# TTP Detail – T1578.004

## TTP Information

Name: Revert Cloud Instance

Description: An adversary may revert changes made to a cloud instance after they have performed malicious activities in attempt to evade detection and remove evidence of their presence. In highly virtualized environments, such as cloud-based infrastructure, this may be accomplished by restoring virtual machine (VM) or data storage snapshots through the cloud management dashboard or cloud APIs.

Another variation of this technique is to utilize temporary storage attached to the compute instance. Most cloud providers provide various types of storage including persistent, local, and/or ephemeral, with the ephemeral types often reset upon stop/restart of the VM.(Citation: Tech Republic - Restore AWS Snapshots)(Citation: Google - Restore Cloud Snapshot)

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Kill Chain Phases

**•** mitre-attack: defense-evasion