Azure
User group
Norway

Entra ID Applications: Uncovering Risks, Misconfigurations, and Attack Vectors

Who am I

Lead Security Architect @ Storebrand

Education

Master of Science in Information Security

Consultant

10+ Years as consultant

MSUG

Part of Microsoft Security User Group Organizers

Hobbies

Gaming in winter and disc golf during summer

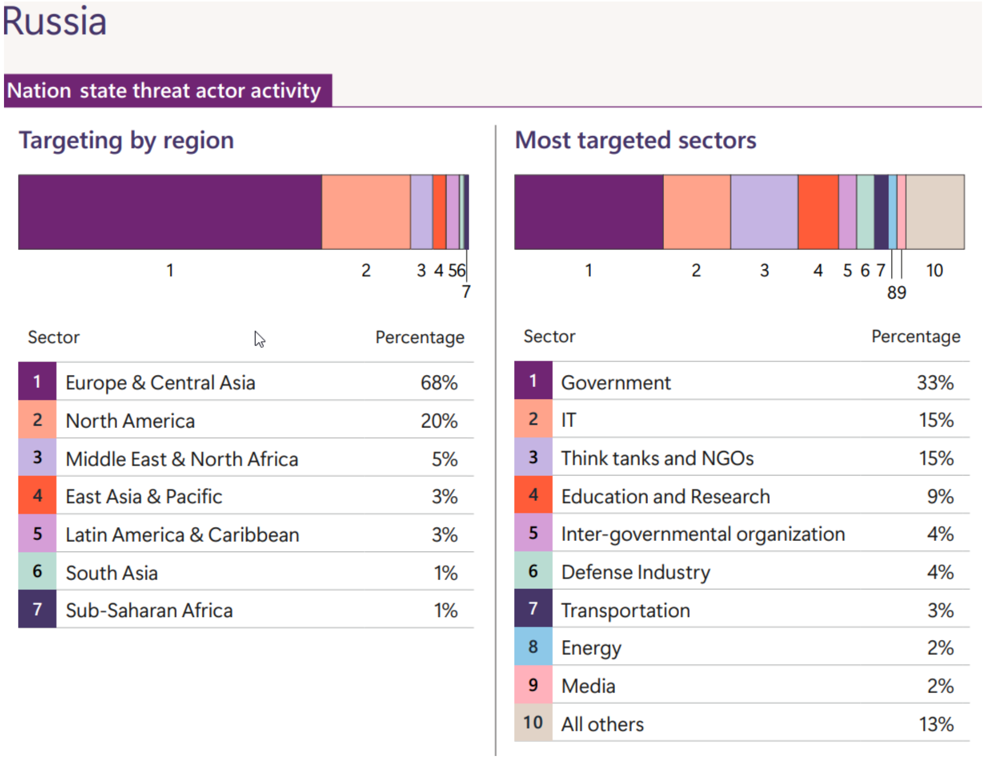
Security MVP

MVP

Agenda

- Security landscape and current state
- Conditional Access Demo
- Detection and protection options
- Illicent consent demo
- Where do I start self assessment?

Threat Landscape: identity



Russia

Nation state threat actor activity

Targeting by region

Sector		Percentage
1	Europe & Central Asia	68%
2	North America	20%
3	Middle East & North Africa	5%
4	East Asia & Pacific	3%
5	Latin America & Caribbean	3%
6	South Asia	1%
7	Sub-Saharan Africa	1%

Most targeted sectors

Sector		Percentage
1	Government	33%
2	IT	15%
3	Think tanks and NGOs	15%
4	Education and Research	9%
5	Inter-governmental organization	4%
6	Defense Industry	4%
7	Transportation	3%
8	Energy	2%
9	Media	2%
10	All others	13%

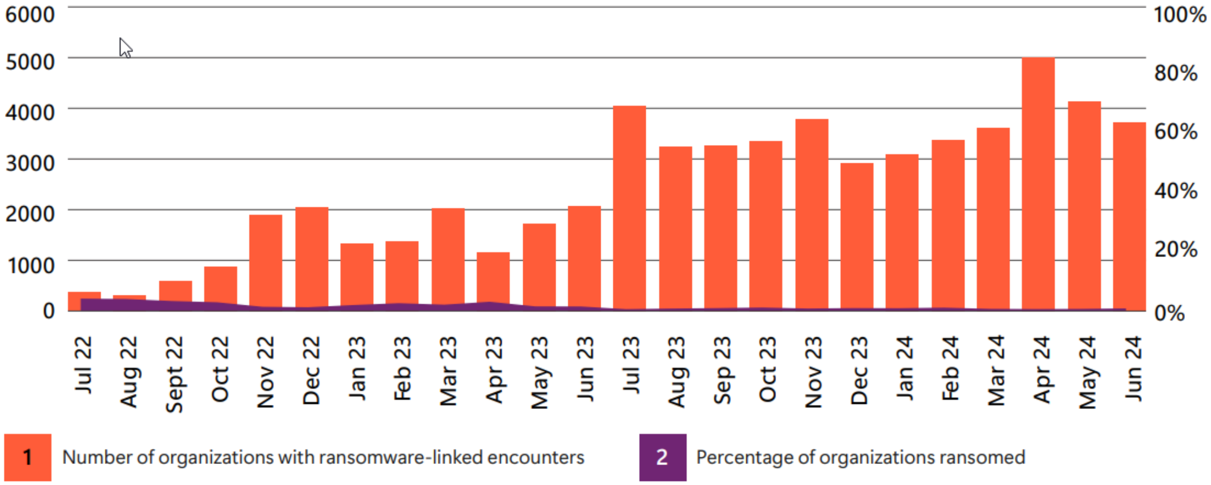
600 million identity attacks per day. As multifactor authentication blocks most password-based attacks, threat actors are shifting their focus

2.6% of workload identity permissions were used and 51% of workload identities were completely inactive.

