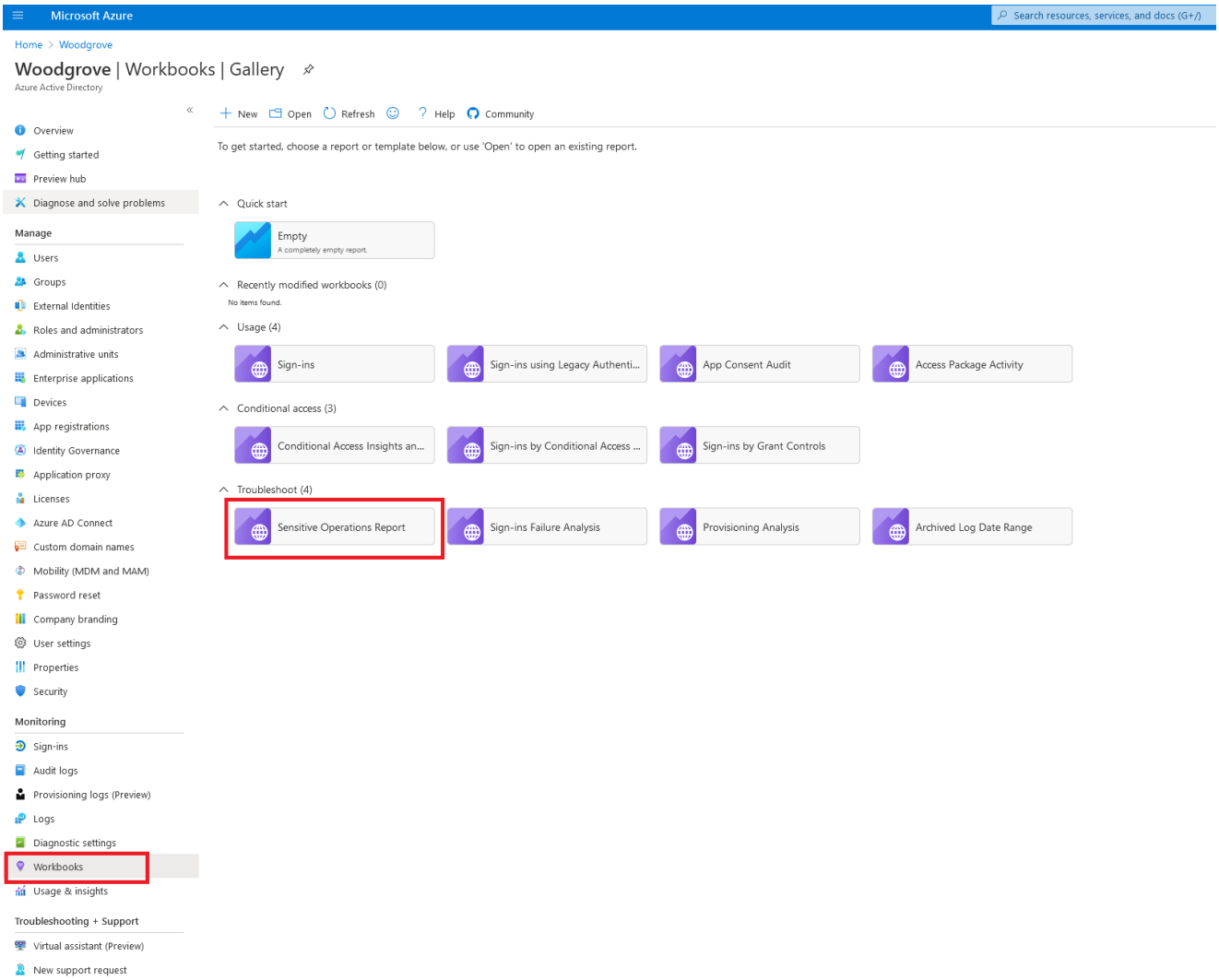
Azure AD workbook to help you assess Solorigate risk

techcommunity.microsoft.com/t5/azure-active-directory-identity/azure-ad-workbook-to-help-you-assess-solorigate-risk/ba-p/2010718

December 22, 2020



Dec 22 2020 01:42 PM

In the interest of helping customers concerned about the Solorigate attacks we are publishing a new workbook in the Azure AD admin portal to assist investigations into the Identity Indicators of Compromise related to the attacks. The information in this workbook is available in Azure AD audit and sign in logs, but the workbook helps you collect and visualize the information in one view.

