# TTP Detail – T1137.001

## TTP Information

Name: Office Template Macros

Description: Adversaries may abuse Microsoft Office templates to obtain persistence on a compromised system. Microsoft Office contains templates that are part of common Office applications and are used to customize styles. The base templates within the application are used each time an application starts. (Citation: Microsoft Change Normal Template)

Office Visual Basic for Applications (VBA) macros (Citation: MSDN VBA in Office) can be inserted into the base template and used to execute code when the respective Office application starts in order to obtain persistence. Examples for both Word and Excel have been discovered and published. By default, Word has a Normal.dotm template created that can be modified to include a malicious macro. Excel does not have a template file created by default, but one can be added that will automatically be loaded.(Citation: enigma0x3 normal.dotm)(Citation: Hexacorn Office Template Macros) Shared templates may also be stored and pulled from remote locations.(Citation: GlobalDotName Jun 2019)

Word Normal.dotm location:<br>
<code>C:\Users\&lt;username&gt;\AppData\Roaming\Microsoft\Templates\Normal.dotm</code>

Excel Personal.xlsb location:<br>
<code>C:\Users\&lt;username&gt;\AppData\Roaming\Microsoft\Excel\XLSTART\PERSONAL.XLSB</code>

Adversaries may also change the location of the base template to point to their own by hijacking the application's search order, e.g. Word 2016 will first look for Normal.dotm under <code>C:\Program Files (x86)\Microsoft Office\root\Office16\</code>, or by modifying the GlobalDotName registry key. By modifying the GlobalDotName registry key an adversary can specify an arbitrary location, file name, and file extension to use for the template that will be loaded on application startup. To abuse GlobalDotName, adversaries may first need to register the template as a trusted document or place it in a trusted location.(Citation: GlobalDotName Jun 2019)

An adversary may need to enable macros to execute unrestricted depending on the system or enterprise security policy on use of macros.

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Kill Chain Phases

**•** mitre-attack: persistence

## Malware

* BackConfig
* Cobalt Strike

## APTs (Intrusion Sets)

* MuddyWater