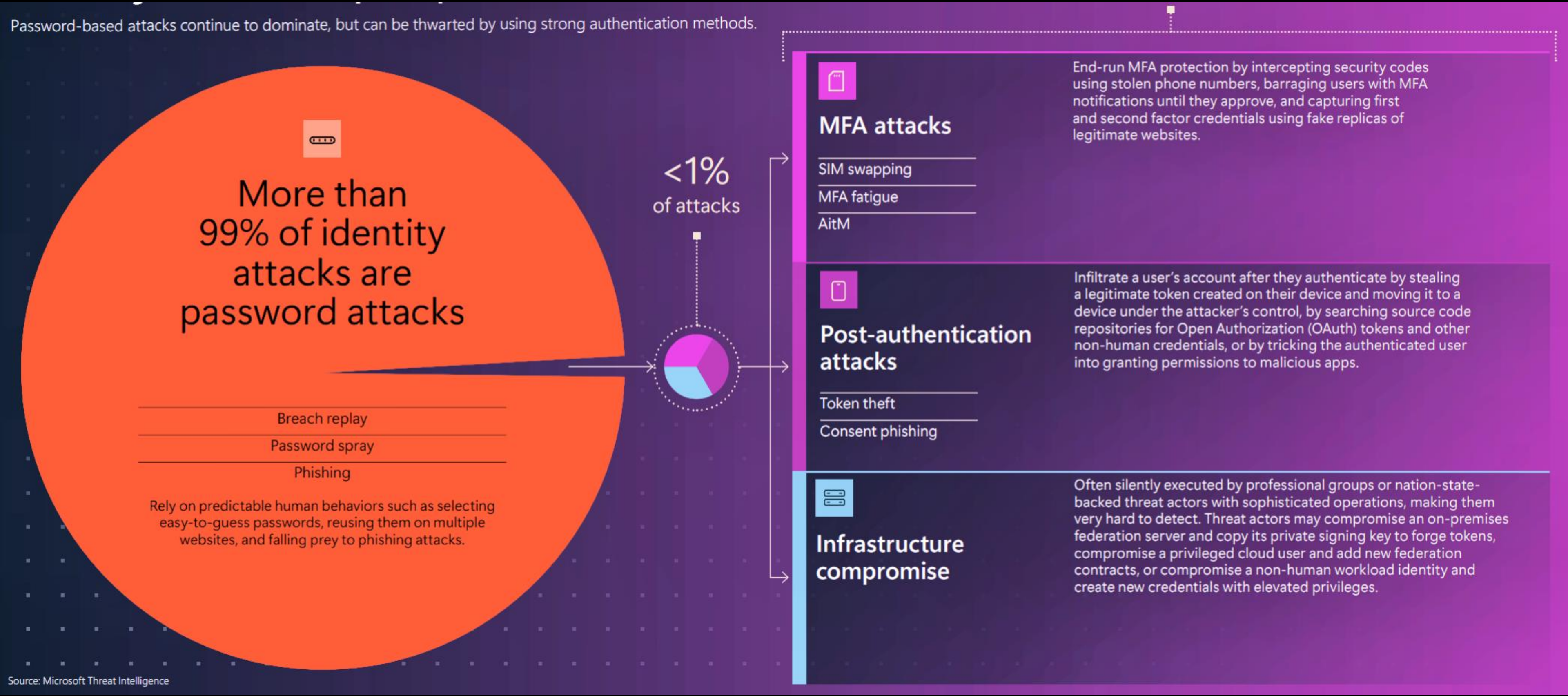
2.75x increase in human-operated ransomware-linked encounters

Ransomware statistics

Organizations with ransom-linked encounters continues to increase while the percentage of those ransomed is decreasing (July 2022–June 2024)



Although organizations with ransom-linked encounters continues to increase, the percentage that are ultimately ransomed (reaching encryption stage) decreased more than threefold over the past two years.



Password-based attacks continue to dominate, but can be thwarted by using strong authentication methods.

More than 99% of identity attacks are password attacks

- Breach replay
- Password spray
- Phishing

Rely on predictable human behaviors such as selecting easy-to-guess passwords, reusing them on multiple websites, and falling prey to phishing attacks.

<1% of attacks

MFA attacks

- SIM swapping
- MFA fatigue
- AitM

End-run MFA protection by intercepting security codes using stolen phone numbers, barraging users with MFA notifications until they approve, and capturing first and second factor credentials using fake replicas of legitimate websites.

Post-authentication attacks

- Token theft
- Consent phishing

Infiltrate a user's account after they authenticate by stealing a legitimate token created on their device and moving it to a device under the attacker's control, by searching source code repositories for Open Authorization (OAuth) tokens and other non-human credentials, or by tricking the authenticated user into granting permissions to malicious apps.

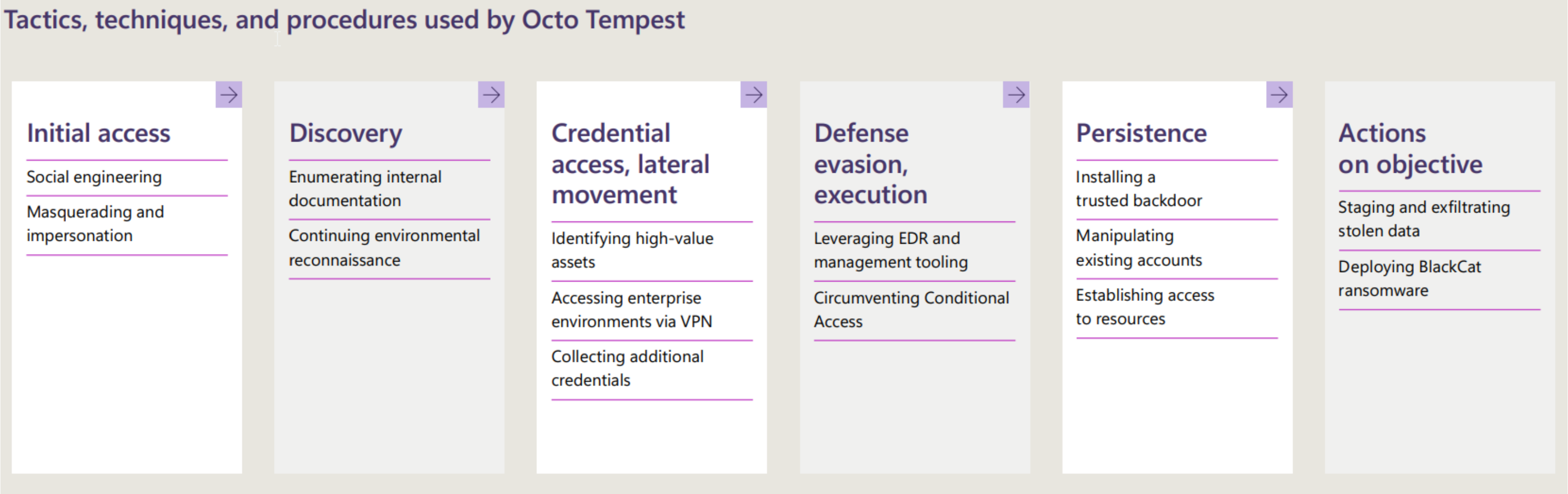
Infrastructure compromise

Often silently executed by professional groups or nation-state-backed threat actors with sophisticated operations, making them very hard to detect. Threat actors may compromise an on-premises federation server and copy its private signing key to forge tokens, compromise a privileged cloud user and add new federation contracts, or compromise a non-human workload identity and create new credentials with elevated privileges.

Source: Microsoft Threat Intelligence

Microsoft Digital Defense report 2024

Octo Tempest (aka Scattered Spider)



Tactics, techniques, and procedures used by Octo Tempest

Initial access

- Social engineering
- Masquerading and impersonation

Discovery

- Enumerating internal documentation
- Continuing environmental reconnaissance

Credential access, lateral movement

- Identifying high-value assets
- Accessing enterprise environments via VPN
- Collecting additional credentials

