# TTP Detail – T1564.009

## TTP Information

Name: Resource Forking

Description: Adversaries may abuse resource forks to hide malicious code or executables to evade detection and bypass security applications. A resource fork provides applications a structured way to store resources such as thumbnail images, menu definitions, icons, dialog boxes, and code.(Citation: macOS Hierarchical File System Overview) Usage of a resource fork is identifiable when displaying a file’s extended attributes, using <code>ls -l@</code> or <code>xattr -l</code> commands. Resource forks have been deprecated and replaced with the application bundle structure. Non-localized resources are placed at the top level directory of an application bundle, while localized resources are placed in the <code>/Resources</code> folder.(Citation: Resource and Data Forks)(Citation: ELC Extended Attributes)

Adversaries can use resource forks to hide malicious data that may otherwise be stored directly in files. Adversaries can execute content with an attached resource fork, at a specified offset, that is moved to an executable location then invoked. Resource fork content may also be obfuscated/encrypted until execution.(Citation: sentinellabs resource named fork 2020)(Citation: tau bundlore erika noerenberg 2020)

## Threat-Mapped Scoring

Score: 1.8

Priority: P4 - Informational (Low)

## Kill Chain Phases

**•** mitre-attack: defense-evasion

## Malware

* Keydnap
* OSX/Shlayer