Detecting Office 365 attacks

Applicability

- Product: Splunk Cloud Platform or Splunk Enterprise
- Feature: Monitoring
- Technology: Splunk Add-on for Microsoft Office 365
- Data: Office 365

Scenario

You manage access to Office 365 resources and services across your organization. More and more companies are using Microsoft's Office 365 cloud offering, and yours is no exception. Attacks against Office 365 are increasing, and as part of your role you need to be able to detect these. These searches allow you to do this.

- To run these searches you must install the Splunk Add-on for Microsoft Office 365. These searches work with o365:management:activity.
- Some commands, parameters, and field names in the searches below may need to be adjusted to match your environment. In addition, to optimize the searches shown below, you should specify an index and a time range when appropriate.

Detection searches

► New Federation creation - Add app role assignment grant to user

This search detects the creation of a new Federation setting by alerting about an specific event related to its creation, called Add app role assignment grant to user.

This search may result in some false positives since the creation of a new Federation is not necessarily malicious. These events still need to be followed closely, as they may indicate federated credential abuse or backdoor via federated identities at a different cloud provider.

```
| search (Operation="Add app role assignment grant to user." Workload=AzureActiveDirectory sourcetype=o365:management:activity)
| stats count min(_time) AS firstTime max(_time) AS lastTime values(Actor{}.ID) AS Actor.ID values(Actor{}.Type) AS Actor.Type BY ActorIpAddress dest ResultStatus
| convert timeformat="%Y-%m-%dT%H:%M:%S" ctime(firstTime)
| convert timeformat="%Y-%m-%dT%H:%M:%S" ctime(lastTime)
```
New Federation creation - Add service principal credentials

This search detects the creation of a new Federation setting by alerting about a specific event related to its creation, called Add service principal credentials.

This search may result in some false positives since the creation of a new Federation is not necessarily malicious. These events still need to be followed closely, as they may indicate federated credential abuse or backdoor via federated identities at a different cloud provider.

Bypass Multi-Factor Authentication (MFA) via trusted IP

This search detects newly added IP addresses/CIDR blocks to the list of Multifactor Authentication (MFA) trusted IPs to bypass MFA. Attackers are often known to use this technique so that they can bypass the MFA system.

Multi-Factor Authentication (MFA) disabled

This search detects when Multi-Factor Authentication (MFA) has been disabled, what entity performed the action, and against what user.
► Excessive authentication failures and attempts against Multi-Factor Authentication (MFA) prompt codes

This search detects when an excessive number of authentication failures occur. The search also detects attempts against Multi-Factor Authentication (MFA) prompt codes.

The threshold for alerting used here is above 10 attempts, which should reduce the number of false positives.

```
| search (UserAuthenticationMethod=* Workload=AzureActiveDirectory sourcetype=o365:management:activity status=Failed) 
| stats count earliest(_time) AS firstTime latest(_time) values(UserAuthenticationMethod) AS UserAuthenticationMethod values(UserAgent) AS UserAgent values(status) AS status values(src_ip) AS src_ip by user 
| where (count > 10) 
| convert timeformat="%Y-%m-%dT%H:%M:%S" ctime(firstTime) 
| convert timeformat="%Y-%m-%dT%H:%M:%S" ctime(lastTime)
```

► Excessive Single Sign-On (SSO) login errors

This search detects accounts with a high number of single sign-on (SSO) logon errors. Excessive logon errors may indicate attempts to brute force a password, or SSO token hijack or reuse.

False positives may occur with this search as logon errors may not be malicious in nature. They may, however, indicate attempts to reuse a token or password obtained via credential access attack.

```
| search (LogonError=SsoArtifactInvalidOrExpired Workload=AzureActiveDirectory sourcetype=o365:management:activity) 
| stats count min(_time) AS firstTime max(_time) AS lastTime BY LogonError ActorIpAddress UserAgent UserId 
| where (count > 5) 
| convert timeformat="%Y-%m-%dT%H:%M:%S" ctime(firstTime) 
| convert timeformat="%Y-%m-%dT%H:%M:%S" ctime(lastTime)
```

► New Federated domain added

This search detects the addition of a new Federated domain.

