# TTP Detail – T1027.012

## TTP Information

Name: LNK Icon Smuggling

Description: Adversaries may smuggle commands to download malicious payloads past content filters by hiding them within otherwise seemingly benign windows shortcut files. Windows shortcut files (.LNK) include many metadata fields, including an icon location field (also known as the `IconEnvironmentDataBlock`) designed to specify the path to an icon file that is to be displayed for the LNK file within a host directory.

Adversaries may abuse this LNK metadata to download malicious payloads. For example, adversaries have been observed using LNK files as phishing payloads to deliver malware. Once invoked (e.g., [Malicious File](https://attack.mitre.org/techniques/T1204/002)), payloads referenced via external URLs within the LNK icon location field may be downloaded. These files may also then be invoked by [Command and Scripting Interpreter](https://attack.mitre.org/techniques/T1059)/[System Binary Proxy Execution](https://attack.mitre.org/techniques/T1218) arguments within the target path field of the LNK.(Citation: Unprotect Shortcut)(Citation: Booby Trap Shortcut 2017)

LNK Icon Smuggling may also be utilized post compromise, such as malicious scripts executing an LNK on an infected host to download additional malicious payloads.

## Threat-Mapped Scoring

Score: 1.4

Priority: P4 - Informational (Low)

## Kill Chain Phases

**•** mitre-attack: defense-evasion