WIZ Research

OAuth Apps in Azure

Everything you need to know

WIZ Research

About us

Shahar Dorfman

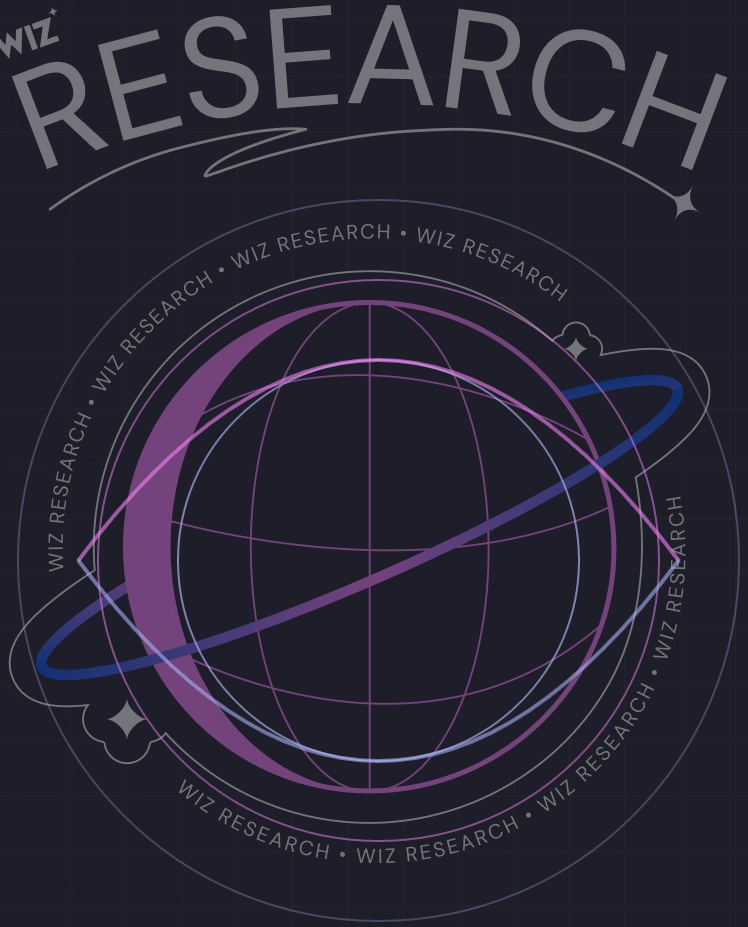
Threat Researcher, Wiz

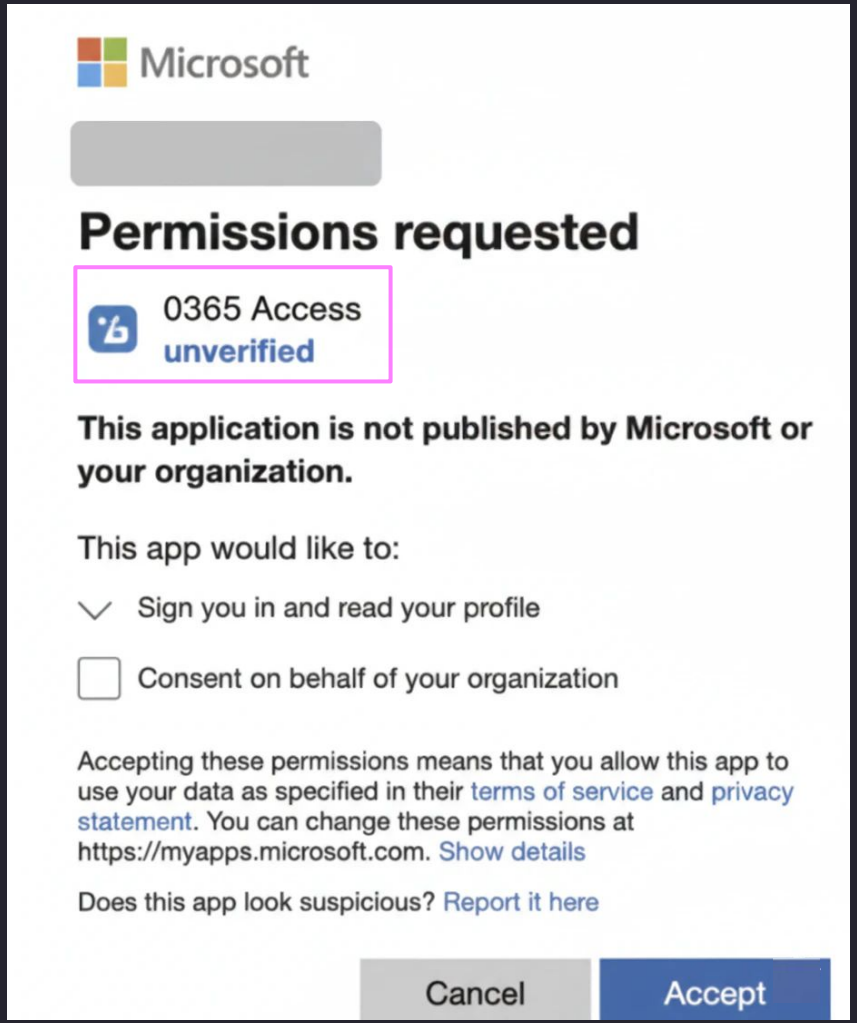
@shahardorf

Sapir Federovsky

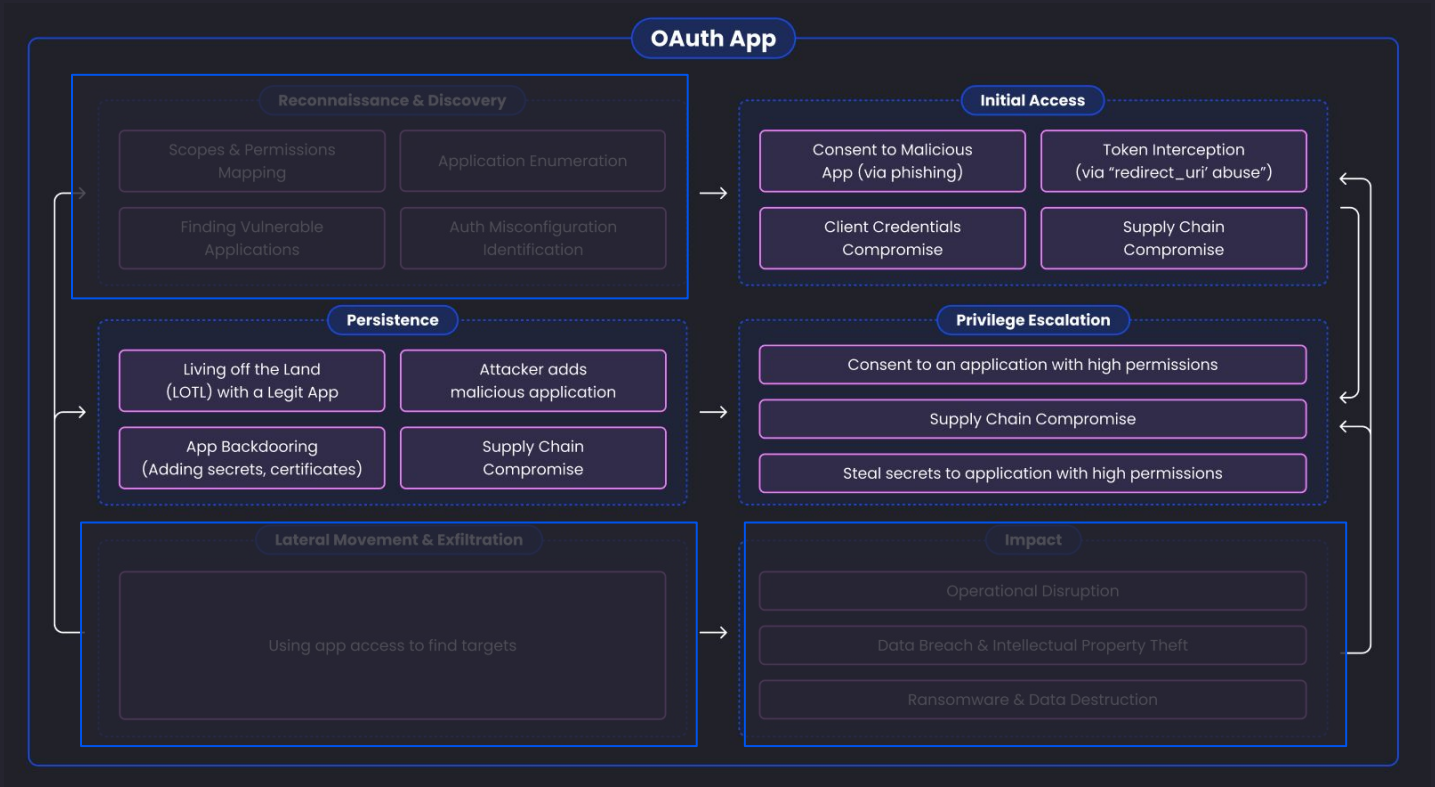
Threat Researcher, Wiz

@sapirxfed




Microsoft
Permissions requested
0365 Access
unverified
This application is not published by Microsoft or your organization.
This app would like to:
Sign you in and read your profile
Consent on behalf of your organization
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
Does this app look suspicious? Report it here
Cancel
Accept

