Microsoft

Hiding in the clouds:

How attackers can use applications for sustained persistence and how to find it

Yochana Henderson @mbeyochana
Mark Morowczynski @markmorow
Program Managers – Microsoft

Agenda

What is application consent and why should you care

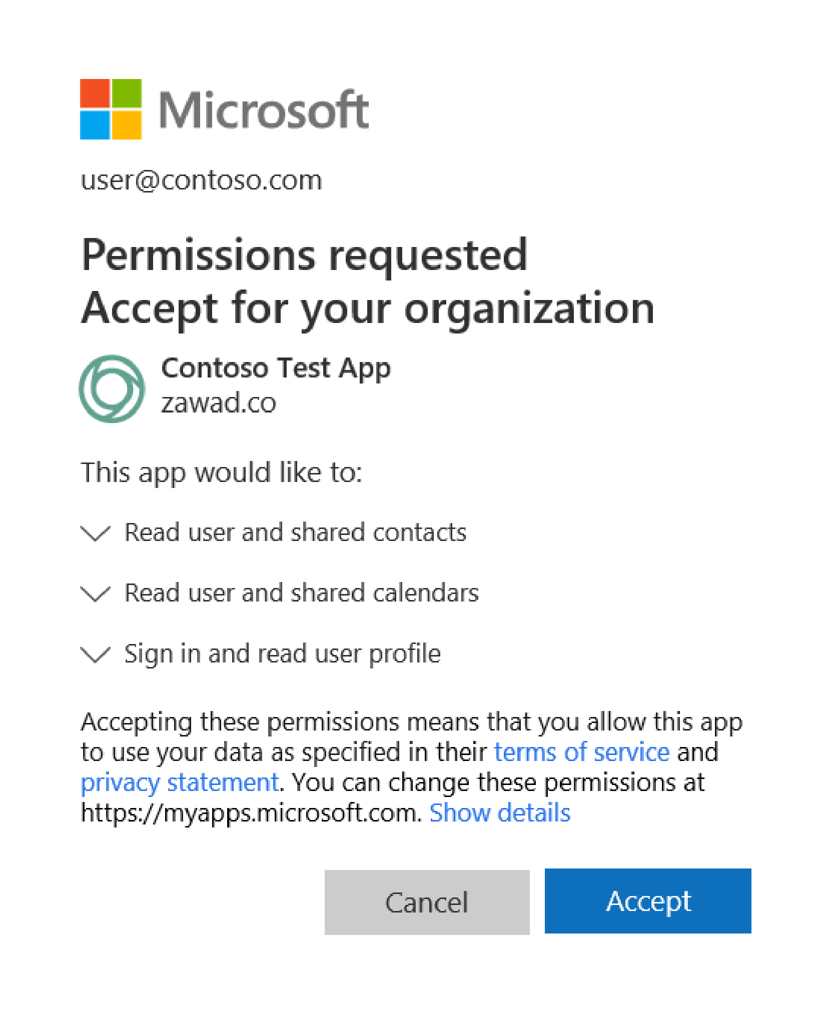
Key permissions to look for

How to investigate consent grants

Best Practices to Protect Yourself from App Consent Attacks

Some terms

- Client application- the **application** (mobile/web/background) requesting access to data on behalf of the user
- Resource application- the **application** (usually a web API) that exposes data or functionality
- Permission- the ability for a **client application** to perform some action on some **data** owned by a **resource application**
- e.g. *read a user's OneDrive files through Microsoft Graph*



Microsoft

user@contoso.com

Permissions requested
Accept for your organization

Contoso Test App
zawad.co

This app would like to:

- Read user and shared contacts
- Read user and shared calendars
- Sign in and read user profile

Accepting these permissions means that you allow this app to use your data as specified in their terms of service and privacy statement. You can change these permissions at https://myapps.microsoft.com. Show details

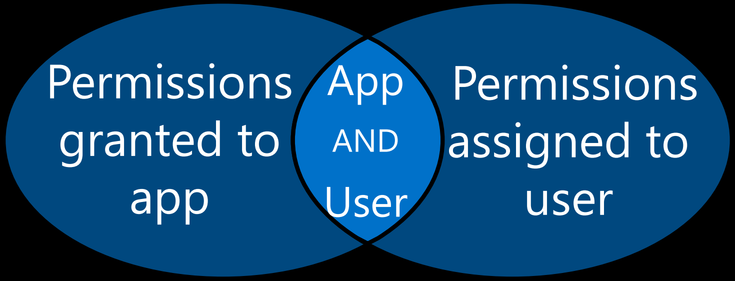
Consent terms

- **Consent prompt**- the process by which a *user* is asked to grant an application the **permission(s)** it has requested
- **Consent grant-** the result of saying “yes” to a consent prompt
- **Admin(istrative) Consent**- the process by which a company administrator grants an **application** to one or more requested **permissions** that cannot be granted by a regular user.
- May allow the app to perform high privilege operations
- Can also consent to this application for all users in the organization (No more user consent for that application)

