Table of Contents

Detection: O365 Disable MFA

Updated Date: 2024-05-11 ID: c783dd98-c703-4252-9e8a-f19d9f5c949e Author: Rod Soto, Splunk Type: TTP

Product: Splunk Enterprise Security

Description

The following analytic identifies instances where Multi-Factor Authentication (MFA) is disabled for a user within the Office 365 environment. It leverages O365 audit logs, specifically focusing on events related to MFA settings. Disabling MFA removes a critical security layer, making accounts more vulnerable to unauthorized access. If confirmed malicious, this activity could indicate an attacker attempting to maintain persistence or an insider threat, significantly increasing the risk of unauthorized access. Immediate investigation is required to validate the reason for disabling MFA, potentially re-enable it, and assess any other suspicious activities related to the affected account.

Search

```
SPL
`o365_management_activity` Operation="Disable Strong Authentication."
| stats count earliest(_time) as firstTime latest(_time) as lastTime by UserType Operation UserId ResultStatus obje
ct
| rename UserType AS user_type, Operation AS action, UserId AS src_user, object AS user, ResultStatus AS result
| `security_content_ctime(firstTime)`
| `security_content_ctime(lastTime)`
| `o365_disable_mfa_filter`
```

Data Source

Name	Platform	Sourcetype	Source	Supported App
O365 Disable Strong Authentication.	N/A	'o365:management:activity'	'o365'	N/A

Macros Used

Name	Value
o365_management_activity	sourcetype=o365:management:activity
o365_disable_mfa_filter	search *

o365_disable_mfa_filter is an empty macro by default. It allows the user to filter out any results (false positives) without editing the SPL.

Annotations

- MITRE ATT&CK + KILL CHAIN PHASES + NIST + CIS - THREAT ACTORS

ID	Technique	Tactic
T1556	Modify Authentication Process	Credential Access

FIN13

Default Configuration

This detection is configured by default in Splunk Enterprise Security to run with the following settings:

Setting	Value
Disabled	true
Cron Schedule	`0 * * * *`
Earliest Time	`-70m@m`
Latest Time	`-10m@m`
Schedule Window	`auto`
Creates Notable	Yes
Rule Title	`%name%`
Rule Description	`%description%`
Notable Event Fields	user, dest
Creates Risk Event	True

> This configuration file applies to all detections of type TTP. These detections will use Risk Based Alerting and generate Notable Events.

Implementation

You must install the Splunk Microsoft Office 365 add-on. This search works with o365:management:activity

Known False Positives

Unless it is a special case, it is uncommon to disable MFA or Strong Authentication

Associated Analytic Story

- Office 365 Persistence Mechanisms

Risk Based Analytics (RBA)

Risk Message	Risk Score	Impact	Confidence
User src_user has executed an operation $action$ for user $user$	64	80	80

> The Risk Score is calculated by the following formula: Risk Score = (Impact * Confidence/100). Initial Confidence and Impact is set by the analytic author.

References

- https://attack.mitre.org/techniques/T1556/

Detection Testing

Test Type	Status	Dataset	Source	Sourcetype
Validation	☑ Passing	N/A	N/A	N/A
Unit	☑ Passing	Dataset	`o365`	`o365:management:activity`
Integration	☑ Passing	Dataset	`o365`	`o365:management:activity`

Replay any dataset to Splunk Enterprise by using our `replay.py` tool or the UI. Alternatively you can replay a dataset into a Splunk Attack Range

Source: GitHub | Version: **3**

← Detection: O365 A...

Detection: O365 F... →