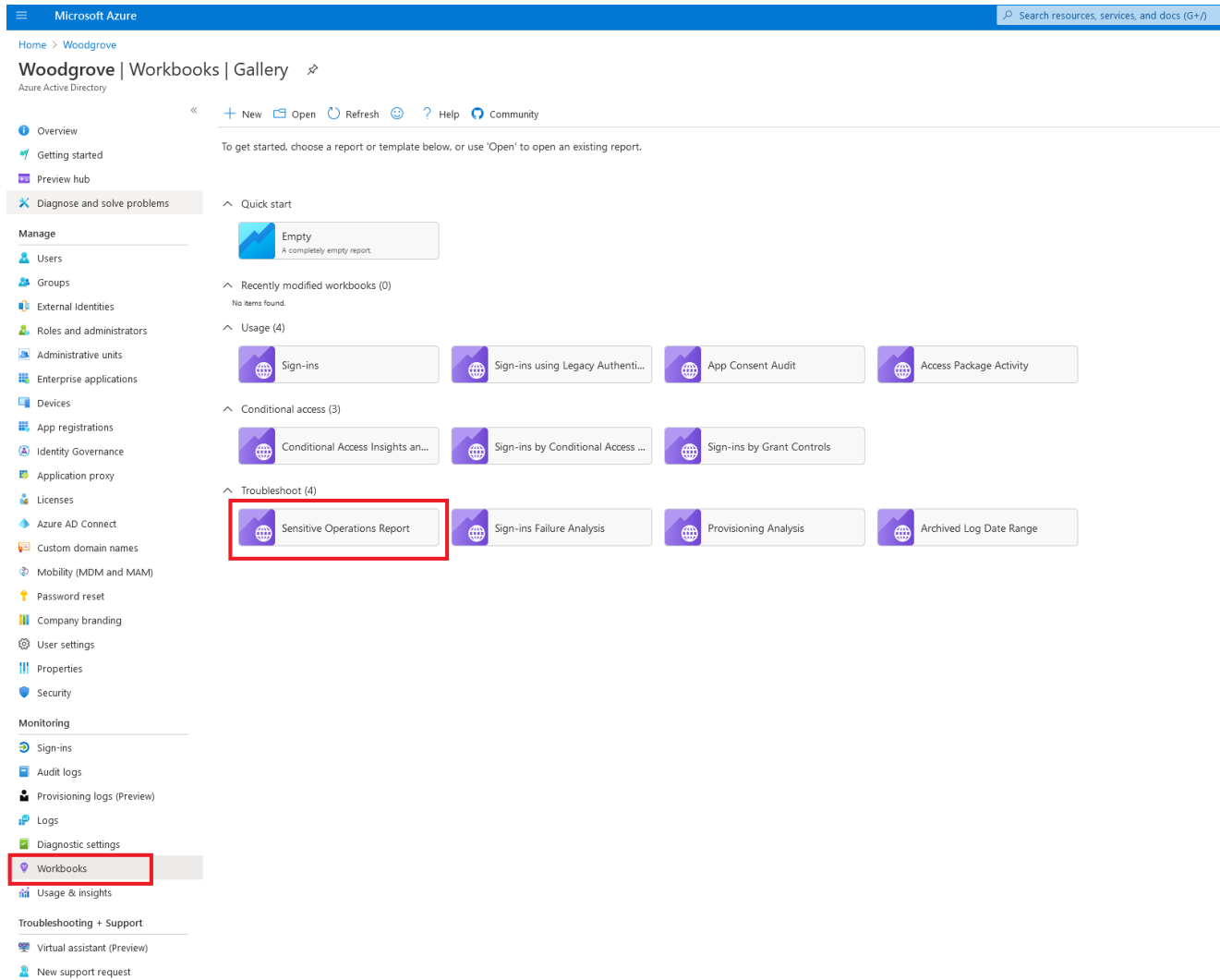


Azure AD workbook to help you assess Solorigate risk

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 your 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**

The screenshot shows the Microsoft Azure portal interface. At the top, there is a search bar and navigation links. The left-hand navigation pane is expanded to show the 'Workbooks' section, which is highlighted with a red rectangular box. The main content area displays a grid of report templates. Under the 'Troubleshoot (4)' category, the 'Sensitive Operations Report' template is highlighted with a red rectangular box. Other visible templates include 'Sign-ins', 'Sign-ins using Legacy Authent...', 'App Consent Audit', 'Access Package Activity', 'Conditional Access Insights an...', 'Sign-ins by Conditional Access ...', 'Sign-ins by Grant Controls', 'Sign-ins Failure Analysis', 'Provisioning Analysis', and 'Archived Log Date Range'.

