# TTP Detail – T1059.006

## TTP Information

Name: Python

Description: Adversaries may abuse Python commands and scripts for execution. Python is a very popular scripting/programming language, with capabilities to perform many functions. Python can be executed interactively from the command-line (via the <code>python.exe</code> interpreter) or via scripts (.py) that can be written and distributed to different systems. Python code can also be compiled into binary executables.(Citation: Zscaler APT31 Covid-19 October 2020)

Python comes with many built-in packages to interact with the underlying system, such as file operations and device I/O. Adversaries can use these libraries to download and execute commands or other scripts as well as perform various malicious behaviors.

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Kill Chain Phases

**•** mitre-attack: execution

## Malware

* Bandook
* Bundlore
* Chaes
* Cobalt Strike
* CoinTicker
* CookieMiner
* DropBook
* Ebury
* FRAMESTING
* KeyBoy
* Keydnap
* Lumma Stealer
* Machete
* MechaFlounder
* Neo-reGeorg
* PUNCHBUGGY
* PoetRAT
* PyDCrypt
* Pysa
* Small Sieve
* SpeakUp
* Turian
* UPSTYLE
* reGeorg

## Tools

* Donut
* IronNetInjector
* Pupy
* Remcos
* SILENTTRINITY

## APTs (Intrusion Sets)

* APT29
* APT37
* APT39
* BRONZE BUTLER
* Cinnamon Tempest
* Dragonfly
* Earth Lusca
* Kimsuky
* Machete
* MuddyWater
* RedCurl
* Rocke
* Tonto Team
* Turla
* ZIRCONIUM