Boot or Logon Autostart Execution: Time Providers, Sub-technique T1547.003 - Enterprise

Archived: 2026-04-05 13:35:10 UTC

Adversaries may abuse time providers to execute DLLs when the system boots. The Windows Time service (W32Time) enables time synchronization across and within domains.[1] W32Time time providers are responsible for retrieving time stamps from hardware/network resources and outputting these values to other network clients. [2]

Time providers are implemented as dynamic-link libraries (DLLs) that are registered in the subkeys of `HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\W32Time\TimeProviders\` .[2] The time provider manager, directed by the service control manager, loads and starts time providers listed and enabled under this key at system startup and/or whenever parameters are changed.[2]

Adversaries may abuse this architecture to establish persistence, specifically by creating a new arbitrarily named subkey pointing to a malicious DLL in the `DllName` value. Administrator privileges are required for time provider registration, though execution will run in context of the Local Service account.[3]

Source: https://attack.mitre.org/techniques/T1547/003