Permission terms

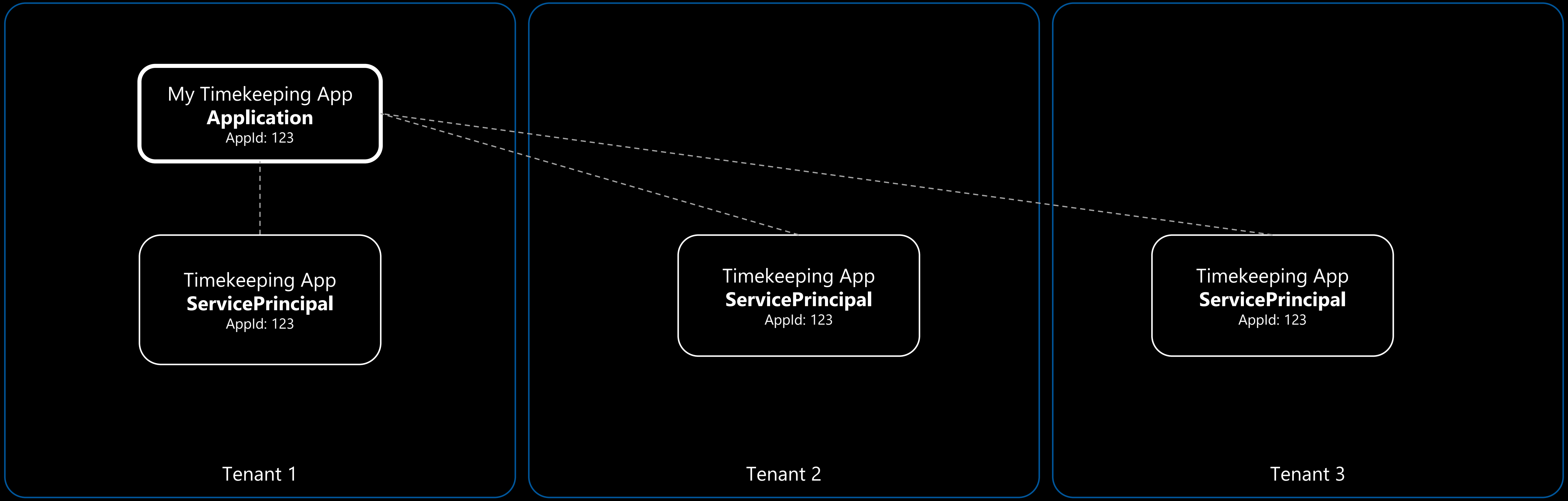
- **Delegated permissions**
  - Used by apps that have a **signed-in user present** in order to make calls on behalf of that user
  - Can **be consented to by non-administrative users**, but **some higher-privileged permissions require admin consent**
  - **"Effective" permissions** are the intersection of the User's underlying permissions and what the application has been granted consent to do
  - **AKA** scopes, OAuth2PermissionGrants, App+User permissions, etc.
- **Application Permissions**
  - Used by apps that run **without a signed-in user present**, like background services
  - Application has permission to do what it was consented to- **no intersection**
  - Always require **admin consent**
  - **AKA** roles, AppRoles, AppOnly permissions, etc.

Permission Types

	Delegated Permissions	Application Permissions
App	Mobile / Web / SPA	Service / Daemon
Scenario	Get access on behalf of user	Get access as a service
Consent	Users for self / IT admin for all users	Only by IT admin
Effective Permissions	 Permissions granted to app App AND User Permissions assigned to user	 Permissions granted to app

Applications and service principals

- **Application**: the *definition* of an app (“App registrations”)
- **Service principal**: the *representation* of an app in the tenant (“Enterprise apps”)



