

Boot or Logon Autostart Execution: Security Support Provider, Sub-technique T1547.005 - Enterprise

Archived: 2026-04-05 17:35:23 UTC

Adversaries may abuse security support providers (SSPs) to execute DLLs when the system boots. Windows SSP DLLs are loaded into the Local Security Authority (LSA) process at system start. Once loaded into the LSA, SSP DLLs have access to encrypted and plaintext passwords that are stored in Windows, such as any logged-on user's Domain password or smart card PINs.

The SSP configuration is stored in two Registry keys: `HKLM\SYSTEM\CurrentControlSet\Control\Lsa\Security Packages` and `HKLM\SYSTEM\CurrentControlSet\Control\Lsa\OSConfig\Security Packages`. An adversary may modify these Registry keys to add new SSPs, which will be loaded the next time the system boots, or when the `AddSecurityPackage` Windows API function is called.^[1]

Source: <https://attack.mitre.org/techniques/T1547/005>