Detection Strategy for T1505.005 – Terminal Services DLL Modification (Windows), Detection Strategy DET0212

Archived: 2026-04-05 17:48:32 UTC

Analytics

- Windows

AN0595

Adversary modifies or replaces the Terminal Services DLL (`termsrv.dll`) or changes the associated `ServiceDll` Registry value to load an arbitrary or patched DLL that enables persistent and enhanced RDP access. This may include binary replacement, registry tampering, and unexpected module loads by the `svchost.exe -k termsvcs` process.

Log Sources

Mutable Elements

Field	Description
TargetDLLPath	Defenders may tune for non-standard DLLs loaded by svchost.exe or termsrv.exe processes.
RegistryKeyTarget	Environment-specific variations in the path to `ServiceDll` registry key (e.g., nested group policies).
TimeWindow	Correlation time window for registry change followed by DLL load or svchost restart.
ParentProcessName	Some environments may spawn registry changes from automation tools or administrative scripts.
