Software Extensions: IDE Extensions, Sub-technique T1176.002 - Enterprise

Archived: 2026-04-05 18:07:46 UTC

Adversaries may abuse an integrated development environment (IDE) extension to establish persistent access to victim systems.[1] IDEs such as Visual Studio Code, IntelliJ IDEA, and Eclipse support extensions - software components that add features like code linting, auto-completion, task automation, or integration with tools like Git and Docker. A malicious extension can be installed through an extension marketplace (i.e., Compromise Software Dependencies and Development Tools) or side-loaded directly into the IDE.[2][3]

In addition to installing malicious extensions, adversaries may also leverage benign ones. For example, adversaries may establish persistent SSH tunnels via the use of the VSCode Remote SSH extension (i.e., IDE Tunneling).

Trust is typically established through the installation process; once installed, the malicious extension is run every time that the IDE is launched. The extension can then be used to execute arbitrary code, establish a backdoor, mine cryptocurrency, or exfiltrate data.[4]

Source: https://attack.mitre.org/techniques/T1176/002