Detection Strategy for T1218.012 Verclsid Abuse, Detection Strategy DET0042

Archived: 2026-04-05 13:53:50 UTC

Analytics

- Windows

AN0118

Detects abuse of verclsid.exe to execute COM objects by monitoring process creation, CLSID arguments, DLLs or scriptlet engines loaded into memory, and If the CLSID points to remote SCT/HTA content, verclsid.exe makes outbound connections.

Log Sources

Mutable Elements

Field	Description
AllowedCLSIDs	Baseline CLSIDs frequently invoked by verclsid.exe in normal shell extension verification.
ParentProcessFilter	Unusual parents (e.g., winword.exe, excel.exe) spawning verclsid.exe should be treated as suspicious.
TimeWindow	Correlation window between verclsid.exe start, module load, and network activity.
ExternalIPRange	Restrict detection to external IPs not in approved ranges to cut noise.
