Detect Active Setup Persistence via StubPath Execution, Detection Strategy DET0312

Archived: 2026-04-05 14:30:22 UTC

Analytics

- Windows

AN0871

Multi-event correlation of Registry creation under Active Setup with anomalous execution of processes at user logon. Behavioral patterns include creation/modification of HKLM Active Setup keys with non-standard StubPath values, followed by process execution from uncommon paths, unsigned binaries, or unusual parent-child lineage post-user login.

Log Sources

Mutable Elements

Field	Description
TimeWindow	Correlate registry change and process execution within a specific user logon session (e.g., 5–10 minutes)
ParentProcessName	Expected parent processes for Active Setup launched binaries (e.g., explorer.exe). Deviations may indicate abuse.
StubPathValueEntropy	Degree of randomness/uncommonness in StubPath values. High entropy may indicate obfuscation.
SignedBinaryStatus	Flag if launched binary in StubPath is unsigned or uncommon for baseline
RegistryKeyOwner	Check which user/context added the Active Setup key to detect privilege abuse