Detection Strategy for AutoHotKey & AutoIT Abuse, Detection Strategy DET0332

Archived: 2026-04-05 16:31:57 UTC

AN0942

Detects execution of AutoHotKey or AutoIT interpreters or compiled scripts used for unauthorized automation, command execution, or payload delivery, correlated with anomalous process lineage, command-line arguments, or script creation events.

Log Sources

Mutable Elements

Field	Description
TimeWindow	Tuning this helps identify automation behavior outside expected user work hours.
ParentProcessName	Used to isolate cases where AHK or AutoIT scripts are spawned by suspicious or unusual processes.
ScriptExtension	Extensions such as .ahk, .au3, or unknown .exe names compiled from these.
ChildProcessCount	Threshold for number of spawned children to detect automation or modular malware behavior.