My Timekeeping App
Application
AppId: 123

Timekeeping App
ServicePrincipal
AppId: 123

Tenant 1

Timekeeping App
ServicePrincipal
AppId: 123

Tenant 2

Timekeeping App
ServicePrincipal
AppId: 123

Tenant 3

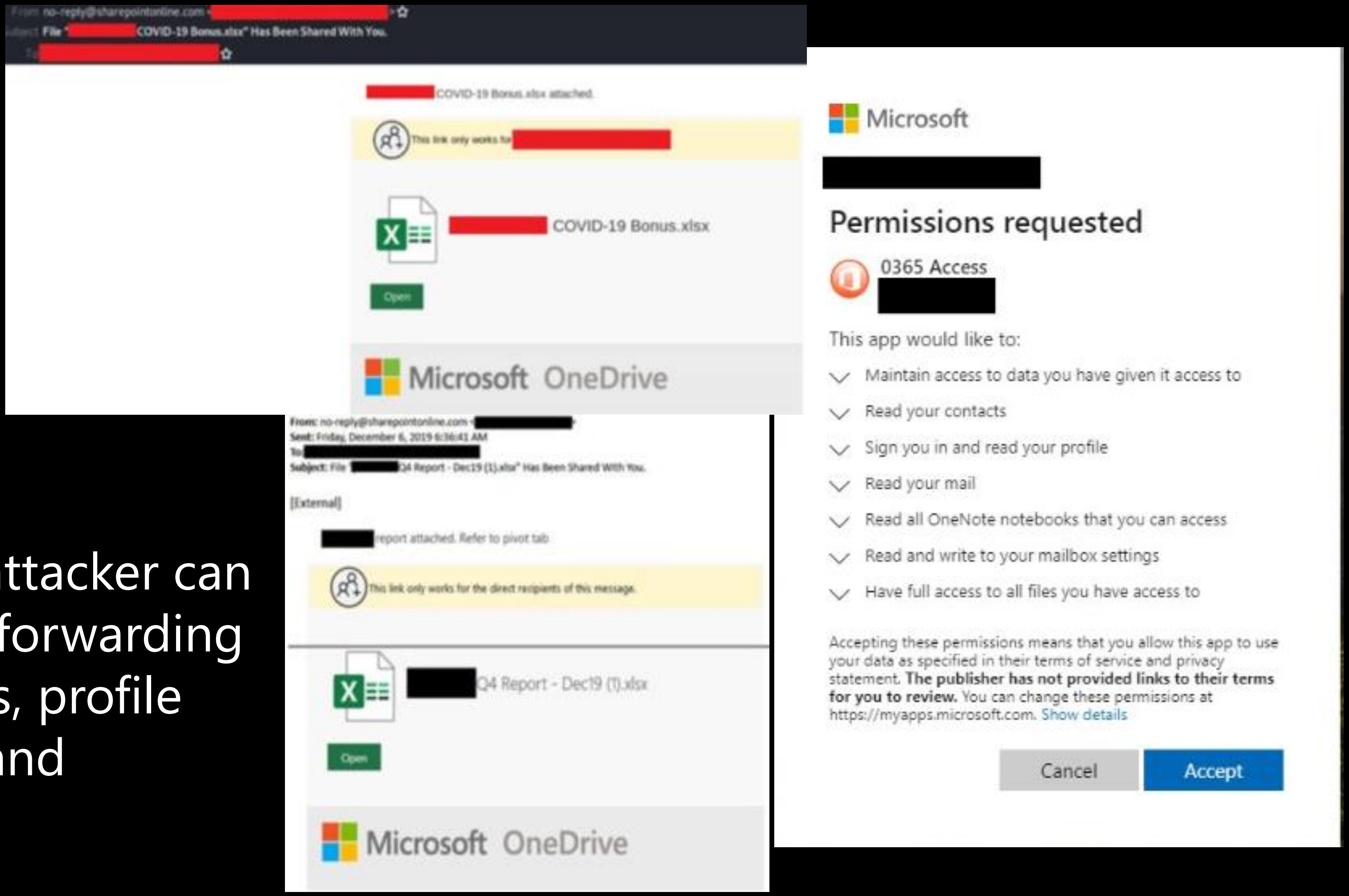
Apps can be authorized to access data

- An app’s service principal is its *security principal*.

- There are many ways a service principal can be granted access:
  - Azure role assignment
  - Directory role assignment
  - Owner of group, application, service principal
  - App-only permission grants (aka. app role assignments)
  - Delegated permission grants
  - Azure Key Vault ACL

Evolving Threat Landscape | Consent Phishing

- Business-themed email
- Covid-19-themed email
- Malicious webapp



From: no-reply@sharepointonline.com <[redacted]>

Subject: File "[redacted]COVID-19 Bonus.xlsx" Has Been Shared With You.

To: [redacted]

[redacted]COVID-19 Bonus.xlsx attached.

This link only works for [redacted]

[redacted] COVID-19 Bonus.xlsx

From: no-reply@sharepointonline.com <[redacted]>
Sent: Friday, December 6, 2019 6:36:41 AM
To: [redacted]
Subject: File "[redacted]Q4 Report - Dec19 (1).xlsx" Has Been Shared With You.

[External]

[redacted] report attached. Refer to pivot tab

This link only works for the direct recipients of this message.

