Software Extensions: Browser Extensions, Sub-technique T1176.001 - Enterprise

Archived: 2026-04-05 14:53:31 UTC

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.[1][2]

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.[3] 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.

Adversaries may abuse how chromium-based browsers load extensions by modifying or replacing the Preferences and/or Secure Preferences files to silently install malicious extensions. When the browser is not running, adversaries can alter these files, ensuring the extension is loaded, granted desired permissions, and will persist in browser sessions. This method does not require user consent and extensions are silently loaded in the background from disk or from the browser's trusted store.[4]

Previous to macOS 11, adversaries could silently install browser extensions via the command line using the `profiles` tool to install malicious `.mobileconfig` files. In macOS 11+, the use of the `profiles` tool can no longer install configuration profiles; however, `.mobileconfig` files can be planted and installed with user interaction.[5]

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.[6][7][8][9]

There have also been instances of botnets using a persistent backdoor through malicious Chrome extensions for Command and Control.[10][11] Adversaries may also use browser extensions to modify browser permissions and components, privacy settings, and other security controls for Defense Evasion.[12][13]

Source: https://attack.mitre.org/techniques/T1176/001