Defense evasion, execution

- Leveraging EDR and management tooling
- Circumventing Conditional Access

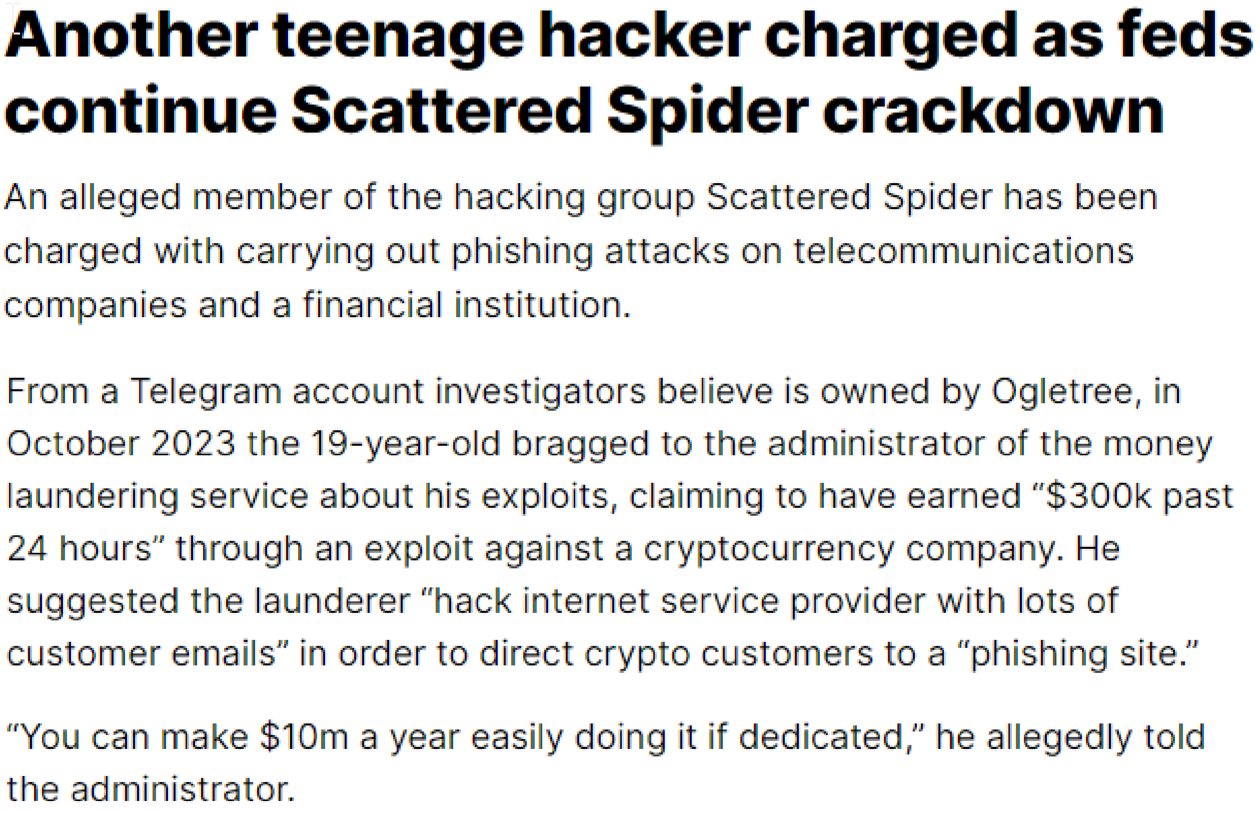
Persistence

- Installing a trusted backdoor
- Manipulating existing accounts
- Establishing access to resources

Actions on objective

- Staging and exfiltrating stolen data
- Deploying BlackCat ransomware

Detection and OpSec

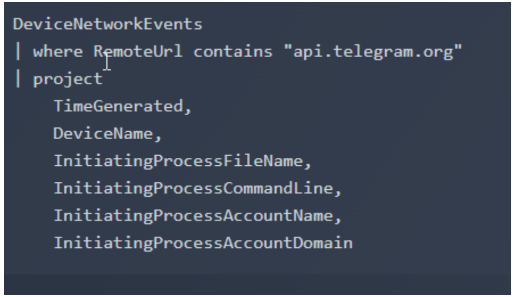


Another teenage hacker charged as feds continue Scattered Spider crackdown

An alleged member of the hacking group Scattered Spider has been charged with carrying out phishing attacks on telecommunications companies and a financial institution.

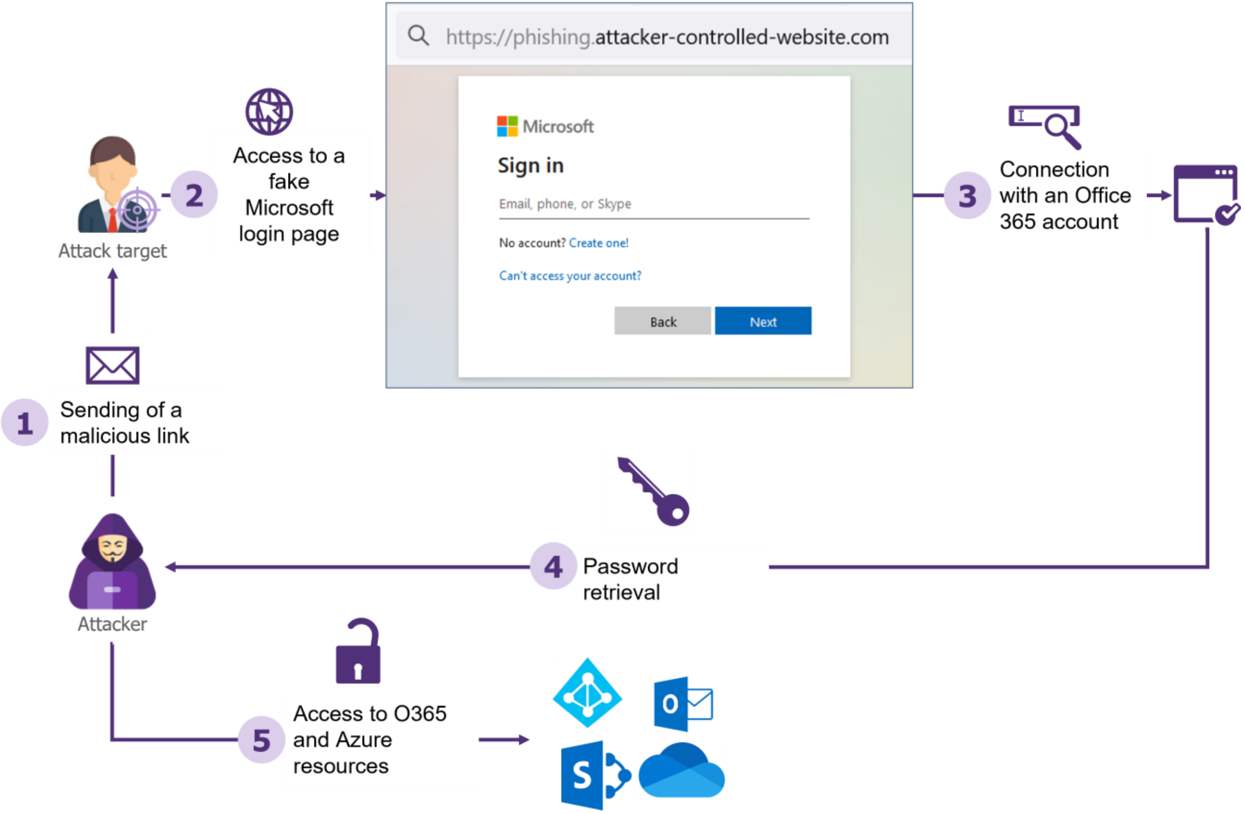
From a Telegram account investigators believe is owned by Ogletree, in October 2023 the 19-year-old bragged to the administrator of the money laundering service about his exploits, claiming to have earned “$300k past 24 hours” through an exploit against a cryptocurrency company. He suggested the launderer “hack internet service provider with lots of customer emails” in order to direct crypto customers to a “phishing site.”

