# TTP Detail – T1027.006

## TTP Information

Name: HTML Smuggling

Description: Adversaries may smuggle data and files past content filters by hiding malicious payloads inside of seemingly benign HTML files. HTML documents can store large binary objects known as JavaScript Blobs (immutable data that represents raw bytes) that can later be constructed into file-like objects. Data may also be stored in Data URLs, which enable embedding media type or MIME files inline of HTML documents. HTML5 also introduced a download attribute that may be used to initiate file downloads.(Citation: HTML Smuggling Menlo Security 2020)(Citation: Outlflank HTML Smuggling 2018)

Adversaries may deliver payloads to victims that bypass security controls through HTML Smuggling by abusing JavaScript Blobs and/or HTML5 download attributes. Security controls such as web content filters may not identify smuggled malicious files inside of HTML/JS files, as the content may be based on typically benign MIME types such as <code>text/plain</code> and/or <code>text/html</code>. Malicious files or data can be obfuscated and hidden inside of HTML files through Data URLs and/or JavaScript Blobs and can be deobfuscated when they reach the victim (i.e. [Deobfuscate/Decode Files or Information](https://attack.mitre.org/techniques/T1140)), potentially bypassing content filters.

For example, JavaScript Blobs can be abused to dynamically generate malicious files in the victim machine and may be dropped to disk by abusing JavaScript functions such as <code>msSaveBlob</code>.(Citation: HTML Smuggling Menlo Security 2020)(Citation: MSTIC NOBELIUM May 2021)(Citation: Outlflank HTML Smuggling 2018)(Citation: nccgroup Smuggling HTA 2017)

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Kill Chain Phases

**•** mitre-attack: defense-evasion

## Malware

* EnvyScout
* QakBot

## APTs (Intrusion Sets)

* APT29