[redacted] Q4 Report - Dec19 (1).xlsx

[redacted]

Permissions requested

0365 Access
[redacted]

This app would like to:

- Maintain access to data you have given it access to
- Read your contacts
- Sign you in and read your profile
- Read your mail
- Read all OneNote notebooks that you can access
- Read and write to your mailbox settings
- Have full access to all files you have access to

Accepting these permissions means that you allow this app to use your data as specified in their terms of service and privacy statement. **The publisher has not provided links to their terms for you to review.** You can change these permissions at https://myapps.microsoft.com. Show details

If the user consents, the attacker can gain access to their mail, forwarding rules, files, contacts, notes, profile and other sensitive data and resources.

What Is Application Consent and why should you care

Key Permissions To Look For

How to investigate illicit consent grants

Best Practices to Protect Yourself from App Consent Attacks

Key permissions to look for

- Mail.*
- Mail.Send
- MailboxSettings.*
- Contacts.*
- People.*
- Files.*
- Notes.*
- Directory.AccessAsUser.All
- Directory.ReadWrite.All

- Application.ReadWrite.All
- Domain.ReadWrite.All
- EduRoster.ReadWrite.All
- Group.ReadWrite.All
- Member.Read.Hidden
- RoleManagement.ReadWrite.Directory
- User.ReadWrite.All
- User.ManageCreds.All
- user_impersonation

* = incl. read and write

And know the low impact permissions too…

- Low Impact Permissions
  - User.Read
  - open_id
  - email
  - profile

What Is Application Consent and Why Should You Care

Key Permissions To Look For

How to investigate illicit consent grants

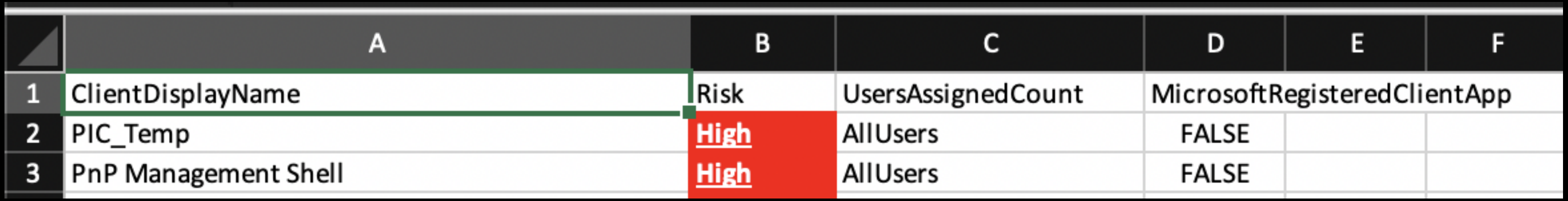
Best Practices to Protect Yourself from App Consent Attacks

How to find illicit consent?

- Office 365 Portal
  - Search the audit logs apps and look for signs, also called Indicators of Compromise (IOC) of attack
  - Review the Security&Compliance Center audit logs
    - If **IsAdminContent** is set to **True** it indicates that someone with Global Administrator access may have granted broad access to data.
- Azure AD Portal
  - Enterprise Apps – Permissions
  - Audit logs
- PowerShell
  - Inventory applications and their granted permissions
  - This is the fastest and most thorough method, with the least amount of overhead.
  - https://aka.ms/getazureadpermissions
- Microsoft Cloud App Security (w/ applicable license)

A few other things to look for…

- Start with HighRiskApps tab & UserAssignedCount AllUsers
  - Every non-Microsoft application with this permission should be reviewed carefully



	A	B	C	D	E	F
1	ClientDisplayName	Risk	UsersAssignedCount	MicrosoftRegisteredClientApp		
2	PIC_Temp	High	AllUsers	FALSE		
3	PnP Management Shell	High	AllUsers	FALSE		

- Review HighRiskUsers Tab
  - Start with those that have high privilege or access to sensitive info (C suite, finance, etc)

- Review Permissions for each delegated application
  - Look for "Read" and "Write" permission or "*.All" permission, and review these carefully because they may not be appropriate.

Other IOCs to consider

- Apps trying to blend in
  - Boring sounding names or misspelled names.
- Suspicious activities such as after office hours and location
- Any deviation from the user’s normal behavior based on the learning of their daily activities
- Date and time of applications being created
  - If the suspected date of compromised is known.