“You can make $10m a year easily doing it if dedicated,” he allegedly told the administrator.



```
DeviceNetworkEvents
| where RemoteUrl contains "api.telegram.org"
| project
    TimeGenerated,
    DeviceName,
    InitiatingProcessFileName,
    InitiatingProcessCommandLine,
    InitiatingProcessAccountName,
    InitiatingProcessAccountDomain
```

Phase 1: Phishing



Attack target

2 Access to a fake Microsoft login page

3 Connection with an Office 365 account

1 Sending of a malicious link

4 Password retrieval

Attacker

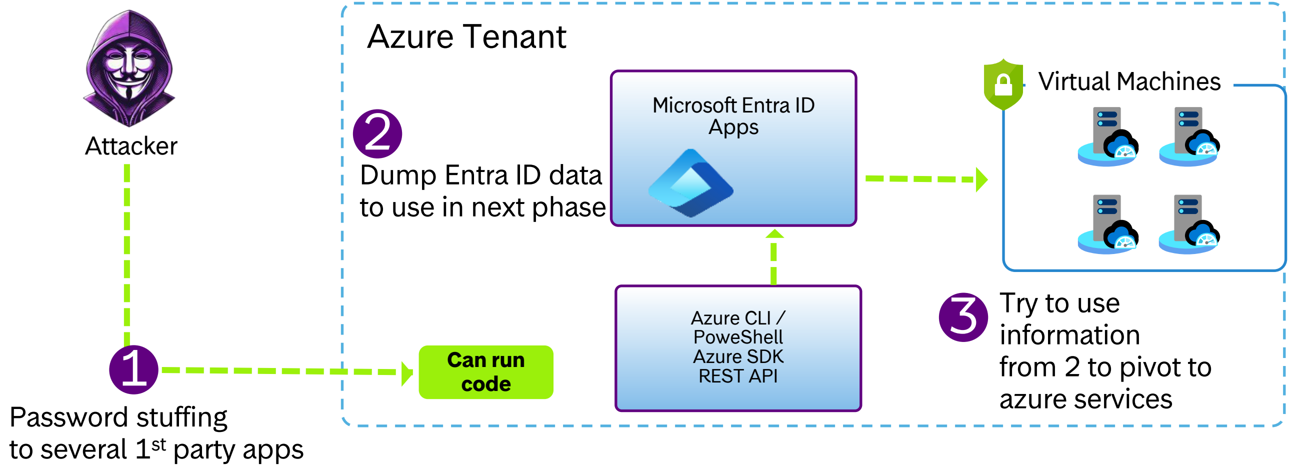
5 Access to O365 and Azure resources

https://phishing.attacker-controlled-website.com
Microsoft
Sign in
Email, phone, or Skype
No account? Create one!
Can't access your account?
Back
Next

Source: riskinsight

Phase 2: Attack path MFA - Reconnaissance

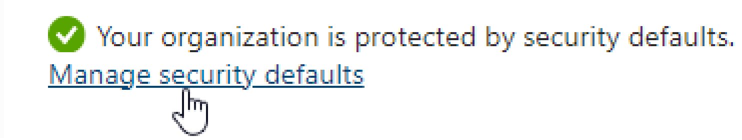
Passwords are strong enough?



1 Password stuffing to several 1st party apps

2 Dump Entra ID data to use in next phase

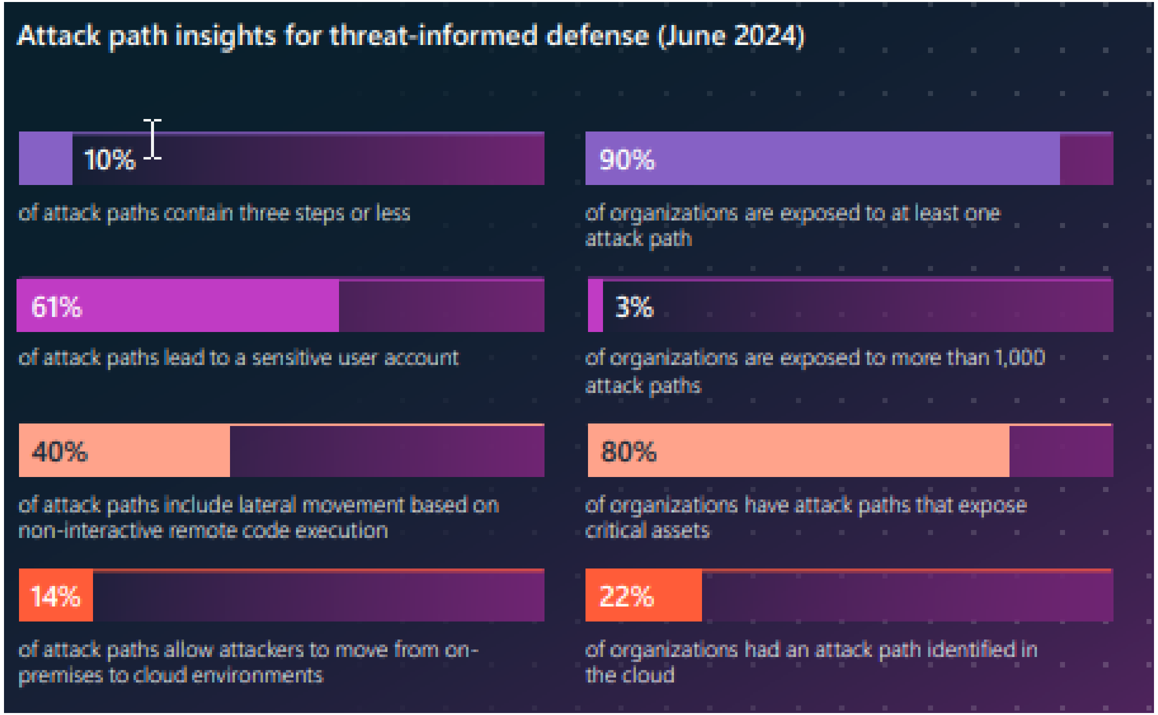
3 Try to use information from 2 to pivot to azure services



✓ Your organization is protected by security defaults.

Manage security defaults

Understand your attack paths



Attack path insights for threat-informed defense (June 2024)

10% of attack paths contain three steps or less

90% of organizations are exposed to at least one attack path

61% of attack paths lead to a sensitive user account

3% of organizations are exposed to more than 1,000 attack paths

40% of attack paths include lateral movement based on non-interactive remote code execution

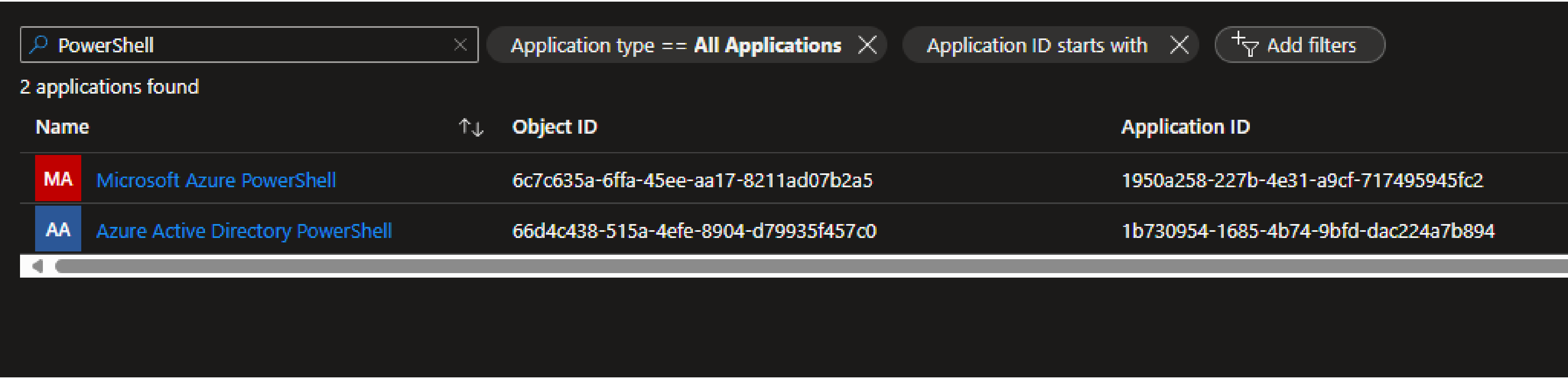
80% of organizations have attack paths that expose critical assets

