# TTP Detail – T1608.001

## TTP Information

Name: Upload Malware

Description: Adversaries may upload malware to third-party or adversary controlled infrastructure to make it accessible during targeting. Malicious software can include payloads, droppers, post-compromise tools, backdoors, and a variety of other malicious content. Adversaries may upload malware to support their operations, such as making a payload available to a victim network to enable [Ingress Tool Transfer](https://attack.mitre.org/techniques/T1105) by placing it on an Internet accessible web server.

Malware may be placed on infrastructure that was previously purchased/rented by the adversary ([Acquire Infrastructure](https://attack.mitre.org/techniques/T1583)) or was otherwise compromised by them ([Compromise Infrastructure](https://attack.mitre.org/techniques/T1584)). Malware can also be staged on web services, such as GitHub or Pastebin, or hosted on the InterPlanetary File System (IPFS), where decentralized content storage makes the removal of malicious files difficult.(Citation: Volexity Ocean Lotus November 2020)(Citation: Talos IPFS 2022)

Adversaries may upload backdoored files, such as application binaries, virtual machine images, or container images, to third-party software stores or repositories (ex: GitHub, CNET, AWS Community AMIs, Docker Hub). By chance encounter, victims may directly download/install these backdoored files via [User Execution](https://attack.mitre.org/techniques/T1204). [Masquerading](https://attack.mitre.org/techniques/T1036) may increase the chance of users mistakenly executing these files.

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Kill Chain Phases

**•** mitre-attack: resource-development

## APTs (Intrusion Sets)

* APT32
* APT42
* BITTER
* BlackByte
* EXOTIC LILY
* Earth Lusca
* FIN7
* Gamaredon Group
* HEXANE
* Kimsuky
* LazyScripter
* LuminousMoth
* Moonstone Sleet
* Mustang Panda
* Mustard Tempest
* OilRig
* Saint Bear
* Sandworm Team
* SideCopy
* Star Blizzard
* TA2541
* TA505
* TeamTNT
* Threat Group-3390