# TTP Detail – T1219.001

## TTP Information

Name: IDE Tunneling

Description: Adversaries may abuse Integrated Development Environment (IDE) software with remote development features to establish an interactive command and control channel on target systems within a network. IDE tunneling combines SSH, port forwarding, file sharing, and debugging into a single secure connection, letting developers work on remote systems as if they were local. Unlike SSH and port forwarding, IDE tunneling encapsulates an entire session and may use proprietary tunneling protocols alongside SSH, allowing adversaries to blend in with legitimate development workflows. Some IDEs, like Visual Studio Code, also provide CLI tools (e.g., `code tunnel`) that adversaries may use to programmatically establish tunnels and generate web-accessible URLs for remote access. These tunnels can be authenticated through accounts such as GitHub, enabling the adversary to control the compromised system via a legitimate developer portal.(Citation: sentinelone operationDigitalEye Dec 2024)(Citation: Unit42 Chinese VSCode 06 September 2024)(Citation: Thornton tutorial VSCode shell September 2023)

Additionally, adversaries may use IDE tunneling for persistence. Some IDEs, such as Visual Studio Code and JetBrains, support automatic reconnection. Adversaries may configure the IDE to auto-launch at startup, re-establishing the tunnel upon execution. Compromised developer machines may also be exploited as jump hosts to move further into the network.

IDE tunneling tools may be built-in or installed as [IDE Extensions](https://attack.mitre.org/techniques/T1176/002).

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Kill Chain Phases

**•** mitre-attack: command-and-control