14% of attack paths allow attackers to move from on-premises to cloud environments

22% of organizations had an attack path identified in the cloud

Detection and protection options

- Demo



PowerShell

Application type == **All Applications**

Application ID starts with

2 applications found

Name	Object ID	Application ID
MA Microsoft Azure PowerShell	6c7c635a-6ffa-45ee-aa17-8211ad07b2a5	1950a258-227b-4e31-a9cf-717495945fc2
AA Azure Active Directory PowerShell	66d4c438-515a-4efe-8904-d79935f457c0	1b730954-1685-4b74-9bfd-dac224a7b894

Application types

1st party apps

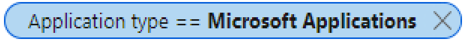
- Developed by Microsoft and are designed to work seamlessly with the Microsoft Ecosystem
- These apps tend to be forgotten but can have a quite large attack surface.
- These apps don’t always result in a service principal being created in your tenant. This can lead to confusion.

Own applications

- Developed or created by the organization
- Typical misconfiguration issues with broad access (owners
- Poor credential management
- Conditional Access
- Lack of monitoring of these apps

3rd party apps

- Managing access can be more complex than 1st party.
- Supply chain review of 3rd party apps is rarely conducted. (NSM Report)
- Conditional Access policy misconfigurations.
- Too broad access
- Lack of risk detection and monitoring


Application type == **Microsoft Applications**

Apps we might want to control or plan for migration

Microsoft Graph PowerShell / Microsoft Graph Command Line Tools
(14d82eec-204b-4c2f-b7e8-296a70dab67e)

Microsoft Graph PowerShell (Recommended)

Azure Active Directory PowerShell (1b730954-1685-4b74-9bfd-dac224a7b894)

Apps can't make API request after February 1st 2025

Microsoft Azure PowerShell (1950a258-227b-4e31-a9cf-717495945fc2)

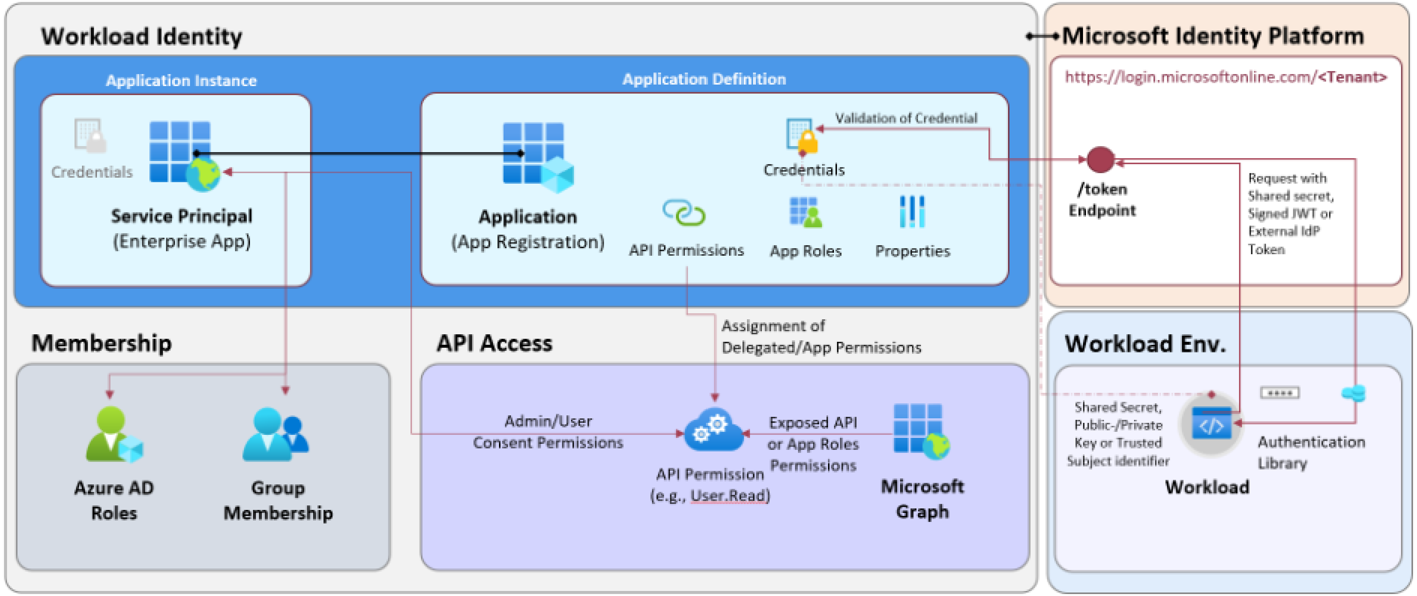
Planned for deprecation March 30, 2024.

Graph Explorer (de8bc8b5-d9f9-48b1-a8ad-b748da725064)

Powerful tool that allows you to make requests and see responses against Microsoft Graph

Verify first-party Microsoft applications

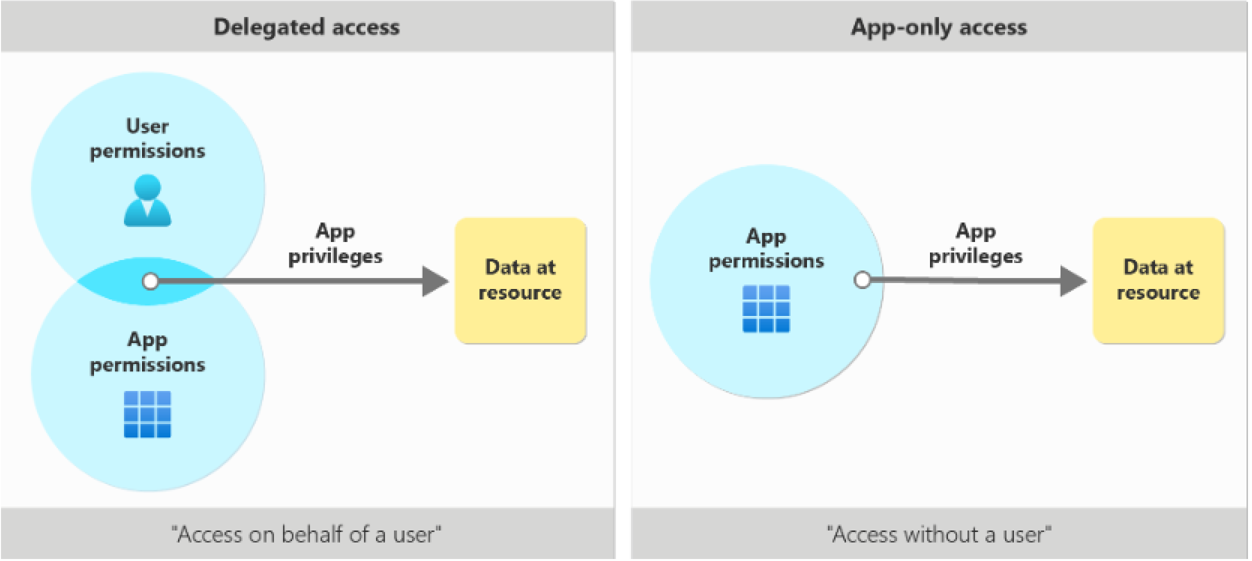
Entra ID Objects of Application Identities



