# TTP Detail – T1587.004

## TTP Information

Name: Exploits

Description: Adversaries may develop exploits that can be used during targeting. An exploit takes advantage of a bug or vulnerability in order to cause unintended or unanticipated behavior to occur on computer hardware or software. Rather than finding/modifying exploits from online or purchasing them from exploit vendors, an adversary may develop their own exploits.(Citation: NYTStuxnet) Adversaries may use information acquired via [Vulnerabilities](https://attack.mitre.org/techniques/T1588/006) to focus exploit development efforts. As part of the exploit development process, adversaries may uncover exploitable vulnerabilities through methods such as fuzzing and patch analysis.(Citation: Irongeek Sims BSides 2017)

As with legitimate development efforts, different skill sets may be required for developing exploits. 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 exploit development capabilities, provided the adversary plays a role in shaping requirements and maintains an initial degree of exclusivity to the exploit.

Adversaries may use exploits during various phases of the adversary lifecycle (i.e. [Exploit Public-Facing Application](https://attack.mitre.org/techniques/T1190), [Exploitation for Client Execution](https://attack.mitre.org/techniques/T1203), [Exploitation for Privilege Escalation](https://attack.mitre.org/techniques/T1068), [Exploitation for Defense Evasion](https://attack.mitre.org/techniques/T1211), [Exploitation for Credential Access](https://attack.mitre.org/techniques/T1212), [Exploitation of Remote Services](https://attack.mitre.org/techniques/T1210), and [Application or System Exploitation](https://attack.mitre.org/techniques/T1499/004)).

## Threat-Mapped Scoring

Score: 1.8

Priority: P4 - Informational (Low)

## Kill Chain Phases

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

## APTs (Intrusion Sets)

* Leviathan
* Volt Typhoon