# TTP Detail – T1036.008

## TTP Information

Name: Masquerade File Type

Description: Adversaries may masquerade malicious payloads as legitimate files through changes to the payload's formatting, including the file’s signature, extension, icon, and contents. Various file types have a typical standard format, including how they are encoded and organized. For example, a file’s signature (also known as header or magic bytes) is the beginning bytes of a file and is often used to identify the file’s type. For example, the header of a JPEG file, is <code> 0xFF 0xD8</code> and the file extension is either `.JPE`, `.JPEG` or `.JPG`.   
  
Adversaries may edit the header’s hex code and/or the file extension of a malicious payload in order to bypass file validation checks and/or input sanitization. This behavior is commonly used when payload files are transferred (e.g., [Ingress Tool Transfer](https://attack.mitre.org/techniques/T1105)) and stored (e.g., [Upload Malware](https://attack.mitre.org/techniques/T1608/001)) so that adversaries may move their malware without triggering detections.   
  
Common non-executable file types and extensions, such as text files (`.txt`) and image files (`.jpg`, `.gif`, etc.) may be typically treated as benign. Based on this, adversaries may use a file extension to disguise malware, such as naming a PHP backdoor code with a file name of <code>test.gif</code>. A user may not know that a file is malicious due to the benign appearance and file extension.  
  
Polygot files, which are files that have multiple different file types and that function differently based on the application that will execute them, may also be used to disguise malicious malware and capabilities.(Citation: polygot\_icedID)

## Threat-Mapped Scoring

Score: 1.8

Priority: P4 - Informational (Low)

## Kill Chain Phases

**•** mitre-attack: defense-evasion

## Malware

* ANDROMEDA
* AvosLocker
* Kapeka
* Lumma Stealer
* MagicRAT
* OSX\_OCEANLOTUS.D
* QakBot
* Raspberry Robin
* StrelaStealer

## Tools

* Brute Ratel C4

## APTs (Intrusion Sets)

* BlackByte
* Volt Typhoon