If attack is confirmed…Start your IR Process

- **Does your Incident Response process cover this scenario?**
- **Stop and remediate the consent grant attack**
  - Disable the malicious Service Principal
  - Revoke Oauth consent grant with PowerShell
    - Remove-AzureADOAuth2PermissionGrant -ObjectId
  - Revoke the Service App role Assignment with PowerShell
    - Remove-AzureADServiceAppRoleAssignment -ObjectId <String> -AppRoleAssignmentId <String>
  - Disable sign-in for the account
  - Remove any persistence mechanisms (e.g. mail forwarding rules)

What Is Application Consent and why should you care

Key Permissions To Look For

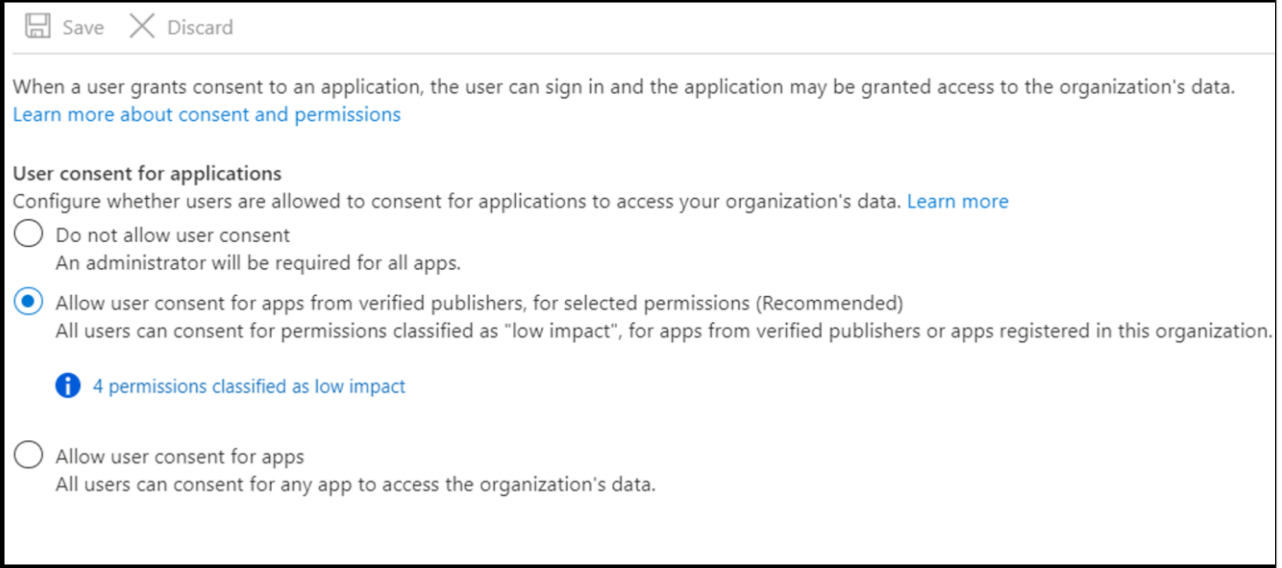
How to investigate illicit consent grants

Best Practices to Protect Yourself from App Consent Attacks

Steps to protect your organization

#1 Set Policies

- Use app consent policies to limit user consent to apps- e.g. only from verified publishers requesting low risk permissions
- Use Microsoft Cloud App Security to automatically revoke an app or a specific user from an app when risk is detected



When a user grants consent to an application, the user can sign in and the application may be granted access to the organization's data.
Learn more about consent and permissions

User consent for applications

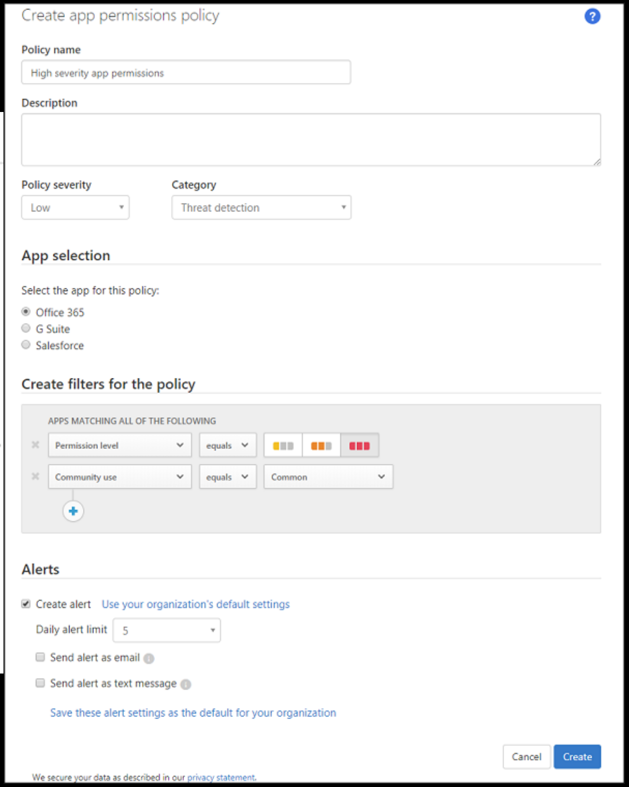
Configure whether users are allowed to consent for applications to access your organization's data. Learn more

○ Do not allow user consent
An administrator will be required for all apps.