The workbook is split into 4 sections, each aimed at providing information associated with the attack patterns we have identified:

1. Modified application and service principal credentials/authentication methods

2. Modified federation settings
3. New permissions granted to service principals
4. Directory role and group membership updates for service principals

First, we'll detail how to access the workbook and then walk through each of these in turn.

Check out this cool video to see it in action!

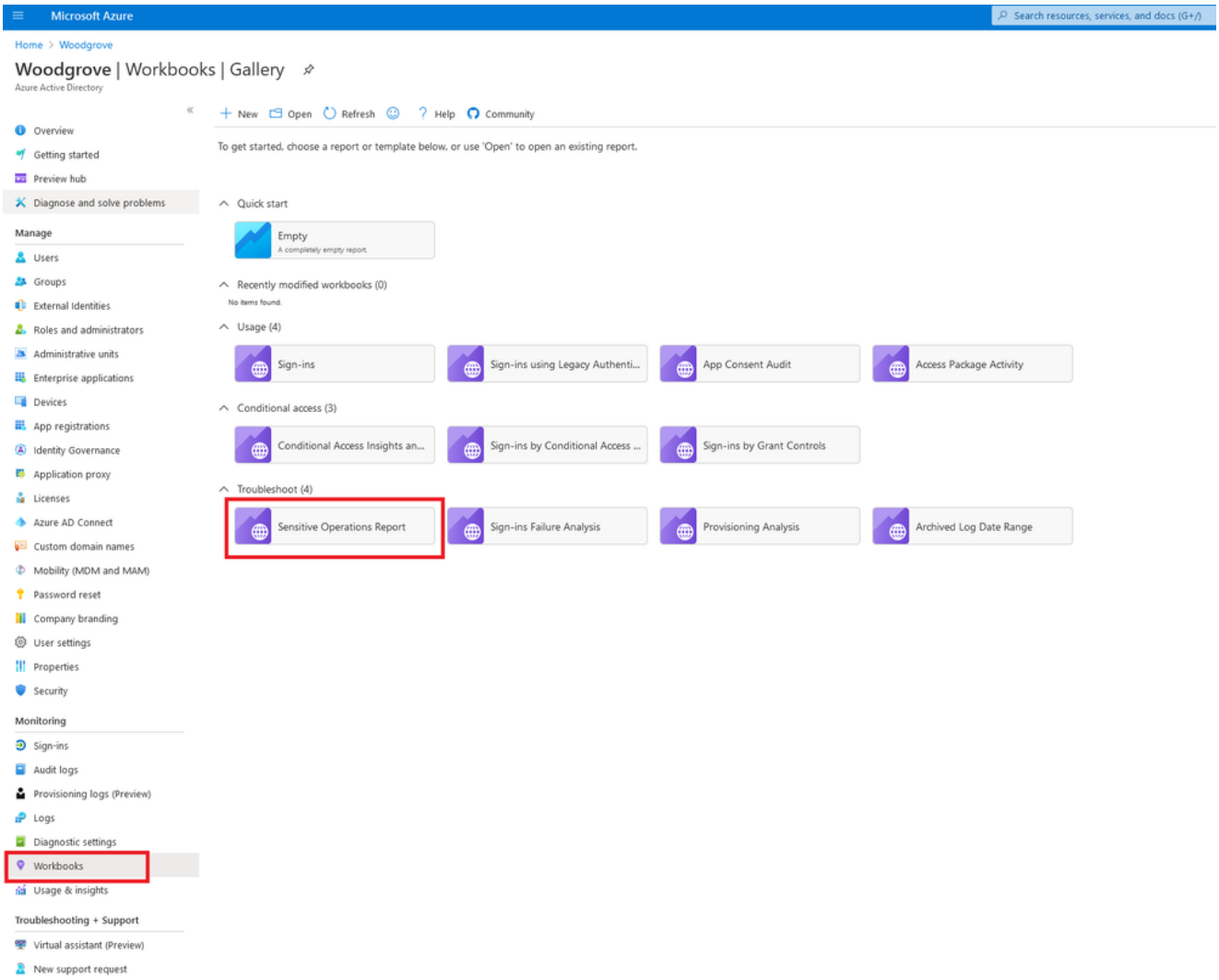
Accessing the workbook

If you organization is new to Azure Monitor workbooks, you'll need to integrate your Azure AD sign-in and audit logs with Azure Monitor before accessing the workbook. This allows you to store, and query, and visualize your logs using workbooks for up to 2 years. Only sign-in and audit events created *after* Azure Monitor integration will be stored, so the workbook will not contain insights prior to that date. Learn more about the prerequisites to Azure Monitor workbooks for Azure Active Directory. If you have previously integrated your Azure AD sign-in and audit logs with Azure Monitor, you can use the workbook to assess past information.