Source: cloud-architekt.net/

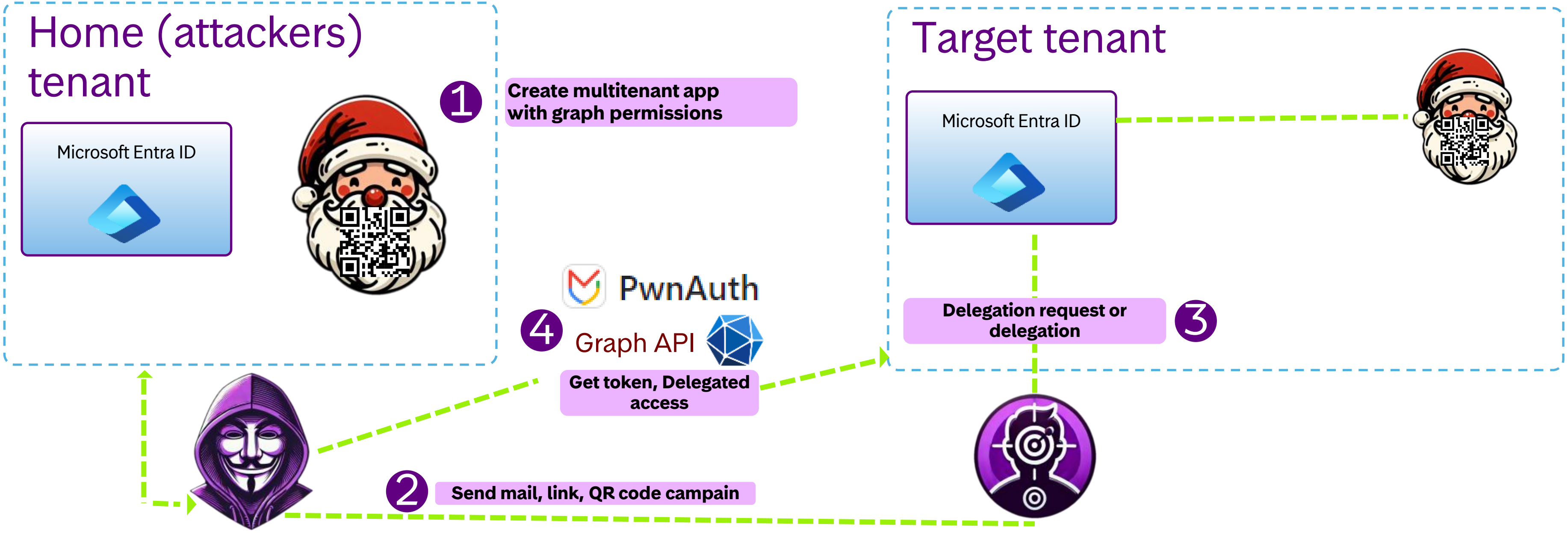
Navigating Entra ID: Consents

Delegated vs application



Illicit consent grant attack

Delegated access scenario



Home (attackers) tenant

Microsoft Entra ID

1 Create multitenant app with graph permissions

PwnAuth

4 Graph API

Get token, Delegated access

2 Send mail, link, QR code campain

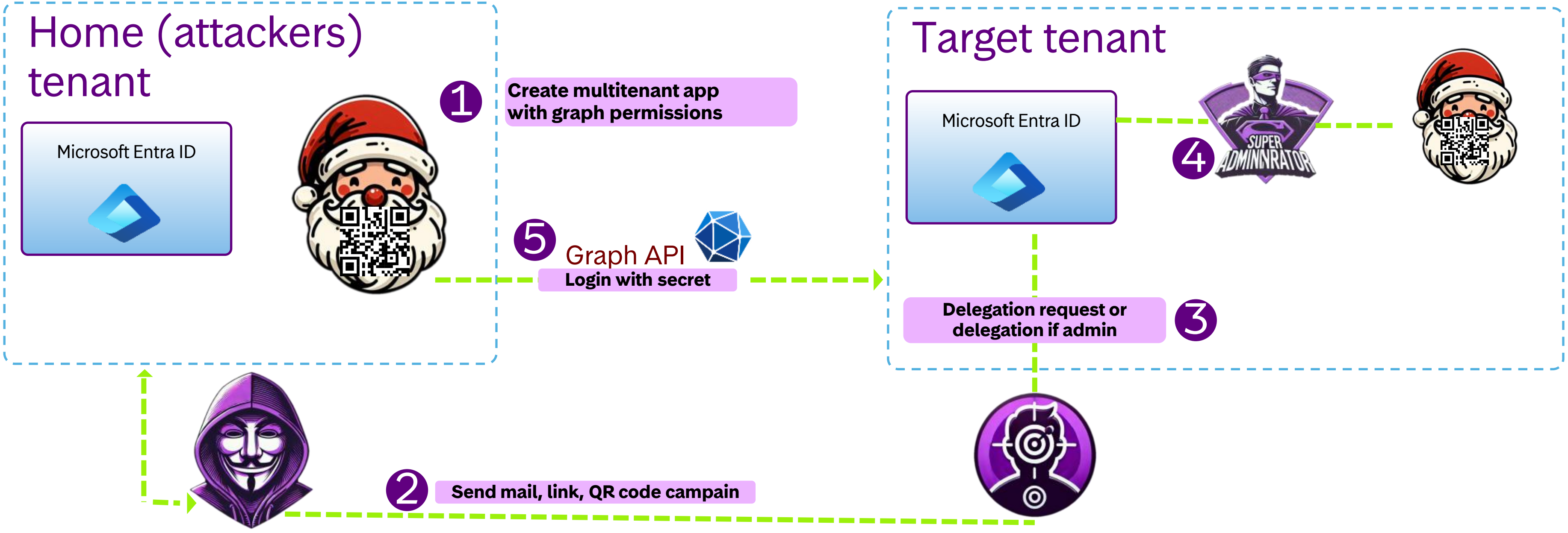
Target tenant

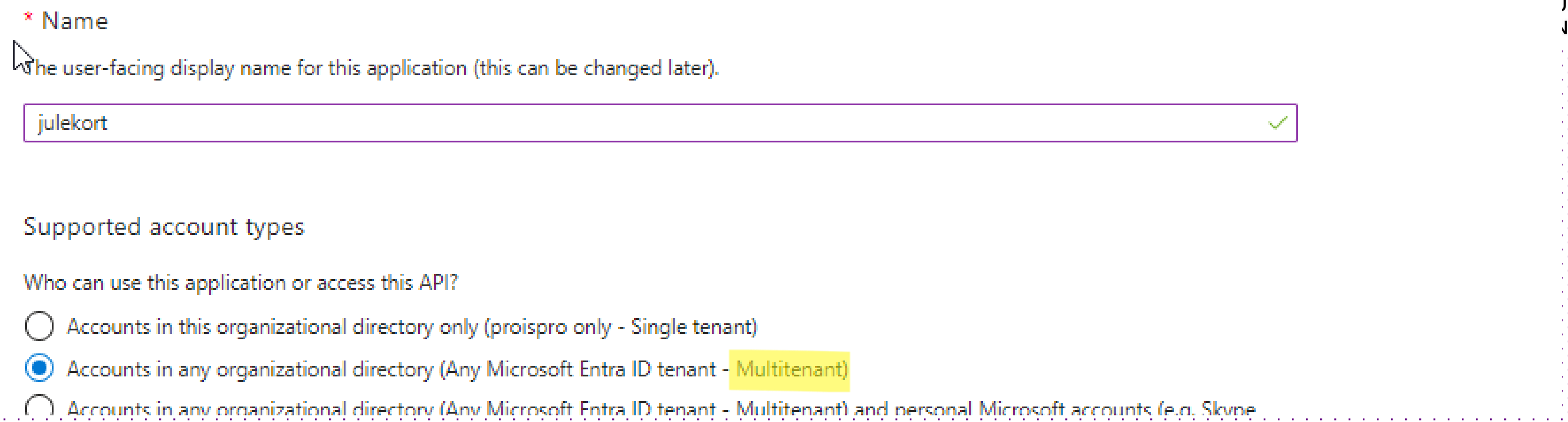
Microsoft Entra ID

Delegation request or delegation 3

Illicit consent grant attack

App consent access scenario





* Name

The user-facing display name for this application (this can be changed later).

julekort ✓

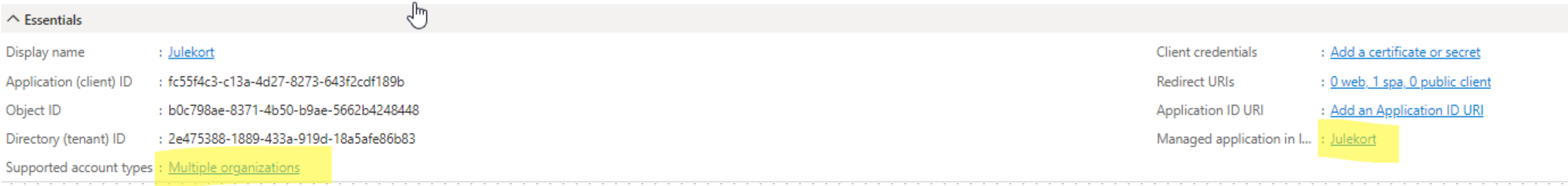
Supported account types

Who can use this application or access this API?

○ Accounts in this organizational directory only (proispro only - Single tenant)

● Accounts in any organizational directory (Any Microsoft Entra ID tenant - Multitenant)

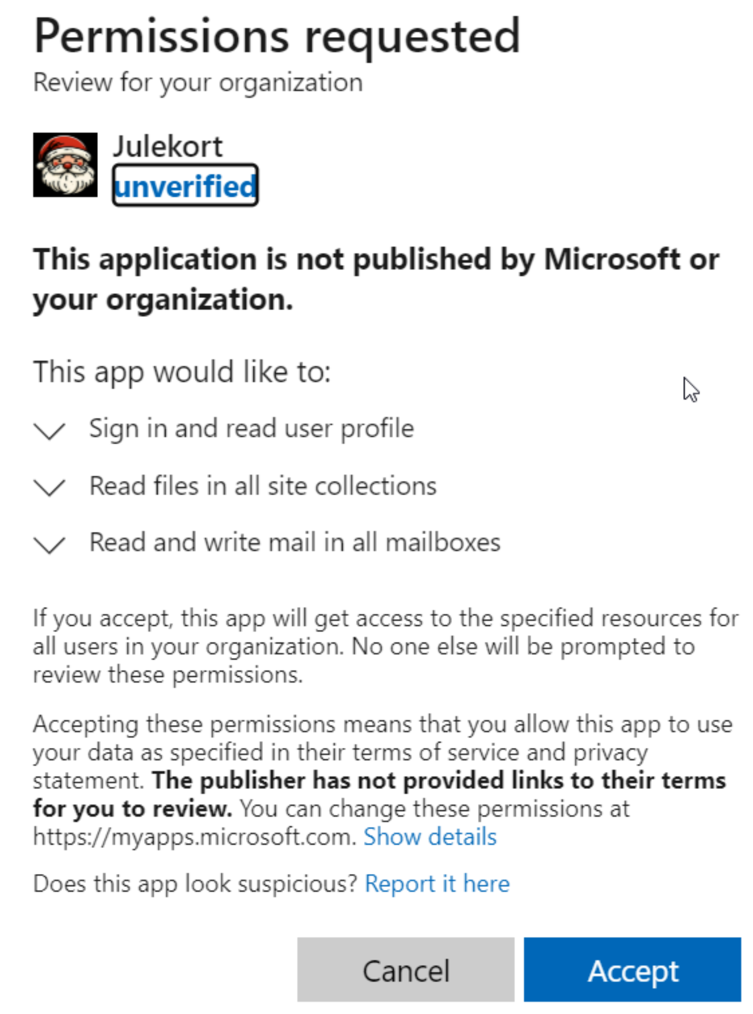
○ Accounts in any organizational directory (Any Microsoft Entra ID tenant - Multitenant) and personal Microsoft accounts (e.g. Skype



Essentials

Display name	: Julekort	Client credentials	: Add a certificate or secret
Application (client) ID	: fc55f4c3-c13a-4d27-8273-643f2cdf189b	Redirect URIs	: 0 web, 1 spa, 0 public client
Object ID	: b0c798ae-8371-4b50-b9ae-5662b4248448	Application ID URI	: Add an Application ID URI
Directory (tenant) ID	: 2e475388-1889-433a-919d-18a5afe86b83	Managed application in l...	: Julekort
Supported account types	: Multiple organizations		

https://tinyurl.com/julekortasug



Permissions requested

Review for your organization

Julekort
unverified

This application is not published by Microsoft or your organization.

This app would like to:

- Sign in and read user profile
- Read files in all site collections
- Read and write mail in all mailboxes

If you accept, this app will get access to the specified resources for all users in your organization. No one else will be prompted to review these permissions.

