# TTP Detail – T1137

## TTP Information

Name: Office Application Startup

Description: Adversaries may leverage Microsoft Office-based applications for persistence between startups. Microsoft Office is a fairly common application suite on Windows-based operating systems within an enterprise network. There are multiple mechanisms that can be used with Office for persistence when an Office-based application is started; this can include the use of Office Template Macros and add-ins.

A variety of features have been discovered in Outlook that can be abused to obtain persistence, such as Outlook rules, forms, and Home Page.(Citation: SensePost Ruler GitHub) These persistence mechanisms can work within Outlook or be used through Office 365.(Citation: TechNet O365 Outlook Rules)

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Kill Chain Phases

**•** mitre-attack: persistence

## APTs (Intrusion Sets)

* APT32
* Gamaredon Group