# TTP Detail – T1027.003

## TTP Information

Name: Steganography

Description: Adversaries may use steganography techniques in order to prevent the detection of hidden information. Steganographic techniques can be used to hide data in digital media such as images, audio tracks, video clips, or text files.

[Duqu](https://attack.mitre.org/software/S0038) was an early example of malware that used steganography. It encrypted the gathered information from a victim's system and hid it within an image before exfiltrating the image to a C2 server.(Citation: Wikipedia Duqu)

By the end of 2017, a threat group used <code>Invoke-PSImage</code> to hide [PowerShell](https://attack.mitre.org/techniques/T1059/001) commands in an image file (.png) and execute the code on a victim's system. In this particular case the [PowerShell](https://attack.mitre.org/techniques/T1059/001) code downloaded another obfuscated script to gather intelligence from the victim's machine and communicate it back to the adversary.(Citation: McAfee Malicious Doc Targets Pyeongchang Olympics)

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Kill Chain Phases

**•** mitre-attack: defense-evasion

## Malware

* ABK
* Avenger
* BBK
* Bandook
* Diavol
* IcedID
* LiteDuke
* ObliqueRAT
* Okrum
* Pikabot
* PolyglotDuke
* PowerDuke
* ProLock
* RDAT
* Raindrop
* Ramsay
* RegDuke
* build\_downer

## Tools

* Invoke-PSImage

## APTs (Intrusion Sets)

* APT37
* Andariel
* BRONZE BUTLER
* Earth Lusca
* Leviathan
* MuddyWater
* TA551
* Tropic Trooper