# TTP Detail – T1176.001

## TTP Information

Name: Browser Extensions

Description: Adversaries may abuse internet browser extensions to establish persistent access to victim systems. Browser extensions or plugins are small programs that can add functionality to and customize aspects of internet browsers. They can be installed directly via a local file or custom URL or through a browser's app store - an official online platform where users can browse, install, and manage extensions for a specific web browser. Extensions generally inherit the web browser's permissions previously granted.(Citation: Wikipedia Browser Extension)(Citation: Chrome Extensions Definition)

Malicious extensions can be installed into a browser through malicious app store downloads masquerading as legitimate extensions, through social engineering, or by an adversary that has already compromised a system. Security can be limited on browser app stores, so it may not be difficult for malicious extensions to defeat automated scanners.(Citation: Malicious Chrome Extension Numbers) Depending on the browser, adversaries may also manipulate an extension's update url to install updates from an adversary-controlled server or manipulate the mobile configuration file to silently install additional extensions.

Previous to macOS 11, adversaries could silently install browser extensions via the command line using the <code>profiles</code> tool to install malicious <code>.mobileconfig</code> files. In macOS 11+, the use of the <code>profiles</code> tool can no longer install configuration profiles; however, <code>.mobileconfig</code> files can be planted and installed with user interaction.(Citation: xorrior chrome extensions macOS)

Once the extension is installed, it can browse to websites in the background, steal all information that a user enters into a browser (including credentials), and be used as an installer for a RAT for persistence.(Citation: Chrome Extension Crypto Miner)(Citation: ICEBRG Chrome Extensions)(Citation: Banker Google Chrome Extension Steals Creds)(Citation: Catch All Chrome Extension)

There have also been instances of botnets using a persistent backdoor through malicious Chrome extensions for [Command and Control](https://attack.mitre.org/tactics/TA0011).(Citation: Stantinko Botnet)(Citation: Chrome Extension C2 Malware) Adversaries may also use browser extensions to modify browser permissions and components, privacy settings, and other security controls for [Defense Evasion](https://attack.mitre.org/tactics/TA0005).(Citation: Browers FriarFox)(Citation: Browser Adrozek)

## Threat-Mapped Scoring

Score: 1.8

Priority: P4 - Informational (Low)

## Kill Chain Phases

**•** mitre-attack: persistence

## Malware

* Bundlore
* Grandoreiro
* Lumma Stealer
* Mispadu
* OSX/Shlayer
* TRANSLATEXT

## APTs (Intrusion Sets)

* Kimsuky