# TTP Detail – T1137.006

## TTP Information

Name: Add-ins

Description: Adversaries may abuse Microsoft Office add-ins to obtain persistence on a compromised system. Office add-ins can be used to add functionality to Office programs. (Citation: Microsoft Office Add-ins) There are different types of add-ins that can be used by the various Office products; including Word/Excel add-in Libraries (WLL/XLL), VBA add-ins, Office Component Object Model (COM) add-ins, automation add-ins, VBA Editor (VBE), Visual Studio Tools for Office (VSTO) add-ins, and Outlook add-ins. (Citation: MRWLabs Office Persistence Add-ins)(Citation: FireEye Mail CDS 2018)

Add-ins can be used to obtain persistence because they can be set to execute code when an Office application starts.

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Kill Chain Phases

**•** mitre-attack: persistence

## Malware

* Bisonal
* LunarLoader
* LunarMail

## APTs (Intrusion Sets)

* Naikon