# TTP Detail – T1578.002

## TTP Information

Name: Create Cloud Instance

Description: An adversary may create a new instance or virtual machine (VM) within the compute service of a cloud account to evade defenses. Creating a new instance may allow an adversary to bypass firewall rules and permissions that exist on instances currently residing within an account. An adversary may [Create Snapshot](https://attack.mitre.org/techniques/T1578/001) of one or more volumes in an account, create a new instance, mount the snapshots, and then apply a less restrictive security policy to collect [Data from Local System](https://attack.mitre.org/techniques/T1005) or for [Remote Data Staging](https://attack.mitre.org/techniques/T1074/002).(Citation: Mandiant M-Trends 2020)

Creating a new instance may also allow an adversary to carry out malicious activity within an environment without affecting the execution of current running instances.

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Kill Chain Phases

**•** mitre-attack: defense-evasion

## APTs (Intrusion Sets)

* LAPSUS$
* Scattered Spider