What is service persistence?

Service persistence is creating or modifying a Windows service so the attacker's payload starts automatically at boot, usually as SYSTEM. Because services auto-start and run with high privilege, this is durable, powerful persistence. Attackers either create a new service pointing at their binary or hijack an existing one (repoint its `binPath` or replace its executable). It needs admin to install or change a service and maps to MITRE T1543.003.

HOW IT WORKS

01 The technique and payload

With admin rights, the attacker installs or hijacks a service:

- Create one set to auto-start: `sc create WinUpdate binPath= "C:\Windows\Temp\p.exe" start= auto` then `sc start WinUpdate`.
- Hijack an existing service by repointing it: `sc config <svc> binPath= "C:\...\p.exe"`, or replace the service's executable on disk (weak service permissions make this easy).
- The payload now runs as SYSTEM at boot.

Documented for defensive context.

> BOOT-TIME SYSTEM
>
> *Service persistence is prized because services start at boot and run as SYSTEM, the highest local privilege. It needs admin to set up, but once in place it is durable and powerful.*

HOW TO DEFEND

- Monitor service creation and changes (Security event 7045, Sysmon); alert on services running from user-writable or temp paths.
- Baseline legitimate services so new ones are obvious.
- Lock down service permissions so existing services cannot be repointed (see weak service permissions).
- Use application allow-listing so a service binary must be approved.
- Limit local admin, the prerequisite for installing or changing services.

SOURCES

[1] MITRE ATT&CK: Create or Modify System Process (T1543)

[2] Microsoft: Windows services

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

Find the backdoors an attacker would leave behind.

securelayer7.net/learn/persistence/what-is-service-persistence

Open online