# TTP Detail – T1221

## TTP Information

Name: Template Injection

Description: Adversaries may create or modify references in user document templates to conceal malicious code or force authentication attempts. For example, Microsoft’s Office Open XML (OOXML) specification defines an XML-based format for Office documents (.docx, xlsx, .pptx) to replace older binary formats (.doc, .xls, .ppt). OOXML files are packed together ZIP archives compromised of various XML files, referred to as parts, containing properties that collectively define how a document is rendered.(Citation: Microsoft Open XML July 2017)

Properties within parts may reference shared public resources accessed via online URLs. For example, template properties may reference a file, serving as a pre-formatted document blueprint, that is fetched when the document is loaded.

Adversaries may abuse these templates to initially conceal malicious code to be executed via user documents. Template references injected into a document may enable malicious payloads to be fetched and executed when the document is loaded.(Citation: SANS Brian Wiltse Template Injection) These documents can be delivered via other techniques such as [Phishing](https://attack.mitre.org/techniques/T1566) and/or [Taint Shared Content](https://attack.mitre.org/techniques/T1080) and may evade static detections since no typical indicators (VBA macro, script, etc.) are present until after the malicious payload is fetched.(Citation: Redxorblue Remote Template Injection) Examples have been seen in the wild where template injection was used to load malicious code containing an exploit.(Citation: MalwareBytes Template Injection OCT 2017)

Adversaries may also modify the <code>\*\template</code> control word within an .rtf file to similarly conceal then download malicious code. This legitimate control word value is intended to be a file destination of a template file resource that is retrieved and loaded when an .rtf file is opened. However, adversaries may alter the bytes of an existing .rtf file to insert a template control word field to include a URL resource of a malicious payload.(Citation: Proofpoint RTF Injection)(Citation: Ciberseguridad Decoding malicious RTF files)

This technique may also enable [Forced Authentication](https://attack.mitre.org/techniques/T1187) by injecting a SMB/HTTPS (or other credential prompting) URL and triggering an authentication attempt.(Citation: Anomali Template Injection MAR 2018)(Citation: Talos Template Injection July 2017)(Citation: ryhanson phishery SEPT 2016)

## Threat-Mapped Scoring

Score: 1.8

Priority: P4 - Informational (Low)

## Kill Chain Phases

**•** mitre-attack: defense-evasion

## Malware

* Chaes
* WarzoneRAT

## APTs (Intrusion Sets)

* APT28
* Confucius
* DarkHydrus
* Dragonfly
* Gamaredon Group
* Inception
* Tropic Trooper