# TTP Detail – T1564.007

## TTP Information

Name: VBA Stomping

Description: Adversaries may hide malicious Visual Basic for Applications (VBA) payloads embedded within MS Office documents by replacing the VBA source code with benign data.(Citation: FireEye VBA stomp Feb 2020)

MS Office documents with embedded VBA content store source code inside of module streams. Each module stream has a <code>PerformanceCache</code> that stores a separate compiled version of the VBA source code known as p-code. The p-code is executed when the MS Office version specified in the <code>\_VBA\_PROJECT</code> stream (which contains the version-dependent description of the VBA project) matches the version of the host MS Office application.(Citation: Evil Clippy May 2019)(Citation: Microsoft \_VBA\_PROJECT Stream)

An adversary may hide malicious VBA code by overwriting the VBA source code location with zero’s, benign code, or random bytes while leaving the previously compiled malicious p-code. Tools that scan for malicious VBA source code may be bypassed as the unwanted code is hidden in the compiled p-code. If the VBA source code is removed, some tools might even think that there are no macros present. If there is a version match between the <code>\_VBA\_PROJECT</code> stream and host MS Office application, the p-code will be executed, otherwise the benign VBA source code will be decompressed and recompiled to p-code, thus removing malicious p-code and potentially bypassing dynamic analysis.(Citation: Walmart Roberts Oct 2018)(Citation: FireEye VBA stomp Feb 2020)(Citation: pcodedmp Bontchev)

## Threat-Mapped Scoring

Score: 1.8

Priority: P4 - Informational (Low)

## Kill Chain Phases

**•** mitre-attack: defense-evasion