OAuth App Attack Path

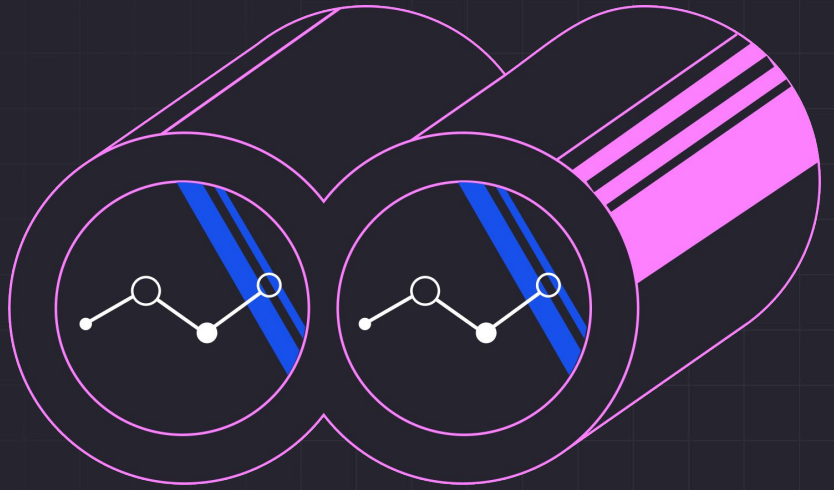


Agenda

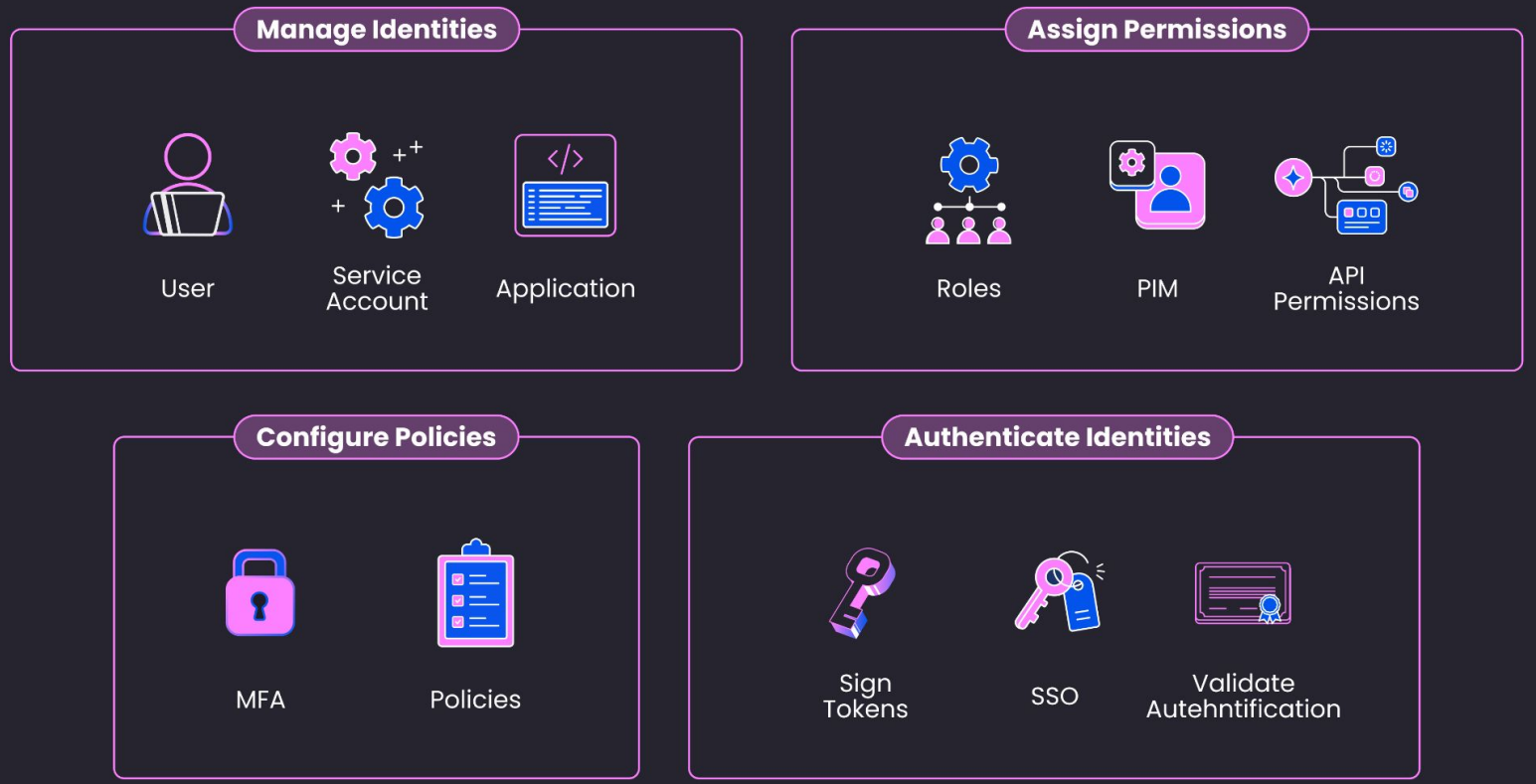
- OAuth Apps Threat Model
- Legitimate App Misused (LoLApps)
- Entra
- Permissions Abuse
- OAuth Apps 101
- Why is it hard
- Malicious Apps
- Compromised App (Supply Chain)

