# TTP Detail – T1547.003

## TTP Information

Name: Time Providers

Description: Adversaries may abuse time providers to execute DLLs when the system boots. The Windows Time service (W32Time) enables time synchronization across and within domains.(Citation: Microsoft W32Time Feb 2018) W32Time time providers are responsible for retrieving time stamps from hardware/network resources and outputting these values to other network clients.(Citation: Microsoft TimeProvider)

Time providers are implemented as dynamic-link libraries (DLLs) that are registered in the subkeys of `HKEY\_LOCAL\_MACHINE\System\CurrentControlSet\Services\W32Time\TimeProviders\`.(Citation: Microsoft TimeProvider) 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.(Citation: Microsoft TimeProvider)

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.(Citation: Github W32Time Oct 2017)

## Threat-Mapped Scoring

Score: 1.8

Priority: P4 - Informational (Low)

## Kill Chain Phases

**•** mitre-attack: persistence

**•** mitre-attack: privilege-escalation