Detection of Malicious Profile Installation via CMSTP.exe, Detection Strategy DET0328

Archived: 2026-04-05 13:18:24 UTC

Analytics

- Windows

AN0932

Execution of CMSTP.exe with arguments pointing to suspicious or remote INF/SCT/DLL payloads, optionally followed by outbound network connections to untrusted IPs, process injection via COM interfaces (CMSTPLUA, CMLUAUTIL), registry modifications registering malicious profiles, or creation of suspicious INF/DLL/SCT files prior to execution.

Log Sources

Mutable Elements

Field	Description
INFPathRegex	Regex for identifying suspicious INF files; adjust to suppress known safe profiles
ExternalIPAllowlist	Domains or IP ranges allowed for CMSTP network connections
COMInterfaceGUIDs	Set of auto-elevated COM interface GUIDs to flag (e.g., CMSTPLUA, CMLUAUTIL)
RegistryKeyAllowlist	Known good registry entries for CMSTP profile registration
TimeWindow	Correlate CMSTP execution with subsequent network activity or process creation within N seconds

---

Source: https://attack.mitre.org/detectionstrategies/DET0328#AN0932