Detecting cloud federated credential abuse in AWS

Applicability

- **Product:** Splunk Cloud Platform or Splunk Enterprise
- **Feature:** [Splunk App for AWS](https://app.splunk.com/app/76418) and [Splunk Add-on for AWS](https://app.splunk.com/app/76417)
- **Data:** Amazon Web Services: CloudTrail
- **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. 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

**Detect AWS SAML access**

To run this search, install the Splunk App for AWS (version 5.1.0 or later) and Splunk Add-on for AWS (version 4.4.0 or later), then configure your [CloudTrail inputs](https://app.splunk.com/app/76417).

You can use this search to detect abnormal AWS SAML access, or credential hijacking or forgery in federated environments using SAML protocol inside the perimeter or cloud provider.

```
| search (eventName=Assumerolewithsaml sourcetype=aws:cloudtrail) | stats count min(_time) AS firstTime max(_time) AS lastTime BY requestParameters.principalArn requestParameters.roleArn requestParameters.roleSessionName recipientAccountId responseElements.issuer sourceIPAddress userAgent
```

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.
AWS SAML update identity provider

To run this search, install the Splunk App for AWS (version 5.1.0 or later) and Splunk Add-on for AWS (version 4.4.0 or later), then configure your CloudTrail inputs.

This search detects updates to a SAML provider in AWS. Updates to a SAML provider need to be monitored closely as they may indicate possible perimeter compromise of federated credentials, or backdoor access from another cloud provider set by the attacker.

This search may return false positives since updating a SAML provider or creating a new one may not necessarily be malicious.

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.

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, or endpoint data sources, such as 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.