Microsoft

Classeurs Azure AD

Daniel Wood

Responsable programme

Sécurité Azure AD Identity

18 février 2021

Série de vidéos consacrées à Solorigate

Importance de l’utilisation du classeur Azure AD pour identifier les modèles d’attaque courants

Microsoft Security

01. Comment accéder au classeur Azure AD

02. Partie 1 : Informations d’identification d’application et de service modifiées et méthodes d’authentification

03. Partie 2 : Paramètres de fédération modifiés

04. Partie 3 : Nouvelles autorisations accordées aux principaux de service

05. Partie 4 : Vue d’ensemble des modifications apportées aux appartenances des principaux de service

01.

Connectez-vous au **portail Azure**.

02.

Accédez à **Azure Active Directory > Surveillance > Classeurs**

03.

Dans la section Résolution des problèmes, ouvrez le **Rapport des opérations sensibles**

01.

Informations d’identification des applications et services modifiées / méthodes d’authentification

Woodgrove | Workbooks | Sensitive Operations Report

Azure Active Directory

External Identities
Roles and administrators
Administrative units
Enterprise applications
Devices
App registrations
Identity Governance
Application proxy
Licenses
Azure AD Connect
Custom domain names
Mobility (MDM and MAM)
Password reset
Company branding
User settings
Properties
Security

Monitoring
Sign-ins
Audit logs
Provisioning logs (Preview)
Logs
Diagnostic settings
Workbooks
Usage & insights

Troubleshooting + Support
Virtual assistant (Preview)
New support request

Workbooks | Edit

Modified Application and Service Principal Credentials/Authentication Methods

Applications and service principals can have multiple authentication methods that are simultaneously valid. It's important to monitor updates to your service principal authentication methods in case bad actors are adding new rogue credentials to allow themselves to authenticate as that service principal.

TimeRange: Last 60 days | Operation name: All | Credential: All | Actor: All | Exclude actor: None

Number of application and service principals updated by authentication method (Last 60 days)

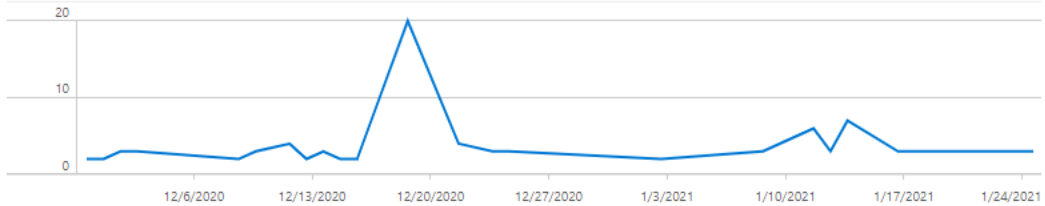
AsymmetricX509Cert	Other/not logged	Password	X509CertAndPassword
15	23	6	1

Top actors updating authentication methods (Last 60 days)

Search

Actor	Actor_Type	ServicePrincipalsChanged
Managed Service Identity	App	12
jeffs@woodgrove.ms	User	3
joeyc@woodgrove.ms	User	3
Azure AD Application Proxy	App	2
Domain Controller Services	App	1
Azure ESTS Service	App	1

Updates to service principal authentication methods over time



count_ (Sum)
91

Recent updates to application/service principal authentication methods

Search

TimeGenerated	OperationName	Actor	Actor_Type	Service_Principal_Name	credential	Service_Principal_ID
1/25/2021, 2:03:34 AM	Add service principal credentials	Managed Service Identity	App	woodgrovechecklist	Other/not logged	1af2f52c-f74f-4a86-8eec-d
1/25/2021, 2:03:34 AM	Add service principal credentials	Managed Service Identity	App	woodgrovechecklist	AsymmetricX509Cert	1af2f52c-f74f-4a86-8eec-d
1/25/2021, 2:03:34 AM	Add service principal credentials	Managed Service Identity	App	woodgrovechecklist	Other/not logged	1af2f52c-f74f-4a86-8eec-d
1/24/2021, 1:03:46 PM	Add service principal credentials	Managed Service Identity	App	woodgrove-app	Other/not logged	dcbce8f2-17b4-4139-8d97-

01.

Informations d’identification d’application et de service modifiées et méthodes d’authentification

Nouvelles informations d’identification ajoutées aux applications et principaux de service, y compris le type d’informations d’identification

Acteurs principaux et volume de modifications d’informations d’identification effectuées

Chronologie des modifications d’informations d’identification

02.

Paramètres de fédération modifiés

Woodgrove | Workbooks | Sensitive Operations Report

Azure Active Directory

External Identities
Roles and administrators
Administrative units
Enterprise applications
Devices
App registrations
Identity Governance
Application proxy
Licenses
Azure AD Connect
Custom domain names
Mobility (MDM and MAM)
Password reset
Company branding
User settings
Properties
Security

Monitoring
Sign-ins
Audit logs
Provisioning logs (Preview)
Logs
Diagnostic settings
Workbooks
Usage & insights

Troubleshooting + Support
Virtual assistant (Preview)
New support request

Workbooks | Edit

Modified application and service principal credentials/authentication methods

New permissions granted to service principals

Directory role and group membership updates to service principals

Modified federation settings

Modified federation settings

This section monitors when a user or application modifies the federation settings on the domain. For example, this alert will trigger when a new Active Directory Federated Service (ADFS) TrustedRealm object, such as a signing certificate, is added to the domain. Modification to domain federation settings should be rare. Confirm the added or modified target domain/URL is legitimate administrator behavior.