To access the workbook:

1. Sign into the Azure portal
2. Navigate to **Azure Active Directory** > **Monitoring** > **Workbooks**

In the Troubleshoot section, open the **Sensitive Operations Report**



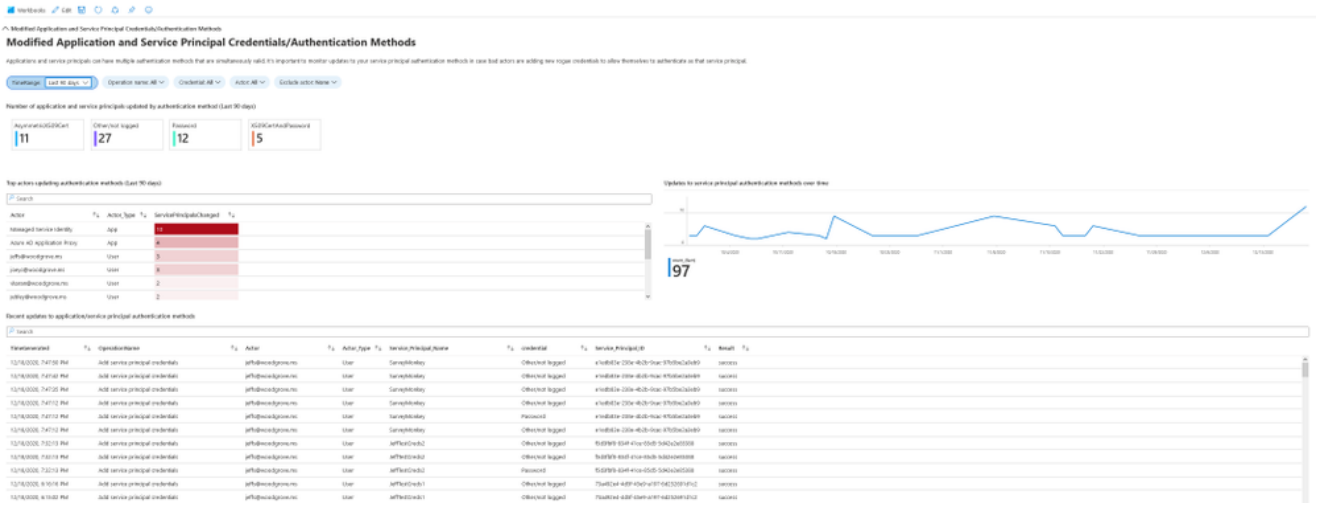
Modified application and service principal credentials/authentication methods

One of the most common ways for attackers to gain persistence in the environment is by adding new credentials to existing applications and service principals. This allows the attacker to authenticate as the target application or service principal, granting them access to all resources to which it has permissions.

This section includes the following data to help you detect such actions:

- All new credentials added to apps and service principals, including the credential type
- Top actors and the amount of credentials modifications they performed
- A timeline for all credential changes

You can use the filters present in this section to further investigate any of the suspicious actors or service principals that were modified.



For more information: Apps & service principals in Azure AD - Microsoft identity platform

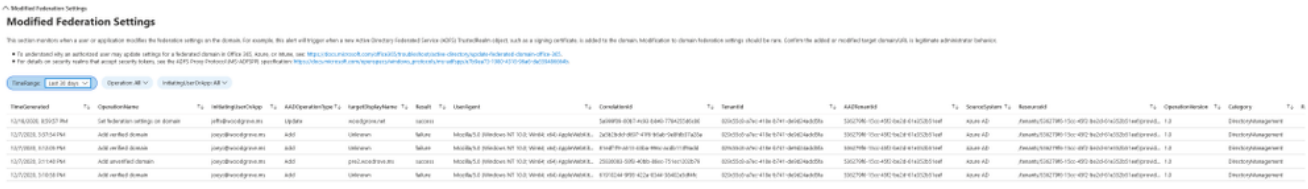
Modified federation settings

Another common approach to gaining a long-term foothold in the environment is modifying the tenant's federated domain trusts and effectively adding an additional, attacker controlled, SAML IDP as a trusted authentication source.

