# TTP Detail – T1137.005

## TTP Information

Name: Outlook Rules

Description: Adversaries may abuse Microsoft Outlook rules to obtain persistence on a compromised system. Outlook rules allow a user to define automated behavior to manage email messages. A benign rule might, for example, automatically move an email to a particular folder in Outlook if it contains specific words from a specific sender. Malicious Outlook rules can be created that can trigger code execution when an adversary sends a specifically crafted email to that user.(Citation: SilentBreak Outlook Rules)

Once malicious rules have been added to the user’s mailbox, they will be loaded when Outlook is started. Malicious rules will execute when an adversary sends a specifically crafted email to the user.(Citation: SilentBreak Outlook Rules)

## Threat-Mapped Scoring

Score: 1.8

Priority: P4 - Informational (Low)

## Kill Chain Phases

**•** mitre-attack: persistence

## Tools

* Ruler