# TTP Detail – T1195

## TTP Information

Name: Supply Chain Compromise

Description: Adversaries may manipulate products or product delivery mechanisms prior to receipt by a final consumer for the purpose of data or system compromise.

Supply chain compromise can take place at any stage of the supply chain including:

\* Manipulation of development tools
\* Manipulation of a development environment
\* Manipulation of source code repositories (public or private)
\* Manipulation of source code in open-source dependencies
\* Manipulation of software update/distribution mechanisms
\* Compromised/infected system images (multiple cases of removable media infected at the factory)(Citation: IBM Storwize)(Citation: Schneider Electric USB Malware)
\* Replacement of legitimate software with modified versions
\* Sales of modified/counterfeit products to legitimate distributors
\* Shipment interdiction

While supply chain compromise can impact any component of hardware or software, adversaries looking to gain execution have often focused on malicious additions to legitimate software in software distribution or update channels.(Citation: Avast CCleaner3 2018)(Citation: Microsoft Dofoil 2018)(Citation: Command Five SK 2011) Targeting may be specific to a desired victim set or malicious software may be distributed to a broad set of consumers but only move on to additional tactics on specific victims.(Citation: Symantec Elderwood Sept 2012)(Citation: Avast CCleaner3 2018)(Citation: Command Five SK 2011) Popular open source projects that are used as dependencies in many applications may also be targeted as a means to add malicious code to users of the dependency.(Citation: Trendmicro NPM Compromise)

## Threat-Mapped Scoring

Score: 1.8

Priority: P4 - Informational (Low)

## Kill Chain Phases

**•** mitre-attack: initial-access

## Malware

* Lumma Stealer
* Raccoon Stealer

## APTs (Intrusion Sets)

* Ember Bear
* OilRig
* Sandworm Team