WIZ Research

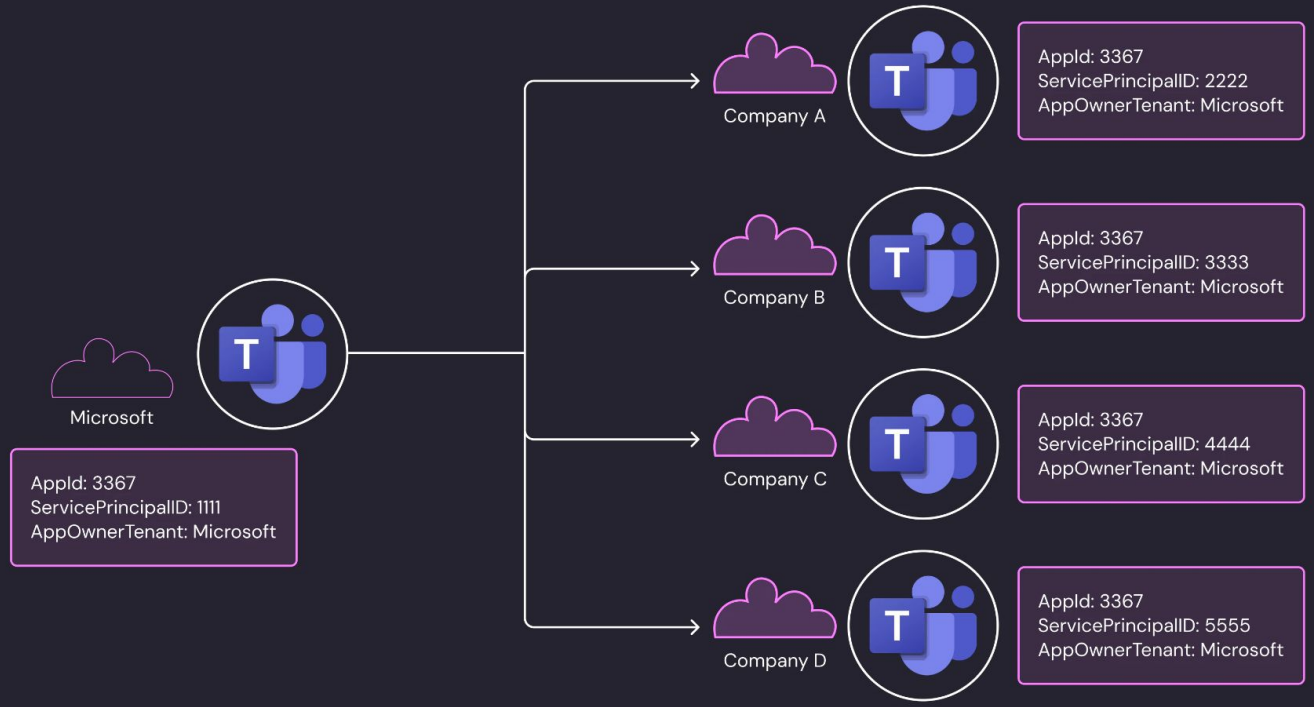
OAuth Apps 101



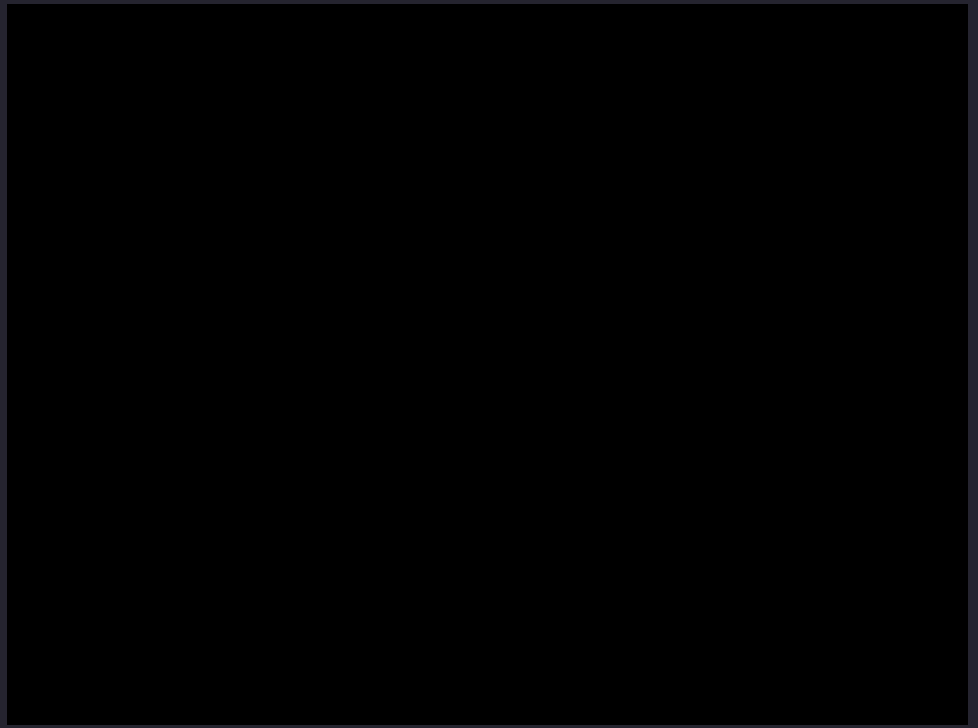
Entra


Manage Identities
User
Service Account
Application
Assign Permissions
Roles
PIM
API Permissions
Configure Policies
MFA
Policies
Authenticate Identities
Sign Tokens
SSO
Validate Autehntification

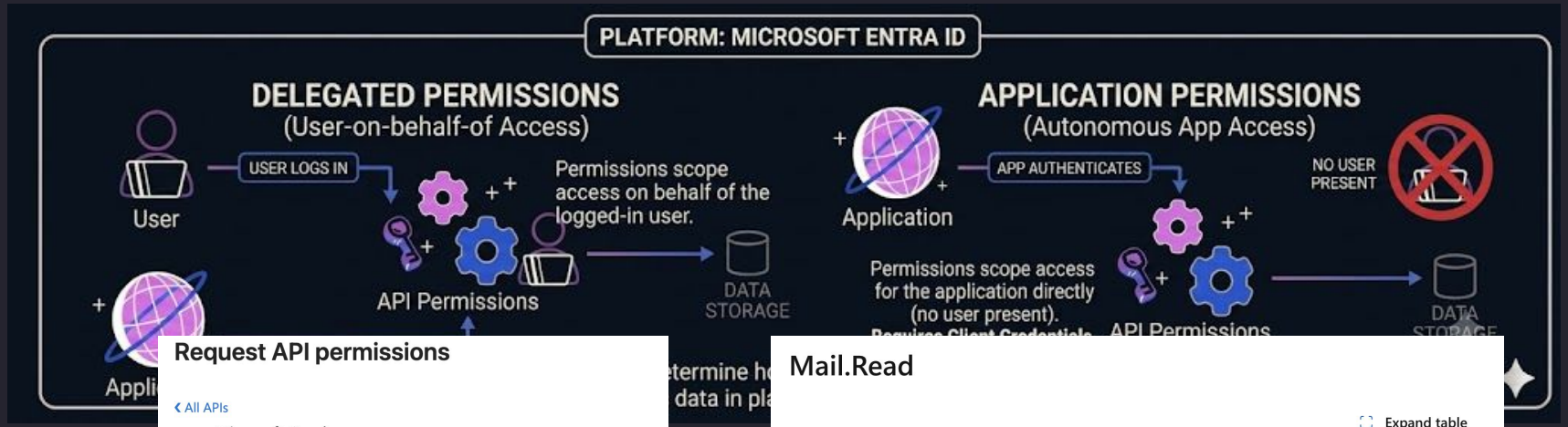
Application vs Service Principal



Creating an OAuth Application



Delegated vs Application Permissions



Request API permissions

‹ All APIs

Microsoft Graph

https://graph.microsoft.com/ Docs

What type of permissions does your application require?

Delegated permissions

Your application needs to access the API as the signed-in user.

