# TTP Detail – T1588.002

## TTP Information

Name: Tool

Description: Adversaries may buy, steal, or download software tools that can be used during targeting. Tools can be open or closed source, free or commercial. A tool can be used for malicious purposes by an adversary, but (unlike malware) were not intended to be used for those purposes (ex: [PsExec](https://attack.mitre.org/software/S0029)). Tool acquisition can involve the procurement of commercial software licenses, including for red teaming tools such as [Cobalt Strike](https://attack.mitre.org/software/S0154). Commercial software may be obtained through purchase, stealing licenses (or licensed copies of the software), or cracking trial versions.(Citation: Recorded Future Beacon 2019)

Adversaries may obtain tools to support their operations, including to support execution of post-compromise behaviors. In addition to freely downloading or purchasing software, adversaries may steal software and/or software licenses from third-party entities (including other adversaries).

## Threat-Mapped Scoring

Score: 1.8

Priority: P4 - Informational (Low)

## Kill Chain Phases

**•** mitre-attack: resource-development

## APTs (Intrusion Sets)

* APT-C-36
* APT1
* APT19
* APT28
* APT29
* APT32
* APT33
* APT38
* APT39
* APT41
* APT42
* Aoqin Dragon
* Aquatic Panda
* BITTER
* BRONZE BUTLER
* BackdoorDiplomacy
* BlackTech
* Blue Mockingbird
* Carbanak
* Chimera
* Cinnamon Tempest
* Cleaver
* Cobalt Group
* CopyKittens
* DarkHydrus
* DarkVishnya
* Dragonfly
* Earth Lusca
* FIN10
* FIN13
* FIN5
* FIN6
* FIN7
* FIN8
* Ferocious Kitten
* GALLIUM
* Gamaredon Group
* Gorgon Group
* HEXANE
* INC Ransom
* Inception
* IndigoZebra
* Ke3chang
* Kimsuky
* LAPSUS$
* Lazarus Group
* Leafminer
* Lotus Blossom
* LuminousMoth
* Magic Hound
* Metador
* Moses Staff
* MuddyWater
* OilRig
* POLONIUM
* Patchwork
* PittyTiger
* Play
* Salt Typhoon
* Sandworm Team
* Sea Turtle
* Silence
* Silent Librarian
* Star Blizzard
* Storm-1811
* TA2541
* TA505
* Threat Group-3390
* Thrip
* Turla
* Volt Typhoon
* WIRTE
* Whitefly
* Wizard Spider
* menuPass