# TTP Detail – T1027.009

## TTP Information

Name: Embedded Payloads

Description: Adversaries may embed payloads within other files to conceal malicious content from defenses. Otherwise seemingly benign files (such as scripts and executables) may be abused to carry and obfuscate malicious payloads and content. In some cases, embedded payloads may also enable adversaries to [Subvert Trust Controls](https://attack.mitre.org/techniques/T1553) by not impacting execution controls such as digital signatures and notarization tickets.(Citation: Sentinel Labs)   
  
Adversaries may embed payloads in various file formats to hide payloads.(Citation: Microsoft Learn) This is similar to [Steganography](https://attack.mitre.org/techniques/T1027/003), though does not involve weaving malicious content into specific bytes and patterns related to legitimate digital media formats.(Citation: GitHub PSImage)   
  
For example, adversaries have been observed embedding payloads within or as an overlay of an otherwise benign binary.(Citation: Securelist Dtrack2) Adversaries have also been observed nesting payloads (such as executables and run-only scripts) inside a file of the same format.(Citation: SentinelLabs reversing run-only applescripts 2021)   
  
Embedded content may also be used as [Process Injection](https://attack.mitre.org/techniques/T1055) payloads used to infect benign system processes.(Citation: Trend Micro) These embedded then injected payloads may be used as part of the modules of malware designed to provide specific features such as encrypting C2 communications in support of an orchestrator module. For example, an embedded module may be injected into default browsers, allowing adversaries to then communicate via the network.(Citation: Malware Analysis Report ComRAT)

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Kill Chain Phases

**•** mitre-attack: defense-evasion

## Malware

* BADHATCH
* CHIMNEYSWEEP
* ComRAT
* DEADEYE
* DEADWOOD
* DUSTPAN
* DUSTTRAP
* Dtrack
* Emotet
* IcedID
* Moneybird
* MultiLayer Wiper
* Netwalker
* Pikabot
* SMOKEDHAM
* Uroburos
* macOS.OSAMiner

## Tools

* Invoke-PSImage

## APTs (Intrusion Sets)

* Lazarus Group
* Moonstone Sleet
* TA577