Application permissions

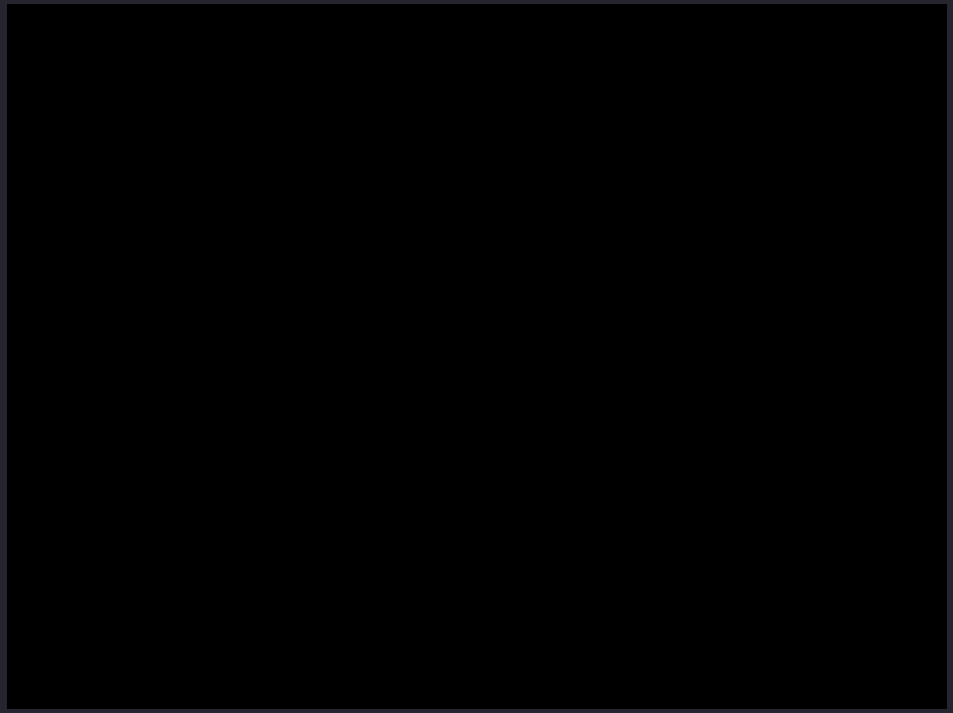
Your application runs as a background service or daemon without a signed-in user.

