Detecting cloud federated credential abuse in Microsoft Office and Azure Active Directory

Applicability

- Product: Splunk Cloud Platform or Splunk Enterprise
- Data: Office 365
- Data: Microsoft Azure Active Directory
- Function: Monitoring

Scenario

You need to be able to detect events that indicate abuse of cloud federated credentials. These credentials are usually extracted from endpoint desktops or servers that provide federation services such as Windows Active Directory Federation Services. Identity federation relies on objects such as Oauth2 tokens, cookies, or SAML assertions in order to provide seamless access between cloud and perimeter environments. If these objects are either hijacked or forged, then attackers are able to pivot into your cloud environment.

This use case contains searches that detect abnormal processes which may indicate the extraction of federated directory objects such as passwords, Oauth2 tokens, certificates, and keys, as well as searches relating to cloud environment events.

- Some commands, parameters, and field names in the searches below may need to be adjusted to match your environment.
- To optimize the searches shown below, you should specify an index and a time range when appropriate.

Detection searches

► Certutil exe certificate extraction

Content developed by the Splunk Security Research team requires the use of consistent, normalized data provided by the Common Information Model (CIM). This search requires the Endpoint data model. For information on installing and using the CIM, see the Common Information Model documentation.

This search looks for arguments to certutil.exe that indicate the manipulation or extraction of the certificate. This certificate can then be used to sign new authentication tokens, especially inside federated environments such as Windows ADFS.
Unless there are specific use cases, manipulating or exporting certificates using `certutil` is uncommon. Extraction of a certificate has been observed during attacks such as Golden SAML and other campaigns targeting federated services.

```
| rename "Processes." AS "*" |
| convert timeformat="%Y-%m-%dT%H:%M:%S" ctime(firstTime) |
| convert timeformat="%Y-%m-%dT%H:%M:%S" ctime(lastTime) |
```

**► Office 365 add app role assignment grant to user**

To successfully implement this search, you must install the Splunk Add-on for Microsoft Office 365. This search works with `o365:management:activity`.

This search detects instances when the operation Add app role assignment grant to user has been carried out. These activities may not necessarily be malicious, however they should be monitored closely.

```
| 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) |
```

**► Office 365 added service principal**

To successfully implement this search, you must install the Splunk Add-on for Microsoft Office 365. This search works with `o365:management:activity`.

This search detects instances when service principal credentials are added. These activities may not necessarily be malicious, however they should be monitored closely.

```
| search (Workload=AzureActiveDirectory signature="Add service principal credentials." sourcetype=o365:management:activity) |
| stats min(_time) AS firstTime max(_time) AS lastTime values(Actor{}.ID) AS Actor.ID |
| values(ModifiedProperties{}.Name) AS ModifiedProperties.Name values(ModifiedProperties{}.NewValue) AS ModifiedProperties.NewValue values(Target{}.ID) AS Target.ID BY ActorIpAddress signature |
| convert timeformat="%Y-%m-%dT%H:%M:%S" ctime(firstTime) |
| convert timeformat="%Y-%m-%dT%H:%M:%S" ctime(lastTime) |
```

**► Office 365 excessive SSO logon errors**

To successfully implement this search, you must install the Splunk Add-on for Microsoft Office 365. This search...
works with `o365:management:activity`.

This search detects accounts with high number of Single Sign On (SSO) logon errors. Excessive logon errors may indicate attempts to bruteforce passwords, or indicate SSO token hijack or reuse.

Logon errors may not be malicious in nature, however they may indicate attempts to reuse a token or password obtained via credential access attack.

```plaintext
| 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)  
```

► **Office 365 new federated domain added**

To successfully implement this search, you must install the [Splunk Add-on for Microsoft Office 365](https://www.splunk.com). This search works with `o365:management:activity`.

This search detects the addition of a new federated domain.

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

```plaintext
| 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)  
```

► **Registry keys used for privilege escalation**

- To successfully implement this search, ensure that your deployment is ingesting data that records registry activity from your hosts to populate the Endpoint data model in the registry node. This is typically populated via endpoint detection-and-response products, such as [Carbon Black](https://www.carbonblack.com), or endpoint data sources, such as [Sysmon](https://docs.microsoft.com/en-us/sysmon). The data used for this search is typically generated via logs that report reads and writes to the registry.
- Click [here](#) for a full explanation of how this search works.

This search looks for modifications to registry keys that can be used to elevate privileges. The registry keys under "Image File Execution Options" are used to intercept calls to an executable and can be used to attach malicious binaries to benign system binaries.

False positives from this search may occur since there are many legitimate applications that must execute upon system startup and will use these registry keys to accomplish that task.
tstats summariesonly=true allow_old_summaries=true count values(Registry.registry_key_name) AS registry_key_name values(Registry.registry_path) AS registry_path min(_time) AS firstTime max(_time) AS lastTime FROM datamodel=Endpoint.Registry where (Registry.registry_path="*Microsoft\Windows NT\CurrentVersion\Image File Execution Options*") AND (Registry.registry_key_name=GlobalFlag OR Registry.registry_key_name=Debugger) BY Registry.dest Registry.user | convert timeformat="%m/%d/%Y %H:%M:%S" ctime(lastTime) | convert timeformat="%m/%d/%Y %H:%M:%S" ctime(firstTime) | rename "Registry.*" AS "*"

---

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 suspicious provisioning activities
- Detecting Google Cloud Platform (GCP) cross-account activity
- Detecting Office 365 attacks
- Detecting privilege escalation in your AWS environment
- Detecting suspicious cloud authentication activities
- Monitoring user activity spikes in AWS

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.