This section includes the following data:

- Changes performed to existing domain federation trusts
- Addition of new domains and trusts

Any actions which modify or add domain federation trusts are rare and should be treated as high fidelity to be investigated as soon as possible.

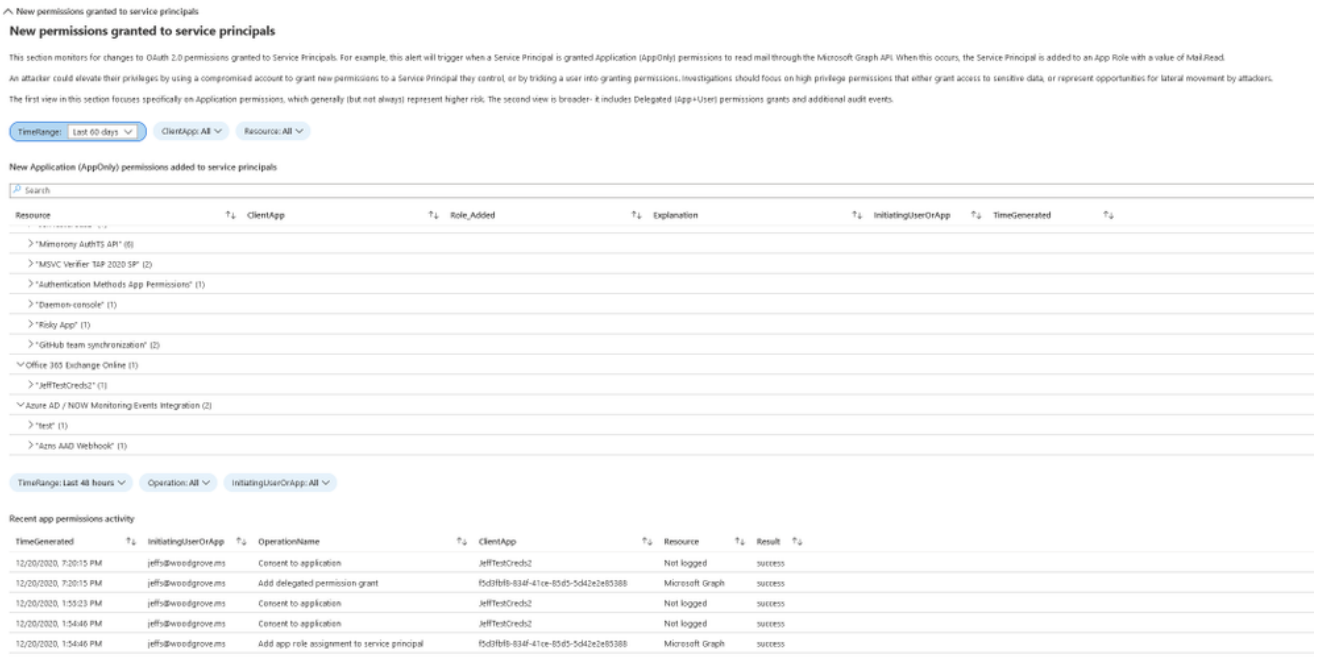


For more information: What is federation with Azure AD?

New permissions granted to service principals

In cases where the attacker cannot find a service principal or an application with a high privilege set of permissions through which to gain access, they will often attempt to add the permissions to another service principal or app.

This section includes a breakdown of the AppOnly permissions grants to existing service principals. Admins should investigate any instances of excessive high permissions being granted, including, but not limited to, Exchange Online, Microsoft Graph and Azure AD Graph.



For more information: Microsoft identity platform scopes, permissions, and consent

Directory role and group membership updates for service principals

Following the logic of the attacker adding new permissions to existing service principals and applications, another approach is adding them to existing directory roles or groups.

This section includes an overview of all changes made to service principal memberships and should be reviewed for any additions to high privilege roles and groups.

Conclusion

This workbook includes an overview of some of the common attack patterns in AAD, not only in Solorigate, and should be used as an investigation aid in conjunction with the steps described in the articles linked at the beginning to ensure your environment is safe and protect is from malicious actors.

For additional hunting with Azure Sentinel see http://aka.ms/sentinelsolorigatehunt.

The Solarwinds attack is an ongoing investigation, and our teams continue to act as first responders to these attacks. As new information becomes available, we will make updates through our Microsoft Security Response Center (MSRC) blog at https://aka.ms/solorigate.

Please reach out to me on twitter at @Alex_t_weinert if you have questions or suggestions for improvement.