- To understand why an authorized user may update settings for a federated domain in Office 365, Azure, or Intune, see: https://docs.microsoft.com/office365/troubleshoot/active-directory/update-federated-domain-office-365.
- For details on security realms that accept security tokens, see the ADFS Proxy Protocol (MS-ADFSPP) specification: https://docs.microsoft.com/openspecs/windows_protocols/ms-adfspp/e7b9ea73-1980-4318-96a6-da559486664b.

TimeRange: Last 60 days | Operation: All | InitiatingUserOrApp: All

TimeGenerated	OperationName	InitiatingUserOrApp	AADOperationType	targetDisplayName	TargetResources	Result	UserAgent
12/18/2020, 8:59:57 PM	Set federation settings on domain	jeffs@woodgrove.ms	Update	woodgrove.net	[{"displayName":"woodgrove.net","administrativeUnits":[],...	success	
12/7/2020, 3:37:54 PM	Add verified domain	joeyc@woodgrove.ms	Add	Unknown	[{"displayName":"Unknown","administrativeUnits":[],"mod...	failure	Mozilla/5.0 (Windows NT 10
12/7/2020, 3:12:05 PM	Add verified domain	joeyc@woodgrove.ms	Add	Unknown	[{"displayName":"Unknown","administrativeUnits":[],"mod...	failure	Mozilla/5.0 (Windows NT 10
12/7/2020, 3:11:40 PM	Add unverified domain	joeyc@woodgrove.ms	Add	pre2.woodrove.ms	[{"displayName":"pre2.woodrove.ms","administrativeUnits...	success	Mozilla/5.0 (Windows NT 10
12/7/2020, 3:10:58 PM	Add verified domain	joeyc@woodgrove.ms	Add	Unknown	[{"displayName":"Unknown","administrativeUnits":[],"mod...	failure	Mozilla/5.0 (Windows NT 10

02.

Paramètres de fédération modifiés

Modifications apportées aux approbations de fédération de domaine

Ajout de nouveaux domaines et approbations

03.

Nouvelles autorisations accordées aux principaux de service

Woodgrove | Workbooks | Sensitive Operations Report

Azure Active Directory

External Identities
Roles and administrators
Administrative units
Enterprise applications
Devices
App registrations
Identity Governance
Application proxy
Licenses
Azure AD Connect
Custom domain names
Mobility (MDM and MAM)
Password reset
Company branding
User settings
Properties
Security

Monitoring

Sign-ins
Audit logs
Provisioning logs (Preview)
Logs
Diagnostic settings
Workbooks
Usage & insights

Troubleshooting + Support

Virtual assistant (Preview)
New support request

Workbooks | Edit

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
Office 365 Exchange Online (4)					
"JeffTestCreds2" (4)					
Microsoft Graph (4)					
"JeffTestCreds2" (3)					
	"JeffTestCreds2"	"Application.Read.All"	"Read all applications"	jeffs@woodgrove.ms	12/20/2020, 1:54:46 PM
	"JeffTestCreds2"	"Mail.Send"	"Send mail as any user"	jeffs@woodgrove.ms	12/22/2020, 11:56:24 AM
	"JeffTestCreds2"	"Mail.ReadWrite"	"Read and write mail in all mailboxes"	jeffs@woodgrove.ms	12/22/2020, 11:56:24 AM
"Mimorony AuthTS API" (1)					
Office 365 SharePoint Online (1)					
"JeffTestCreds2" (1)					

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

Recent app permissions activity

TimeGenerated	InitiatingUserOrApp	OperationName	ClientApp	Resource	Result
1/26/2021, 4:25:23 PM	jerryw@woodgrove.ms	Consent to application	CCE Test	Not logged	success

04.

Vue d’ensemble des modifications apportées aux appartenances des principaux de service

Woodgrove | Workbooks | Sensitive Operations Report

Azure Active Directory

External Identities
Roles and administrators
Administrative units
Enterprise applications
Devices
App registrations
Identity Governance
Application proxy
Licenses
Azure AD Connect
Custom domain names
Mobility (MDM and MAM)
Password reset
Company branding
User settings
Properties
Security

Monitoring
Sign-ins
Audit logs
Provisioning logs (Preview)
Logs
Diagnostic settings
Workbooks
Usage & insights

Troubleshooting + Support
Virtual assistant (Preview)
New support request

Workbooks | Edit

Sensitive Operations Report - Apps, Service Principals and Federation Settings

Workspace: All

This workbook is intended to help identify suspicious application and service principal activity that may indicate compromises in your environment. Learn more about best practices to protect M365 from attacks.

Modified application and service principal credentials/authentication methods

New permissions granted to service principals

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 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 rules and Groups that either grant access to sensitive data or represent opportunities for lateral movement by attackers.

TimeRange: Last 60 days | Operation: Add member to role | InitiatingUserOrApp: All

Select
- [ ] All

Items
- [x] Add member to role
- [ ] Add eligible member to role
- [ ] Add scoped member to role
- [ ] Add member to group

TimeGenerated	InitiatingU	ServicePrincipalDisplayName	GroupOrRoleNameAddedTo
12/22/2020, 11:49:13 AM	jeffs@woo	JeffTestCreds2	"Application Administrator"
12/22/2020, 11:52:28 AM	jeffs@woo	Risky App	"Global Administrator"
12/20/2020, 7:46:25 PM	jeffs@woo	JeffTestCreds2	"Security Operator"

Modified federation settings

Étapes suivantes

01 Regardez la série de vidéos consacrées à Solorigate ici

02 Visitez le site de Sécurité Microsoft pour plus de mises à jour : www.microsoft.com/en-us/security/business

03 Lisez les billets de blog sur : www.microsoft.com/security/blog/

https://aka.ms/solorigate