This search may result in some false positives since the creation of a new Federation is not necessarily malicious. These events still need to be followed closely, as they may indicate federated credential abuse or backdoor via federated identities at a similar or different cloud provider.

```
| search (Operation="Add-FederatedDomain" Workload=Exchange sourcetype=o365:management:activity) 
| stats count min(_time) AS firstTime max(_time) AS lastTime values(Parameters{}.Value) AS Parameters. Value BY ObjectId Operation OrganizationName OriginatingServer UserId UserKey 
| convert timeformat="%Y-%m-%dT%H:%M:%S" ctime(firstTime) 
| convert timeformat="%Y-%m-%dT%H:%M:%S" ctime(lastTime)
```

► PST file export alert

This search detects when a user has performed an eDiscovery search or exported a personal storage table (PST)
file from the search. This PST file usually includes sensitive information, including email body content.

This search may result in some false positives since PST export can be done for legitimate purposes. However, due to the sensitive nature of its content, it should be monitored.

| search (Category=ThreatManagement Name="eDiscovery search started or exported" sourcetype=o365:management:activity) |
| stats count earliest(_time) AS firstTime latest(_time) AS lastTime BY Source Severity AlertEntityId Operation Name |
| convert timeformat="%Y-%m-%dT%H:%M:%S" ctime(firstTime) |
| convert timeformat="%Y-%m-%dT%H:%M:%S" ctime(lastTime) |

► Suspicious admin email forwarding

This search detects when an admin configured a forwarding rule for multiple mailboxes to the same destination.

| search (Operation=Set-Mailbox sourcetype=o365:management:activity) |
| spath input=Parameters |
| search ForwardingAddress=* |
| rename Identity AS src_user |
| stats dc(src_user) AS count_src_user earliest(_time) AS firstTime latest(_time) AS lastTime values(src_user) AS src_user values(user) AS user by ForwardingAddress |
| where (count_src_user > 1) |
| convert timeformat="%Y-%m-%dT%H:%M:%S" ctime(firstTime) |
| convert timeformat="%Y-%m-%dT%H:%M:%S" ctime(lastTime) |

► Suspicious rights delegation

This search detects the assignment of rights to access content from another mailbox. This is usually only assigned to a service account.

| search (Operation=Add-MailboxPermission sourcetype=o365:management:activity) |
| spath input=Parameters |
| search (AccessRights=FullAccess OR AccessRights=SendAs OR AccessRights=SendOnBehalf) |
| rename User AS src_user, Identity AS dest_user |
| stats count earliest(_time) AS firstTime latest(_time) AS lastTime BY user src_user dest_user Operation AccessRights |
| convert timeformat="%Y-%m-%dT%H:%M:%S" ctime(firstTime) |
| convert timeformat="%Y-%m-%dT%H:%M:%S" ctime(lastTime) |

► Suspicious user email forwarding

This search detects the assignment of rights to access content from another mailbox. This is usually only assigned to a service account.

| search (Operation=Set-Mailbox sourcetype=o365:management:activity) |
| spath input=Parameters |
| search ForwardingSmtpAddress=* |
| rename Identity AS src_user |

The information provided in Splunk Lantern is intended for informational and educational purposes only. All information is provided in good faith, however, Splunk disclaims any and all representations and warranties, express and implied, regarding the information provided, including without limitation any warranties and representations regarding the completeness, adequacy or accuracy of the information. You agree to take full responsibility for the results arising from the use of the information provided.
Additional resources

This use case is included within Splunk Enterprise Security, a Splunk app that provides prebuilt content and searches to help answer root-cause questions in real-time about malicious and anomalous events in your IT infrastructure. In addition, Splunk Enterprise Security provides a number of other searches to help reinforce your Cloud Security posture, including:

- Detecting AWS cross-account activity
- Detecting AWS network ACL activity
- Detecting AWS suspicious provisioning activities
- Monitoring user activity spikes in AWS
- Monitoring AWS EC2 for suspicious login activities
- Monitoring AWS S3 for suspicious activities
- Monitoring AWS for suspicious traffic
- Monitoring AWS EC2 for unusual modifications

The information provided in Splunk Lantern is intended for informational and educational purposes only. All information is provided in good faith, however, Splunk disclaims any and all representations and warranties, express and implied, regarding the information provided, including without limitation any warranties and representations regarding the completeness, adequacy or accuracy of the information. You agree to take full responsibility for the results arising from the use of the information provided.