# TTP Detail – T1195.002

## TTP Information

Name: Compromise Software Supply Chain

Description: Adversaries may manipulate application software prior to receipt by a final consumer for the purpose of data or system compromise. Supply chain compromise of software can take place in a number of ways, including manipulation of the application source code, manipulation of the update/distribution mechanism for that software, or replacing compiled releases with a modified version.

Targeting may be specific to a desired victim set or may be distributed to a broad set of consumers but only move on to additional tactics on specific victims.(Citation: Avast CCleaner3 2018)(Citation: Command Five SK 2011)

## Threat-Mapped Scoring

Score: 1.8

Priority: P4 - Informational (Low)

## Kill Chain Phases

**•** mitre-attack: initial-access

## Malware

* CCBkdr
* GoldenSpy
* SUNSPOT

## APTs (Intrusion Sets)

* APT41
* Cobalt Group
* Daggerfly
* Dragonfly
* FIN7
* GOLD SOUTHFIELD
* Moonstone Sleet
* Sandworm Team
* Threat Group-3390