Server Software Component: Terminal Services DLL, Sub-technique T1505.005 - Enterprise

Archived: 2026-04-05 14:23:19 UTC

Adversaries may abuse components of Terminal Services to enable persistent access to systems. Microsoft Terminal Services, renamed to Remote Desktop Services in some Windows Server OSs as of 2022, enable remote terminal connections to hosts. Terminal Services allows servers to transmit a full, interactive, graphical user interface to clients via RDP.[1]

Windows Services that are run as a "generic" process (ex: `svchost.exe`) load the service's DLL file, the location of which is stored in a Registry entry named `ServiceDll`.[2] The `termsrv.dll` file, typically stored in `%SystemRoot%\System32\`, is the default `ServiceDll` value for Terminal Services in `HKLM\System\CurrentControlSet\services\TermService\Parameters\`.

Adversaries may modify and/or replace the Terminal Services DLL to enable persistent access to victimized hosts.[3] Modifications to this DLL could be done to execute arbitrary payloads (while also potentially preserving normal `termsrv.dll` functionality) as well as to simply enable abusable features of Terminal Services. For example, an adversary may enable features such as concurrent Remote Desktop Protocol sessions by either patching the `termsrv.dll` file or modifying the `ServiceDll` value to point to a DLL that provides increased RDP functionality.[4][5] On a non-server Windows OS this increased functionality may also enable an adversary to avoid Terminal Services prompts that warn/log out users of a system when a new RDP session is created.

Source: https://attack.mitre.org/techniques/T1505/005