What is a scheduled task backdoor?

A scheduled task backdoor uses the Windows Task Scheduler to re-run an attacker's payload on a trigger: at logon, at boot, on idle, or every few minutes. It is durable and flexible, a task can run as SYSTEM and survive reboots, and it blends in with the many legitimate scheduled tasks. Creating a task for all users or as SYSTEM needs admin; per-user tasks do not. It maps to MITRE T1053.005 and is a staple of Windows persistence.

HOW IT WORKS

01 The technique and payload

The attacker registers a task that relaunches their payload:

- At logon: `schtasks /create /tn "Updater" /tr "C:\Users\Public\p.exe" /sc onlogon`
- Every 5 minutes (resilient C2 callback): `schtasks /create /tn "Sync" /tr "p.exe" /sc minute /mo 5`
- As SYSTEM (needs admin): add `/ru SYSTEM`.
- PowerShell `Register-ScheduledTask` does the same.

The task persists across reboots and reappears on its trigger. Documented for defensive context.

> FLEXIBLE AND DURABLE
>
> *Scheduled tasks beat run keys on flexibility and resilience: they can run as SYSTEM, fire on many triggers, and re-call out every few minutes. They blend into the crowd of legitimate tasks.*

HOW TO DEFEND

- Monitor task creation and changes (Security event 4698, Sysmon); alert on tasks running from user-writable paths or scripting hosts.
- Baseline legitimate scheduled tasks so new ones stand out.
- Use application allow-listing so a task cannot launch an unknown binary.
- Limit local admin to block SYSTEM and all-user tasks.
- Review tasks with frequent triggers (every-minute callbacks are suspicious).

SOURCES

[1] MITRE ATT&CK: Scheduled Task/Job (T1053)

[2] Microsoft: Task Scheduler

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

Find the backdoors an attacker would leave behind.

securelayer7.net/learn/persistence/what-is-a-scheduled-task-backdoor

Open online