Newly added Active Directory credentials

An Azure service principal is an identity that has access to an application, such as Active Directory. You might need to look for new Active Directory credentials granted to an existing service principal when doing the following:

- Detecting lateral movement with Active Directory data

Prerequisites

In order to execute this procedure in your environment, the following data, services, or apps are required:

- Splunk Enterprise or Splunk Cloud Platform
- Microsoft Azure Active Directory audit data
- Microsoft Azure Add-on for Splunk

Example

Your company uses SolarWinds Orion business software, which suffered the Sunburst Backdoor attack. You want to identify any lateral movement associated with attack by seeing if new Active Directory credentials have been granted to an existing service principal.

To optimize the search shown below, you should specify an index and a time range.

1. Run the following search:

   | sourcetype="azure:aad:audit" activityDisplayName="Add service principal credentials"

Search explanation

The table provides an explanation of what each part of this search achieves. You can adjust this query based on the specifics of your environment.

<table>
<thead>
<tr>
<th>Splunk Search</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>sourcetype=&quot;azure:aad:audit&quot;</td>
<td>Search only Azure Active Directory audit data.</td>
</tr>
<tr>
<td>activityDisplayName=&quot;Add service principal credentials&quot;</td>
<td>Search for the &quot;add service principal credentials&quot; action.</td>
</tr>
</tbody>
</table>

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.
Result

After identifying new credentials added to existing service principals, you might also want to search for newly added service principals. Additionally, the Microsoft Azure Add-on for Splunk has searches and pre-built security content for Azure data that can help you interpret these results and take additional steps to resolve security concerns related to newly added Active Directory credentials.