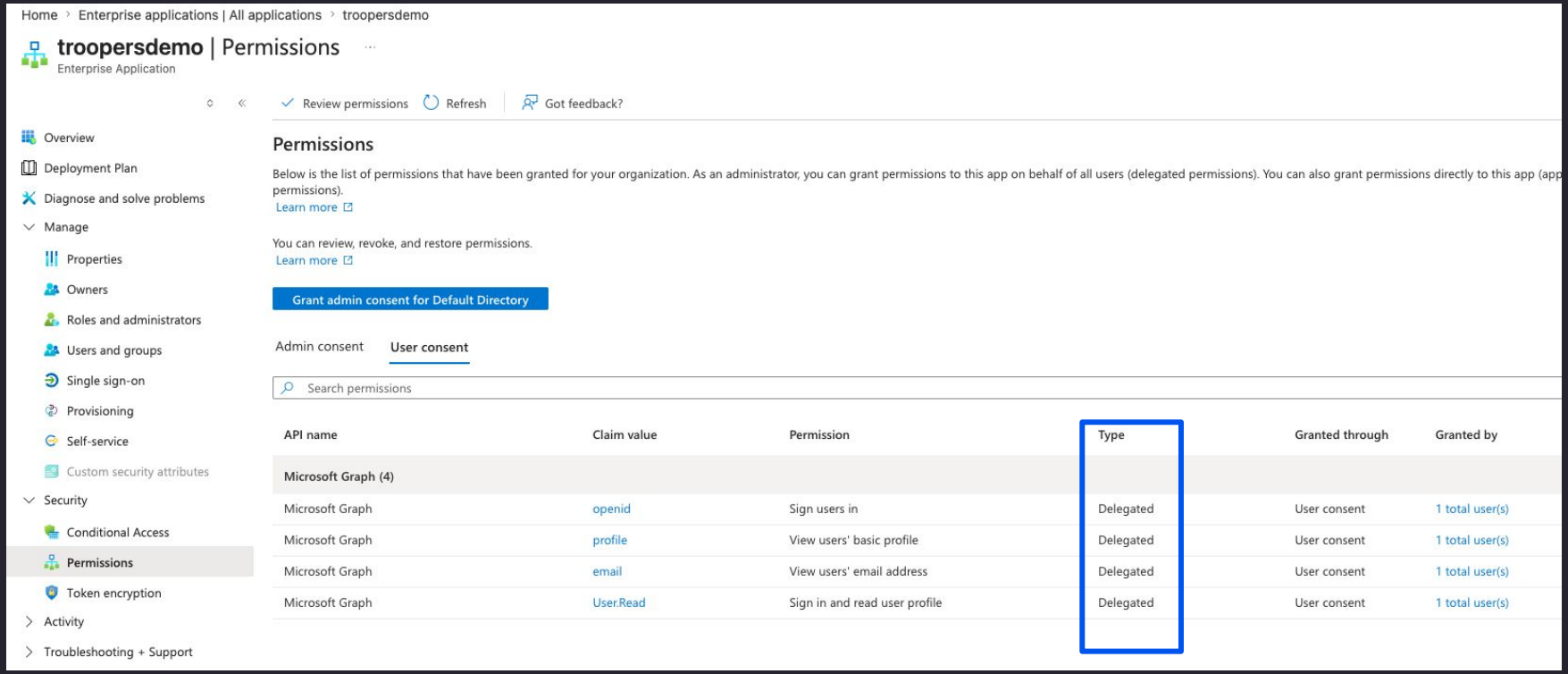
Mail.Read

Expand table

Category	Application	Delegated
Identifier	810c84a8-4a9e-49e6-bf7d-12d183f40d01	570282fd-fa5c-430d-a7fd-fc8dc98a9dca
DisplayText	Read mail in all mailboxes	Read user mail
Description	Allows the app to read mail in all mailboxes without a signed-in user.	Allows the app to read the signed-in user's mailbox.
AdminConsentRequired	Yes	No

OAuth Consent




Home › Enterprise applications | All applications › troopersdemo
troopersdemo | Permissions
Enterprise Application
Review permissions
Refresh
Got feedback?
Overview
Deployment Plan
Diagnose and solve problems
Manage
Properties
Owners
Roles and administrators
Users and groups
Single sign-on
Provisioning
Self-service
Custom security attributes
Security
Conditional Access
Permissions
Token encryption
Activity
Troubleshooting + Support
Permissions
Below is the list of permissions that have been granted for your organization. As an administrator, you can grant permissions to this app on behalf of all users (delegated permissions). You can also grant permissions directly to this app (app permissions).
Learn more
You can review, revoke, and restore permissions.
Learn more
Grant admin consent for Default Directory
Admin consent
User consent
Search permissions
API name
Claim value
Permission
Type
Granted through
Granted by
Microsoft Graph (4)
Microsoft Graph
openid
Sign users in
Delegated
User consent
1 total user(s)
Microsoft Graph
profile
View users' basic profile
Delegated
User consent
1 total user(s)
Microsoft Graph
email
View users' email address
Delegated
User consent
1 total user(s)
Microsoft Graph
User.Read
Sign in and read user profile
Delegated
User consent
1 total user(s)

What Was Created?

App ID: 0d2fa037-dc1a-4153-80e5-bd30a17fb247,

App owner Tenant id: 237e701c-327f-4cad-a5a1-ddda2412d89d9,

Consent Date: 2025-09-05T14:09:03.000Z,

Creation Date: 1970-01-01T00:00:00.000Z,

Homepage: https://docusign.com,

Display name: Docusign for Outlook,

Reply URL:

https://services.dev.docusign.net/integrations-office/v1.0/App/eSignature,

Verified publisher: Docusign,

Verified publisher ID: 2290474

The App Behind the Attack

Malicious App

Legitimate App Misused (LoLApps)

Overprivileged/Leaked Creds of App

Compromised App (Supply Chain)

Malicious App

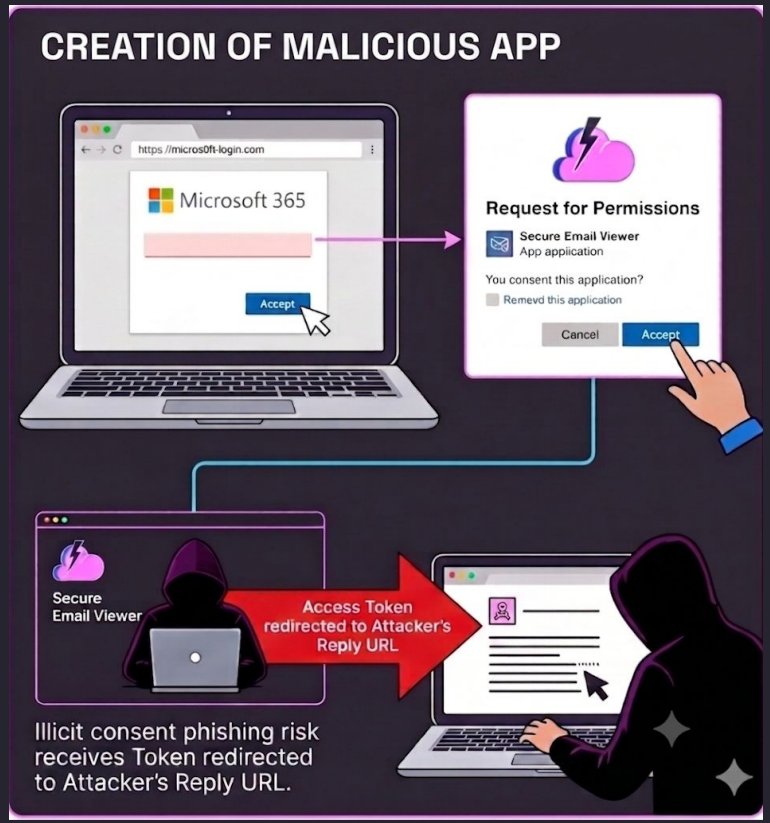
Create malicious apps to steal tokens through a crafted reply URL, maintain tenant persistence, and achieve privileges.

