# TTP Detail – T1218.015

## TTP Information

Name: Electron Applications

Description: Adversaries may abuse components of the Electron framework to execute malicious code. The Electron framework hosts many common applications such as Signal, Slack, and Microsoft Teams.(Citation: Electron 2) Originally developed by GitHub, Electron is a cross-platform desktop application development framework that employs web technologies like JavaScript, HTML, and CSS.(Citation: Electron 3) The Chromium engine is used to display web content and Node.js runs the backend code.(Citation: Electron 1)

Due to the functional mechanics of Electron (such as allowing apps to run arbitrary commands), adversaries may also be able to perform malicious functions in the background potentially disguised as legitimate tools within the framework.(Citation: Electron 1) For example, the abuse of `teams.exe` and `chrome.exe` may allow adversaries to execute malicious commands as child processes of the legitimate application (e.g., `chrome.exe --disable-gpu-sandbox --gpu-launcher="C:\Windows\system32\cmd.exe /c calc.exe`).(Citation: Electron 6-8)

Adversaries may also execute malicious content by planting malicious [JavaScript](https://attack.mitre.org/techniques/T1059/007) within Electron applications.(Citation: Electron Security)

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Kill Chain Phases

**•** mitre-attack: defense-evasion

## Malware

* Lumma Stealer