# TTP Detail – T1574.011

## TTP Information

Name: Services Registry Permissions Weakness

Description: Adversaries may execute their own malicious payloads by hijacking the Registry entries used by services. Adversaries may use flaws in the permissions for Registry keys related to services to redirect from the originally specified executable to one that they control, in order to launch their own code when a service starts. Windows stores local service configuration information in the Registry under <code>HKLM\SYSTEM\CurrentControlSet\Services</code>. The information stored under a service's Registry keys can be manipulated to modify a service's execution parameters through tools such as the service controller, sc.exe, [PowerShell](https://attack.mitre.org/techniques/T1059/001), or [Reg](https://attack.mitre.org/software/S0075). Access to Registry keys is controlled through access control lists and user permissions. (Citation: Registry Key Security)(Citation: malware\_hides\_service)

If the permissions for users and groups are not properly set and allow access to the Registry keys for a service, adversaries may change the service's binPath/ImagePath to point to a different executable under their control. When the service starts or is restarted, then the adversary-controlled program will execute, allowing the adversary to establish persistence and/or privilege escalation to the account context the service is set to execute under (local/domain account, SYSTEM, LocalService, or NetworkService).

Adversaries may also alter other Registry keys in the service’s Registry tree. For example, the <code>FailureCommand</code> key may be changed so that the service is executed in an elevated context anytime the service fails or is intentionally corrupted.(Citation: Kansa Service related collectors)(Citation: Tweet Registry Perms Weakness)

The <code>Performance</code> key contains the name of a driver service's performance DLL and the names of several exported functions in the DLL.(Citation: microsoft\_services\_registry\_tree) If the <code>Performance</code> key is not already present and if an adversary-controlled user has the <code>Create Subkey</code> permission, adversaries may create the <code>Performance</code> key in the service’s Registry tree to point to a malicious DLL.(Citation: insecure\_reg\_perms)

Adversaries may also add the <code>Parameters</code> key, which stores driver-specific data, or other custom subkeys for their malicious services to establish persistence or enable other malicious activities.(Citation: microsoft\_services\_registry\_tree)(Citation: troj\_zegost) Additionally, If adversaries launch their malicious services using svchost.exe, the service’s file may be identified using <code>HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\servicename\Parameters\ServiceDll</code>.(Citation: malware\_hides\_service)

## Threat-Mapped Scoring

Score: 1.8

Priority: P4 - Informational (Low)

## Kill Chain Phases

**•** mitre-attack: persistence

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

**•** mitre-attack: defense-evasion