# TTP Detail – T1027.008

## TTP Information

Name: Stripped Payloads

Description: Adversaries may attempt to make a payload difficult to analyze by removing symbols, strings, and other human readable information. Scripts and executables may contain variables names and other strings that help developers document code functionality. Symbols are often created by an operating system’s `linker` when executable payloads are compiled. Reverse engineers use these symbols and strings to analyze code and to identify functionality in payloads.(Citation: Mandiant golang stripped binaries explanation)(Citation: intezer stripped binaries elf files 2018)

Adversaries may use stripped payloads in order to make malware analysis more difficult. For example, compilers and other tools may provide features to remove or obfuscate strings and symbols. Adversaries have also used stripped payload formats, such as run-only AppleScripts, a compiled and stripped version of [AppleScript](https://attack.mitre.org/techniques/T1059/002), to evade detection and analysis. The lack of human-readable information may directly hinder detection and analysis of payloads.(Citation: SentinelLabs reversing run-only applescripts 2021)

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Kill Chain Phases

**•** mitre-attack: defense-evasion

## Malware

* Cuckoo Stealer
* macOS.OSAMiner