# TTP Detail – T1176

## TTP Information

Name: Software Extensions

Description: Adversaries may abuse software extensions to establish persistent access to victim systems. Software extensions are modular components that enhance or customize the functionality of software applications, including web browsers, Integrated Development Environments (IDEs), and other platforms.(Citation: Chrome Extension C2 Malware)(Citation: Abramovsky VSCode Security) Extensions are typically installed via official marketplaces, app stores, or manually loaded by users, and they often inherit the permissions and access levels of the host application.

Malicious extensions can be introduced through various methods, including social engineering, compromised marketplaces, or direct installation by users or by adversaries who have already gained access to a system. Malicious extensions can be named similarly or identically to benign extensions in marketplaces. Security mechanisms in extension marketplaces may be insufficient to detect malicious components, allowing adversaries to bypass automated scanners or exploit trust established during the installation process. Adversaries may also abuse benign extensions to achieve their objectives, such as using legitimate functionality to tunnel data or bypass security controls.

The modular nature of extensions and their integration with host applications make them an attractive target for adversaries seeking to exploit trusted software ecosystems. Detection can be challenging due to the inherent trust placed in extensions during installation and their ability to blend into normal application workflows.

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Kill Chain Phases

**•** mitre-attack: persistence