# TTP Detail – T1496.001

## TTP Information

Name: Compute Hijacking

Description: Adversaries may leverage the compute resources of co-opted systems to complete resource-intensive tasks, which may impact system and/or hosted service availability.

One common purpose for [Compute Hijacking](https://attack.mitre.org/techniques/T1496/001) is to validate transactions of cryptocurrency networks and earn virtual currency. Adversaries may consume enough system resources to negatively impact and/or cause affected machines to become unresponsive.(Citation: Kaspersky Lazarus Under The Hood Blog 2017) Servers and cloud-based systems are common targets because of the high potential for available resources, but user endpoint systems may also be compromised and used for [Compute Hijacking](https://attack.mitre.org/techniques/T1496/001) and cryptocurrency mining.(Citation: CloudSploit - Unused AWS Regions) Containerized environments may also be targeted due to the ease of deployment via exposed APIs and the potential for scaling mining activities by deploying or compromising multiple containers within an environment or cluster.(Citation: Unit 42 Hildegard Malware)(Citation: Trend Micro Exposed Docker APIs)

Additionally, some cryptocurrency mining malware identify then kill off processes for competing malware to ensure it’s not competing for resources.(Citation: Trend Micro War of Crypto Miners)

## Threat-Mapped Scoring

Score: 1.8

Priority: P4 - Informational (Low)

## Kill Chain Phases

**•** mitre-attack: impact

## Malware

* Bonadan
* CookieMiner
* DarkGate
* Hildegard
* Kinsing
* LoudMiner
* Lucifer
* Skidmap

## Tools

* Imminent Monitor

## APTs (Intrusion Sets)

* APT41
* Blue Mockingbird
* Rocke
* TeamTNT