● Allow user consent for apps from verified publishers, for selected permissions (Recommended)
All users can consent for permissions classified as "low impact", for apps from verified publishers or apps registered in this organization.

4 permissions classified as low impact

○ Allow user consent for apps
All users can consent for any app to access the organization's data.



Create app permissions policy

Policy name: High severity app permissions

Description:

Policy severity: Low

Category: Threat detection

App selection

Select the app for this policy:

● Office 365
○ G Suite
○ Salesforce

Create filters for the policy

APPS MATCHING ALL OF THE FOLLOWING

Permission level equals ■■■ ■■■ ■■■

Community use equals Common

Alerts

☑ Create alert Use your organization's default settings

Daily alert limit: 5

□ Send alert as email

□ Send alert as text message

Save these alert settings as the default for your organization

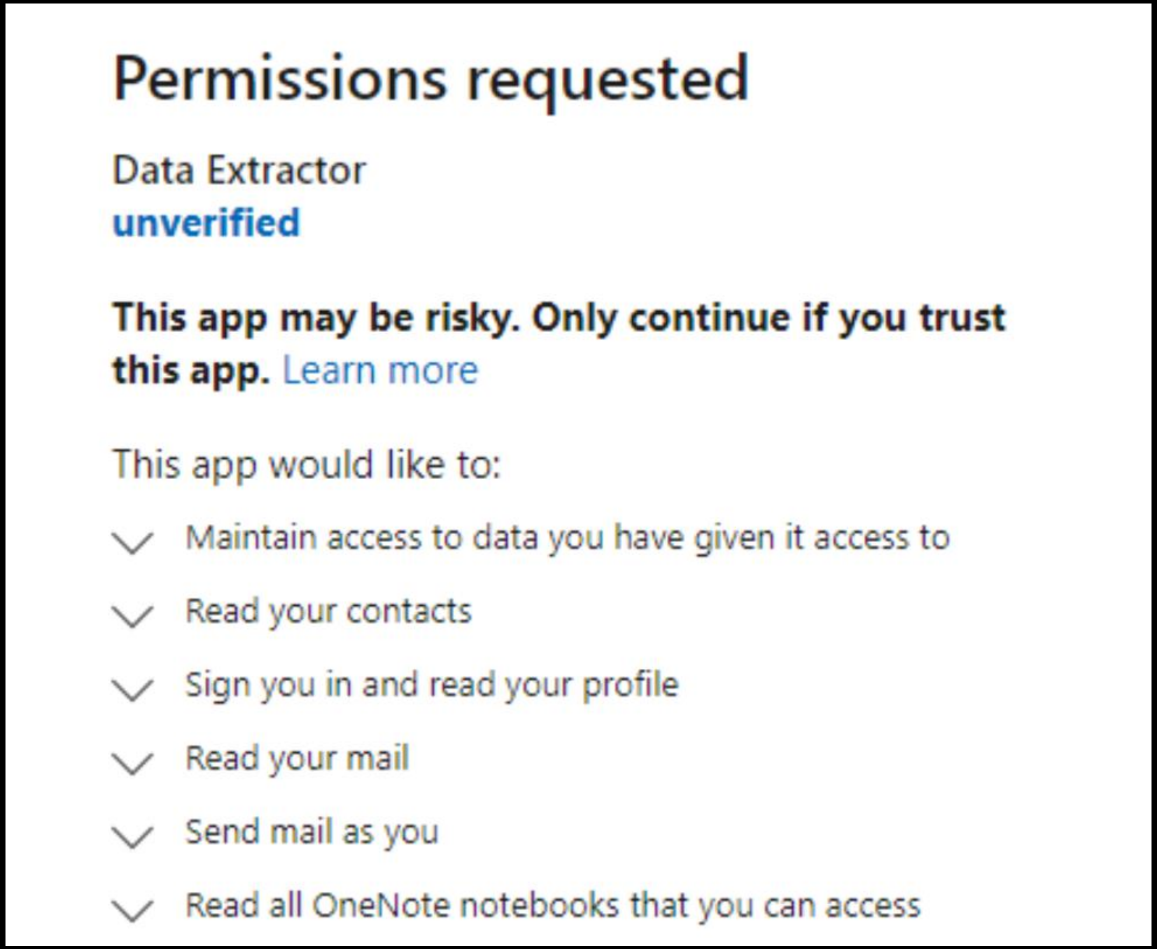
We secure your data as described in our privacy statement.