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.

^ New permissions granted to service principals

New permissions granted to service principals

This section monitors for changes to OAuth 2.0 permissions granted to Service Principals. For example, this alert will trigger when a Service Principal is granted Application (AppOnly) permissions to read mail through the Microsoft Graph API. When this occurs, the Service Principal is added to an App Role with a value of Mail.Read.

An attacker could elevate their privileges by using a compromised account to grant new permissions to a Service Principal they control, or by tricking a user into granting permissions. Investigations should focus on high privilege permissions that either grant access to sensitive data, or represent opportunities for lateral movement by attackers.

The first view in this section focuses specifically on Application permissions, which generally (but not always) represent higher risk. The second view is broader - it includes Delegated (App+User) permissions grants and additional audit events.

TimeRange: Last 60 days | ClientApp: All | Resource: All

New Application (AppOnly) permissions added to service principals

Search

Resource	ClientApp	Role_Added	Explanation	InitiatingUserOrApp	TimeGenerated
> "Mimemory Authn API" (8)					
> "MSVC Verifier TSP 2020 SP" (2)					
> "Authentication Methods App Permissions" (1)					
> "Daemon-console" (1)					
> "Relay App" (1)					
> "GitHub team synchronization" (2)					
> "Office 365 Exchange Online" (1)					
> "JeffTestCred2" (1)					
> "Azure AD / NOW Monitoring Events Integration" (2)					
> "test" (1)					
> "Azro AAD Webhook" (1)					

TimeRange: Last 48 hours | Operation: All | InitiatingUserOrApp: All

Recent app permissions activity

TimeGenerated	InitiatingUserOrApp	OperationName	ClientApp	Resource	Result
12/20/2020, 7:20:15 PM	jeff@woodgrove.ms	Consent to application	JeffTestCred2	Not logged	success
12/20/2020, 7:20:15 PM	jeff@woodgrove.ms	Add delegated permission grant	f5d3fbf-634f-41ce-85d5-5d42c2e85388	Microsoft Graph	success
12/20/2020, 1:53:23 PM	jeff@woodgrove.ms	Consent to application	JeffTestCred2	Not logged	success
12/20/2020, 1:54:40 PM	jeff@woodgrove.ms	Consent to application	JeffTestCred2	Not logged	success
12/20/2020, 1:54:46 PM	jeff@woodgrove.ms	Add app role assignment to service principal	f5d3fbf-634f-41ce-85d5-5d42c2e85388	Microsoft Graph	success

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.

^ Directory role and group membership updates to service principals

Directory role and group membership updates to service principals

This section monitors for Service Principals being added as members of Directory Roles (admin roles) or Groups. For example, this alert will trigger when a Service Principal is added to the Company Administrator or Application Administrator role.

An attacker could elevate their privileges by adding a Service Principal they control to a high privileged role or a group that is used to protect access to sensitive resources. Investigations should focus on administrator roles and Groups that either grant access to sensitive data or represent opportunities for lateral movement by attackers.

TimeRange: Last 90 days | Operation: Add member to role | InitiatingUserOrApp: All

TimeGenerated	InitiatingUserOrApp	OperationName	ServicePrincipalDisplayName	GroupOrRoleNameAdd...
12/20/2020, 7:46:25 PM	jeff@woodgrove.ms	Add member to role	JeffTestCred2	"Security Operator"

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/sentinel-solorigate-hunt>.

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](https://twitter.com/Alex_t_weinert) if you have questions or suggestions for improvement.