

Search site

Analytic Stories

Detections

Playbooks Data Sources

Blog

About



Table of Contents

Description

Search

Data Source

Macros Used

Annotations

Default Configuration

Implementation

Known False Positives

Associated Analytic Story

Risk Based Analytics (RBA)

References

Detection Testing

Detection: O365 New Federated Domain Added

Updated Date: 2024-05-28 ID: e155876a-6048-11eb-ae93-0242ac130002 Author: Rod Soto, Mauricio Velazco Splunk

Type: TTP

Product: Splunk Enterprise Security

Description

The following analytic identifies the addition of a new federated domain in an Office 365 environment. This behavior is detected by analyzing Office 365 management activity logs, specifically filtering for Workload=Exchange and Operation="Add-FederatedDomain". The addition of a new federated domain is significant as it may indicate unauthorized changes or potential compromises. If confirmed malicious, attackers could establish a backdoor, bypass security measures, or exfiltrate data, leading to data breaches and unauthorized access to sensitive information. Immediate investigation is required to review the details of the added domain and any concurrent suspicious activities.

Search

```
`o365_management_activity` Operation IN ("*add*", "*new*") AND Operation="*domain*"

| stats count values(ModifiedProperties{}.NewValue) as new_value by user user_agent authentication_service action Workload Operation

| `security_content_ctime(firstTime)`
| `security_content_ctime(lastTime)`
| `o365_new_federated_domain_added_filter`
```

Data Source

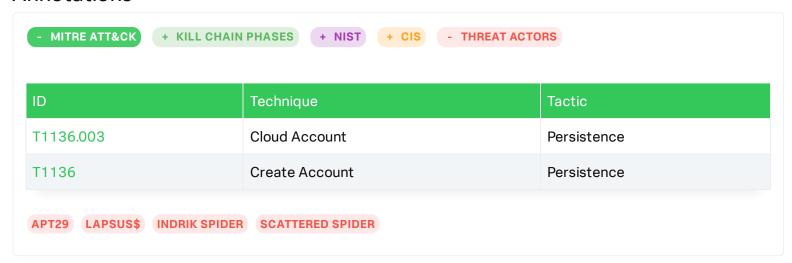
Name	Platform	Sourcetype	Source	Supported App
0365	N/A	'o365:management:activity'	'0365'	N/A

Macros Used

Name	Value	
o365_management_activity	sourcetype=o365:management:activity	
o365_new_federated_domain_added_filter	search *	

o365_new_federated_domain_added_filter is an empty macro by default. It allows the user to filter out any results (false positives) without editing the SPL.

Annotations



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 splunk Microsoft Office 365 add-on. This search works with o365:management:activity.

Known False Positives

The creation of a new Federated domain is not necessarily malicious, however these events need to be followed closely, as it may indicate federated credential abuse or backdoor via federated identities at a similar or different cloud provider.

Associated Analytic Story

- Cloud Federated Credential Abuse
- Office 365 Persistence Mechanisms

Risk Based Analytics (RBA)

Risk Message	Risk Score	Impact	Confidence
User \$user\$ has added a new federated domain \$new_value\$	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://www.fireeye.com/content/dam/fireeye-www/blog/pdfs/wp-m-unc2452-2021-000343-01.pdf
- https://www.cisa.gov/uscert/ncas/alerts/aa21-008a
- https://www.splunk.com/en_us/blog/security/a-golden-saml-journey-solarwinds-continued.html
- https://blog.sygnia.co/detection-and-hunting-of-golden-saml-attack?hsLang=en
- https://o365blog.com/post/aadbackdoor/

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: 4

← Detection: Networ...

Detection: Okta ID...

 $@\ 2005$ - 2024 Splunk LLC All rights reserved.