

Boot or Logon Autostart Execution: Authentication Package, Sub-technique T1547.002 - Enterprise

Archived: 2026-04-05 18:28:18 UTC

Adversaries may abuse authentication packages to execute DLLs when the system boots. Windows authentication package DLLs are loaded by the Local Security Authority (LSA) process at system start. They provide support for multiple logon processes and multiple security protocols to the operating system.^[1]

Adversaries can use the autostart mechanism provided by LSA authentication packages for persistence by placing a reference to a binary in the Windows Registry location `HKLM\SYSTEM\CurrentControlSet\Control\Lsa\` with the key value of `"Authentication Packages"=<target binary>`. The binary will then be executed by the system when the authentication packages are loaded.

Source: <https://attack.mitre.org/techniques/T1547/002>