Steps to protect your organization

#2 Risk-based user step-up consent (enabled by default)

Risk-based step-up consent:

- When a **risky consent** request is detected, request will be “stepped up” to **require admin approval**
- **Warning will be shown** to users and admins, but only admin can grant permissions
- Audit event will be logged



Permissions requested

Data Extractor
unverified

This app may be risky. Only continue if you trust this app. Learn more

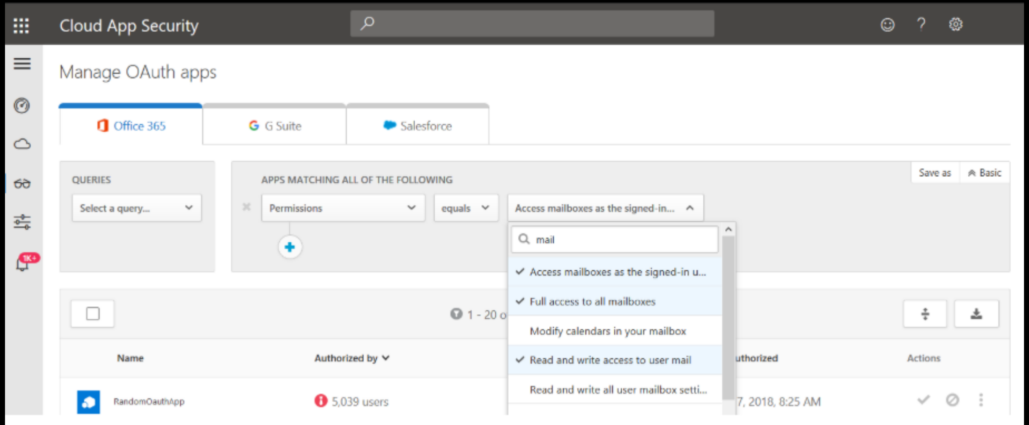
This app would like to:

- Maintain access to data you have given it access to
- Read your contacts
- Sign you in and read your profile
- Read your mail
- Send mail as you
- Read all OneNote notebooks that you can access

Steps to protect your organization

#3 Detect risky OAuth apps

- Good: Audit apps and consented permissions
  - https://aka.ms/getazureadpermissions
- Better: Use Azure Monitor to set alerts to automatically send you notifications when an OAuth app meets certain criteria
  - App requires high permissions
  - App was authorized by >50 users
- Best: Detect risky apps by hunting using CASB like MCAS
  - Permission level high security
  - Community use not common
  - Apps authorized by external users



Manage OAuth apps

APPS MATCHING ALL OF THE FOLLOWING

Permissions equals Access mailboxes as the signed-in...

mail

- ✓ Access mailboxes as the signed-in u...
- ✓ Full access to all mailboxes
- Modify calendars in your mailbox
- ✓ Read and write access to user mail
- Read and write all user mailbox setti...

