# TTP Detail – T1562.008

## TTP Information

Name: Disable or Modify Cloud Logs

Description: An adversary may disable or modify cloud logging capabilities and integrations to limit what data is collected on their activities and avoid detection. Cloud environments allow for collection and analysis of audit and application logs that provide insight into what activities a user does within the environment. If an adversary has sufficient permissions, they can disable or modify logging to avoid detection of their activities.

For example, in AWS an adversary may disable CloudWatch/CloudTrail integrations prior to conducting further malicious activity.(Citation: Following the CloudTrail: Generating strong AWS security signals with Sumo Logic) They may alternatively tamper with logging functionality – for example, by removing any associated SNS topics, disabling multi-region logging, or disabling settings that validate and/or encrypt log files.(Citation: AWS Update Trail)(Citation: Pacu Detection Disruption Module) In Office 365, an adversary may disable logging on mail collection activities for specific users by using the `Set-MailboxAuditBypassAssociation` cmdlet, by disabling M365 Advanced Auditing for the user, or by downgrading the user’s license from an Enterprise E5 to an Enterprise E3 license.(Citation: Dark Reading Microsoft 365 Attacks 2021)

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Kill Chain Phases

**•** mitre-attack: defense-evasion

## Tools

* Pacu

## APTs (Intrusion Sets)

* APT29