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

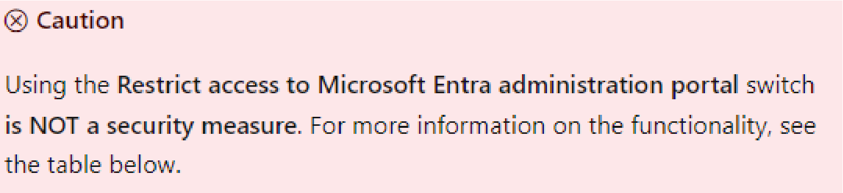
Does this app look suspicious? Report it here

Demo 3rd party app rights

Setup basic application governance

Setup Entra ID User settings

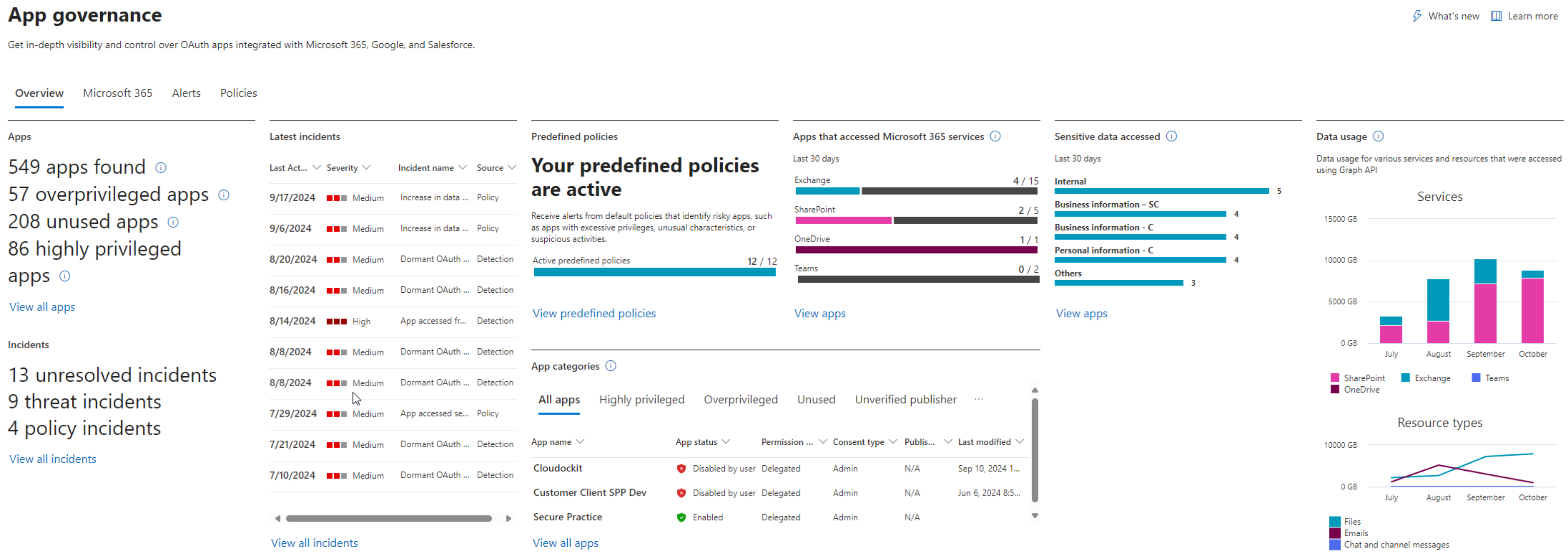
- **Only administrators are Allowed to register applications.**
- **Only administrators are allowed to consent to applications.**
- **An admin consent workflow be configured for applications.**
- **Group owners should not be allowed to consent to applications.**



ⓧ Caution

Using the **Restrict access to Microsoft Entra administration portal** switch **is NOT a security measure**. For more information on the functionality, see the table below.

Azure
User group
Norway



App governance

What's new Learn more

Get in-depth visibility and control over OAuth apps integrated with Microsoft 365, Google, and Salesforce.

Overview Microsoft 365 Alerts Policies

Apps

549 apps found ⓘ
57 overprivileged apps ⓘ
208 unused apps ⓘ
86 highly privileged apps ⓘ

View all apps

Incidents

13 unresolved incidents
9 threat incidents
4 policy incidents

View all incidents

Latest incidents

Last Act...	Severity	Incident name	Source
9/17/2024	Medium	Increase in data ...	Policy
9/6/2024	Medium	Increase in data ...	Policy
8/20/2024	Medium	Dormant OAuth ...	Detection
8/16/2024	Medium	Dormant OAuth ...	Detection
8/14/2024	High	App accessed fr...	Detection
8/8/2024	Medium	Dormant OAuth ...	Detection
8/8/2024	Medium	Dormant OAuth ...	Detection
7/29/2024	Medium	App accessed se...	Policy
7/21/2024	Medium	Dormant OAuth ...	Detection
7/10/2024	Medium	Dormant OAuth ...	Detection

View all incidents

Predefined policies

Your predefined policies are active

Receive alerts from default policies that identify risky apps, such as apps with excessive privileges, unusual characteristics, or suspicious activities.

Active predefined policies 12 / 12

View predefined policies

Apps that accessed Microsoft 365 services ⓘ

Last 30 days

Exchange	4 / 15
SharePoint	2 / 5
OneDrive	1 / 1
Teams	0 / 2

View apps

Sensitive data accessed ⓘ

Last 30 days

Internal	5
Business information – SC	4
Business information - C	4
Personal information - C	4
Others	3

View apps

App categories ⓘ

All apps Highly privileged Overprivileged Unused Unverified publisher ···

App name	App status	Permission ...	Consent type	Publis...	Last modified
Cloudockit	Disabled by user	Delegated	Admin	N/A	Sep 10, 2024 1...
Customer Client SPP Dev	Disabled by user	Delegated	Admin	N/A	Jun 6, 2024 8:5...
Secure Practice	Enabled	Delegated	Admin	N/A	

View all apps

Data usage ⓘ

Data usage for various services and resources that were accessed using Graph API

Security portal – must be turned on

Self-assessment

- Inventory off applications is key
- Legal obligations to Dora
- Start with tier 0 rights
- Check if you have broad email send rights
- Use Role based access for application in Exchange online.
- When creating apps, use least privileged scopes
- Create gallery applications if possible

Navigating Entra ID: Detection and OPS

Detection with log analytics –> Monitor alert, Sentinel incident or hunting

Costs graph activity of this log?

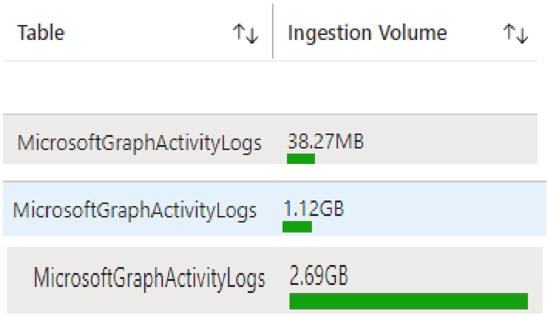
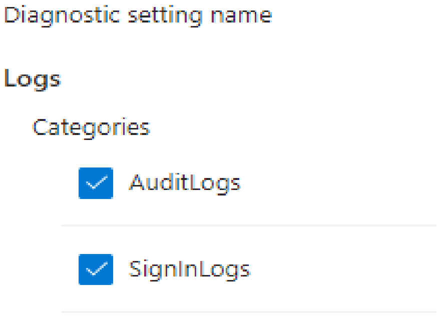


	Table	Ingestion Volume
Corp A 200 users	MicrosoftGraphActivityLogs	38.27MB
Corp B 40K users	MicrosoftGraphActivityLogs	1.12GB
Corp Finance	MicrosoftGraphActivityLogs	2.69GB



Diagnostic setting name

Logs

Categories

☑ AuditLogs

☑ SignInLogs

References / Tools

AzureAD/MSIdentityTools: PowerShell modules Entra ID
https://graphpermissions.merill.net/
MFASweep: A tool for checking if MFA status
Microsoft Digital Defense Report 2024
aka.ms/AzADSPI - Insights and change tracking on Microsoft Entra ID Service Principals
AppConsent
A New App Consent Attack: Hidden Consent Grant - Semperis

Azure
User group
Norway

DO YOU HAVE ANY QUESTIONS?