Name	Authorized by	uthorized	Actions
RandomOauthApp	5,039 users	7, 2018, 8:25 AM	

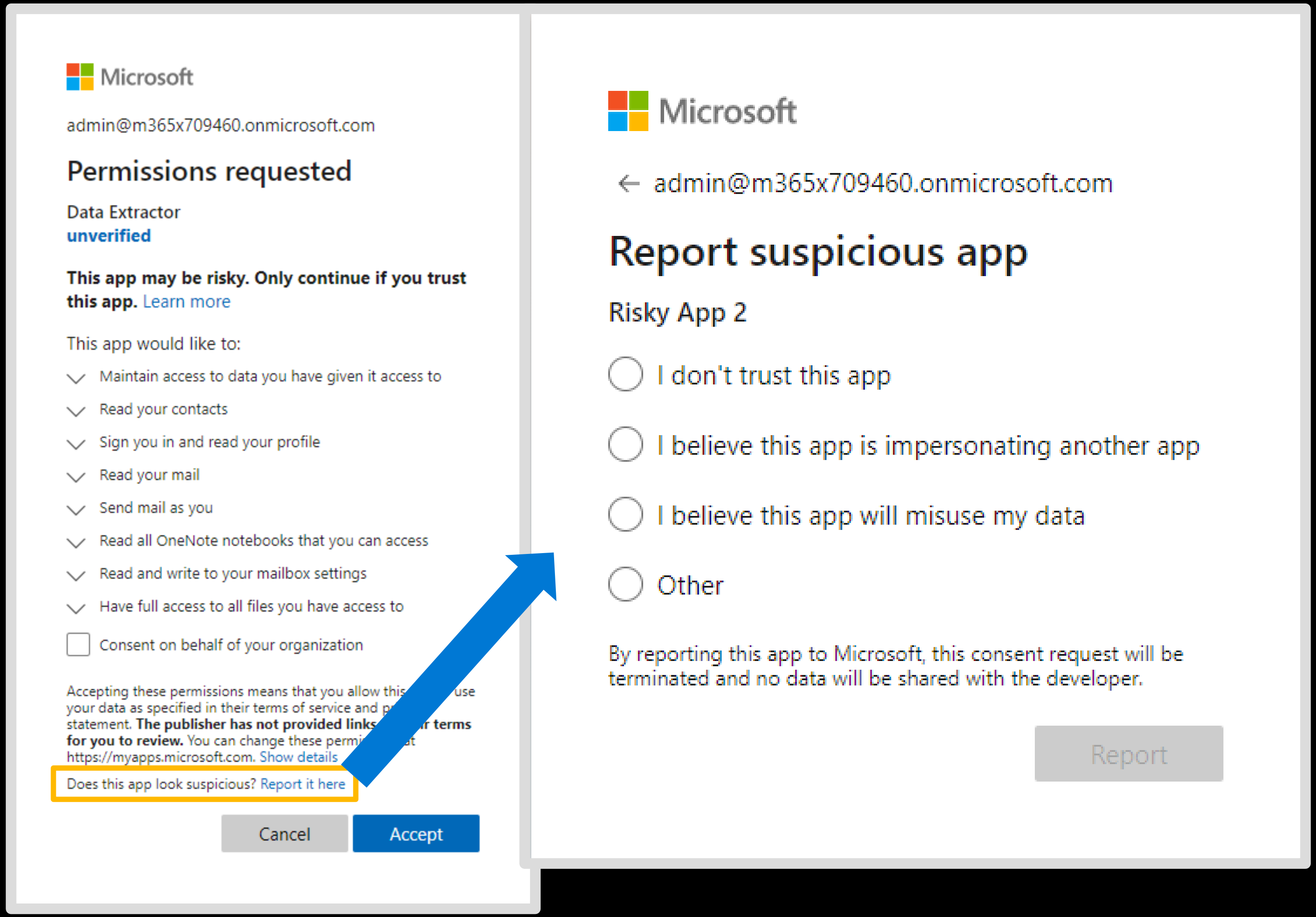
Steps to protect your organization

#4 Developers: check your app – it's probably overprivileged

- New permissions coming all the time
  - +60% since Build 2019
  - 25+ new Teams permissions
  - 20+ identity & access permissions
- Only ask for what is absolutely necessary
  - Directory.* permissions are never least privilege
  - https://aka.ms/GraphBestPractices and https://aka.ms/IdentityPlatformChecklist
- Teams apps: *Use resource specific permissions*
  - Enables apps to access only the teams they need aka.ms/rsc-teams to start
- Developer Guidance: https://aka.ms/IdentityDeveloperSeries

Report suspicious apps

Report suspicious apps to Microsoft for investigation directly from the consent screen or using MCAS



Microsoft

admin@m365x709460.onmicrosoft.com

Permissions requested

Data Extractor
unverified

This app may be risky. Only continue if you trust this app. Learn more

This app would like to:

- Maintain access to data you have given it access to
- Read your contacts
- Sign you in and read your profile
- Read your mail
- Send mail as you
- Read all OneNote notebooks that you can access
- Read and write to your mailbox settings
- Have full access to all files you have access to

□ Consent on behalf of your organization

Accepting these permissions means that you allow this use your data as specified in their terms of service and p statement. **The publisher has not provided links r terms for you to review.** You can change these permi at https://myapps.microsoft.com. Show details

Does this app look suspicious? Report it here

Microsoft

← admin@m365x709460.onmicrosoft.com

Report suspicious app

Risky App 2

○ I don't trust this app

○ I believe this app is impersonating another app

○ I believe this app will misuse my data

○ Other

By reporting this app to Microsoft, this consent request will be terminated and no data will be shared with the developer.

Go Do’s

- Inventory applications and their permissions using the Azure Active Directory portal or PowerShell
- Automate threat response by implementing risk-based step-up consent and MCAS policies
- Educate your organization on consent tactics (phishing, user and admin consent framework)
- Educate your developers to ensure they follow the recommended security best practices
    - https://aka.ms/IdentityPlatformChecklist
    - http://aka.ms/GraphBestPractices

Resources

- Five steps to securing your identity infrastructure
  - https://aka.ms/securitysteps
- Azure Active Directory consent framework
  - https://aka.ms/consent-framework
- Detect and Remediate Illicit Consent Grants
  - https://aka.ms/O365consentinvestigation
- Managing consent to applications and evaluating consent requests
  - https://aka.ms/manage-consent

Q&A

Yochana Henderson @mbeyochana
Mark Morowczynski @markmorow
Program Managers – Microsoft