# TTP Detail – T1027.017

## TTP Information

Name: SVG Smuggling

Description: Adversaries may smuggle data and files past content filters by hiding malicious payloads inside of seemingly benign SVG files.(Citation: Trustwave SVG Smuggling 2025) SVGs, or Scalable Vector Graphics, are vector-based image files constructed using XML. As such, they can legitimately include `<script>` tags that enable adversaries to include malicious JavaScript payloads. However, SVGs may appear less suspicious to users than other types of executable files, as they are often treated as image files.

SVG smuggling can take a number of forms. For example, threat actors may include content that:

\* Assembles malicious payloads(Citation: Talos SVG Smuggling 2022)
\* Downloads malicious payloads(Citation: Cofense SVG Smuggling 2024)
\* Redirects users to malicious websites(Citation: Bleeping Computer SVG Smuggling 2024)
\* Displays interactive content to users, such as fake login forms and download buttons.(Citation: Bleeping Computer SVG Smuggling 2024)

SVG Smuggling may be used in conjunction with [HTML Smuggling](https://attack.mitre.org/techniques/T1027/006) where an SVG with a malicious payload is included inside an HTML file.(Citation: Talos SVG Smuggling 2022) SVGs may also be included in other types of documents, such as PDFs.

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Kill Chain Phases

**•** mitre-attack: defense-evasion