# TTP Detail – T1547.014

## TTP Information

Name: Active Setup

Description: Adversaries may achieve persistence by adding a Registry key to the Active Setup of the local machine. Active Setup is a Windows mechanism that is used to execute programs when a user logs in. The value stored in the Registry key will be executed after a user logs into the computer.(Citation: Klein Active Setup 2010) These programs will be executed under the context of the user and will have the account's associated permissions level.

Adversaries may abuse Active Setup by creating a key under <code> HKLM\SOFTWARE\Microsoft\Active Setup\Installed Components\</code> and setting a malicious value for <code>StubPath</code>. This value will serve as the program that will be executed when a user logs into the computer.(Citation: Mandiant Glyer APT 2010)(Citation: Citizenlab Packrat 2015)(Citation: FireEye CFR Watering Hole 2012)(Citation: SECURELIST Bright Star 2015)(Citation: paloalto Tropic Trooper 2016)

Adversaries can abuse these components to execute malware, such as remote access tools, to maintain persistence through system reboots. Adversaries may also use [Masquerading](https://attack.mitre.org/techniques/T1036) to make the Registry entries look as if they are associated with legitimate programs.

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Kill Chain Phases

**•** mitre-attack: persistence

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

## Malware

* PoisonIvy