs in, no privileges beyond the current user needed for the HKCU keys. It is the simplest and most common Windows persistence, which also makes it one of the first places defenders look. It maps to MITRE T1547.001.

HOW IT WORKS

01 The technique and payload

The attacker adds a run-key value pointing at their payload:

- Current user (no admin needed): `reg add HKCU\Software\Microsoft\Windows\CurrentVersion\Run /v Updater /d "C:\Users\Public\p.exe" /f`
- All users (needs admin): the same under `HKLM`.
- The payload now executes at each logon (HKCU) or boot (HKLM).

Attackers often name the value to look legitimate ("Updater", "OneDrive"). Documented for defensive context.

> SIMPLE AND WATCHED
>
> *Run keys are the most common Windows persistence because they are trivial to set and need no admin for HKCU. That also makes them the first place defenders and EDR look, so attackers pair them with stealthier methods.*

HOW TO DEFEND

- Monitor the Run/RunOnce keys (HKCU and HKLM) for new or changed values; EDR and Sysmon catch these well.
- Baseline legitimate autostart entries so additions stand out (tools like autoruns enumerate them).
- Use application allow-listing so an unknown payload cannot execute even if a run key points at it.
- Limit local admin to keep attackers out of the HKLM (all-users) keys.
- Alert on suspicious value names and paths (user-writable directories, scripting hosts).

SOURCES

[1] MITRE ATT&CK: Boot or Logon Autostart Execution (T1547)

[2] Microsoft: Run and RunOnce registry keys

[3] MITRE ATT&CK: Persistence (TA0003)

Find the backdoors an attacker would leave behind.

`securelayer7.net/learn/persistence/what-is-a-registry-run-key`

Open online