# TTP Detail – T1059.007

## TTP Information

Name: JavaScript

Description: Adversaries may abuse various implementations of JavaScript for execution. JavaScript (JS) is a platform-independent scripting language (compiled just-in-time at runtime) commonly associated with scripts in webpages, though JS can be executed in runtime environments outside the browser.(Citation: NodeJS)

JScript is the Microsoft implementation of the same scripting standard. JScript is interpreted via the Windows Script engine and thus integrated with many components of Windows such as the [Component Object Model](https://attack.mitre.org/techniques/T1559/001) and Internet Explorer HTML Application (HTA) pages.(Citation: JScrip May 2018)(Citation: Microsoft JScript 2007)(Citation: Microsoft Windows Scripts)

JavaScript for Automation (JXA) is a macOS scripting language based on JavaScript, included as part of Apple’s Open Scripting Architecture (OSA), that was introduced in OSX 10.10. Apple’s OSA provides scripting capabilities to control applications, interface with the operating system, and bridge access into the rest of Apple’s internal APIs. As of OSX 10.10, OSA only supports two languages, JXA and [AppleScript](https://attack.mitre.org/techniques/T1059/002). Scripts can be executed via the command line utility <code>osascript</code>, they can be compiled into applications or script files via <code>osacompile</code>, and they can be compiled and executed in memory of other programs by leveraging the OSAKit Framework.(Citation: Apple About Mac Scripting 2016)(Citation: SpecterOps JXA 2020)(Citation: SentinelOne macOS Red Team)(Citation: Red Canary Silver Sparrow Feb2021)(Citation: MDSec macOS JXA and VSCode)

Adversaries may abuse various implementations of JavaScript to execute various behaviors. Common uses include hosting malicious scripts on websites as part of a [Drive-by Compromise](https://attack.mitre.org/techniques/T1189) or downloading and executing these script files as secondary payloads. Since these payloads are text-based, it is also very common for adversaries to obfuscate their content as part of [Obfuscated Files or Information](https://attack.mitre.org/techniques/T1027).

## Threat-Mapped Scoring

Score: 1.4

Priority: P4 - Informational (Low)

## Kill Chain Phases

**•** mitre-attack: execution

## Malware

* AppleSeed
* Astaroth
* Avaddon
* BlackByte Ransomware
* Bundlore
* Chaes
* Cobalt Strike
* DarkWatchman
* EnvyScout
* GRIFFON
* Gootloader
* InvisiMole
* JSS Loader
* KONNI
* KOPILUWAK
* Latrodectus
* Metamorfo
* NanHaiShu
* POWERSTATS
* QakBot
* SocGholish
* SpicyOmelette
* StrelaStealer
* Valak
* WARPWIRE
* Xbash
* jRAT

## Tools

* Donut
* FRP

## APTs (Intrusion Sets)

* APT32
* Cobalt Group
* Earth Lusca
* Evilnum
* FIN6
* FIN7
* Higaisa
* Indrik Spider
* Kimsuky
* LazyScripter
* Leafminer
* Molerats
* MoustachedBouncer
* MuddyWater
* Saint Bear
* Sidewinder
* Silence
* Star Blizzard
* TA505
* TA577
* TA578
* Turla
* Winter Vivern