# TTP Detail – T1547.004

## TTP Information

Name: Winlogon Helper DLL

Description: Adversaries may abuse features of Winlogon to execute DLLs and/or executables when a user logs in. Winlogon.exe is a Windows component responsible for actions at logon/logoff as well as the secure attention sequence (SAS) triggered by Ctrl-Alt-Delete. Registry entries in <code>HKLM\Software[\\Wow6432Node\\]\Microsoft\Windows NT\CurrentVersion\Winlogon\</code> and <code>HKCU\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\</code> are used to manage additional helper programs and functionalities that support Winlogon.(Citation: Cylance Reg Persistence Sept 2013)

Malicious modifications to these Registry keys may cause Winlogon to load and execute malicious DLLs and/or executables. Specifically, the following subkeys have been known to be possibly vulnerable to abuse: (Citation: Cylance Reg Persistence Sept 2013)

\* Winlogon\Notify - points to notification package DLLs that handle Winlogon events
\* Winlogon\Userinit - points to userinit.exe, the user initialization program executed when a user logs on
\* Winlogon\Shell - points to explorer.exe, the system shell executed when a user logs on

Adversaries may take advantage of these features to repeatedly execute malicious code and establish persistence.

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Kill Chain Phases

**•** mitre-attack: persistence

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

## Malware

* Bazar
* Cannon
* DarkTortilla
* Dipsind
* Gazer
* KeyBoy
* LockBit 3.0
* Remexi
* Revenge RAT

## APTs (Intrusion Sets)

* Tropic Trooper
* Turla
* Wizard Spider