# TTP Detail – T1587.001

## TTP Information

Name: Malware

Description: Adversaries may develop malware and malware components that can be used during targeting. Building malicious software can include the development of payloads, droppers, post-compromise tools, backdoors (including backdoored images), packers, C2 protocols, and the creation of infected removable media. Adversaries may develop malware to support their operations, creating a means for maintaining control of remote machines, evading defenses, and executing post-compromise behaviors.(Citation: Mandiant APT1)(Citation: Kaspersky Sofacy)(Citation: ActiveMalwareEnergy)(Citation: FBI Flash FIN7 USB)

As with legitimate development efforts, different skill sets may be required for developing malware. The skills needed may be located in-house, or may need to be contracted out. Use of a contractor may be considered an extension of that adversary's malware development capabilities, provided the adversary plays a role in shaping requirements and maintains a degree of exclusivity to the malware.

Some aspects of malware development, such as C2 protocol development, may require adversaries to obtain additional infrastructure. For example, malware developed that will communicate with Twitter for C2, may require use of [Web Services](https://attack.mitre.org/techniques/T1583/006).(Citation: FireEye APT29)

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Kill Chain Phases

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

## APTs (Intrusion Sets)

* APT29
* Aoqin Dragon
* Cleaver
* FIN13
* FIN7
* Indrik Spider
* Ke3chang
* Kimsuky
* Lazarus Group
* LuminousMoth
* Moonstone Sleet
* Moses Staff
* OilRig
* Play
* RedCurl
* Salt Typhoon
* Sandworm Team
* TeamTNT
* Turla