Permissions

Whatever the attacker configured the app to request

What attacker needs to do

Build the app, phish the user



Legitimate App Misused (LoLApps)

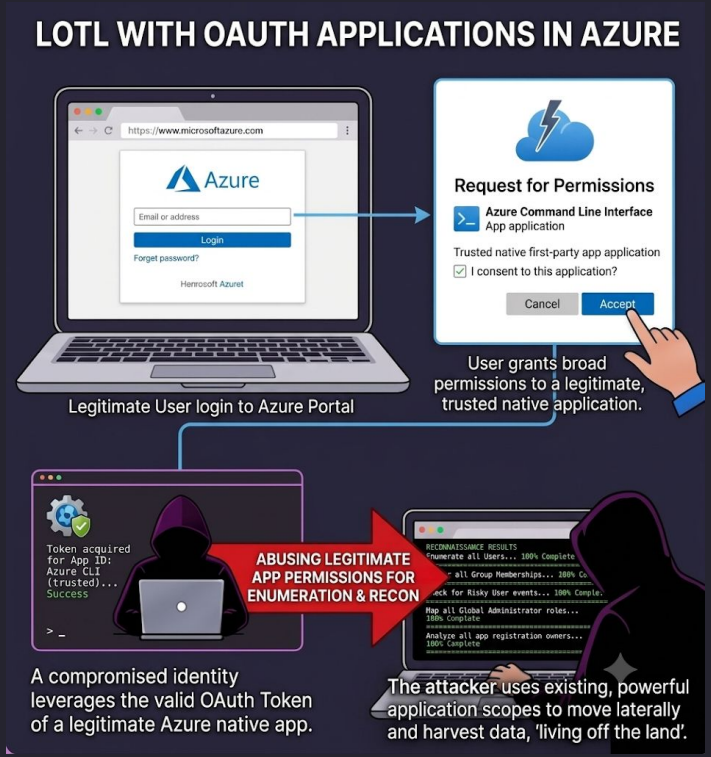
Abusing the built-in features of normal, trusted apps for malicious purposes.

Permissions

Whatever the app can do with the user access

What attacker needs to do

Get the user's password



Overprivileged/Leaked Creds of App

Abuse permissions, secrets or certificates to expand access and maintain persistence.

Permissions

Whatever the app has

What attacker needs to do

Find the app's credentials / add their own secret

Compromised App (Supply Chain)

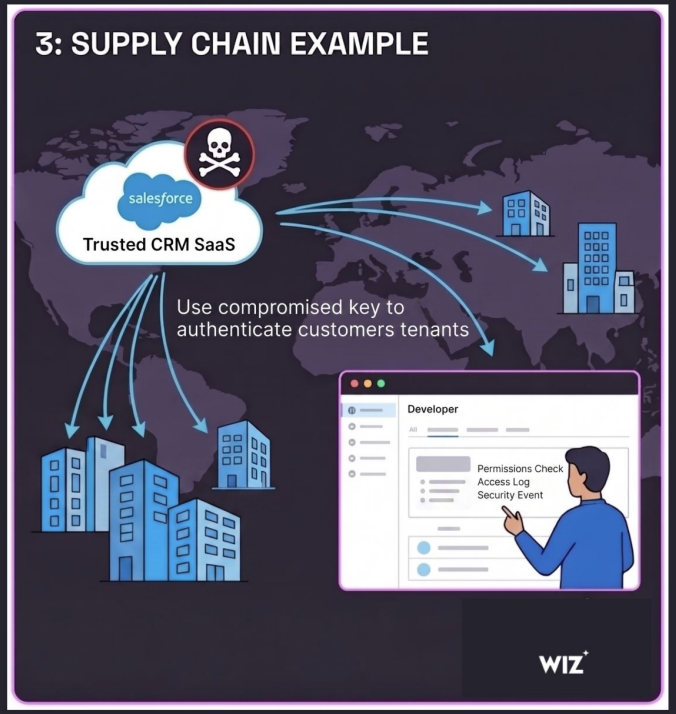
Gaining tenant access by compromising a trusted, pre-integrated third-party application.

Permissions

Whatever you gave the vendor

What attacker needs to do

Hack the vendor, not you



The App Behind the Attack

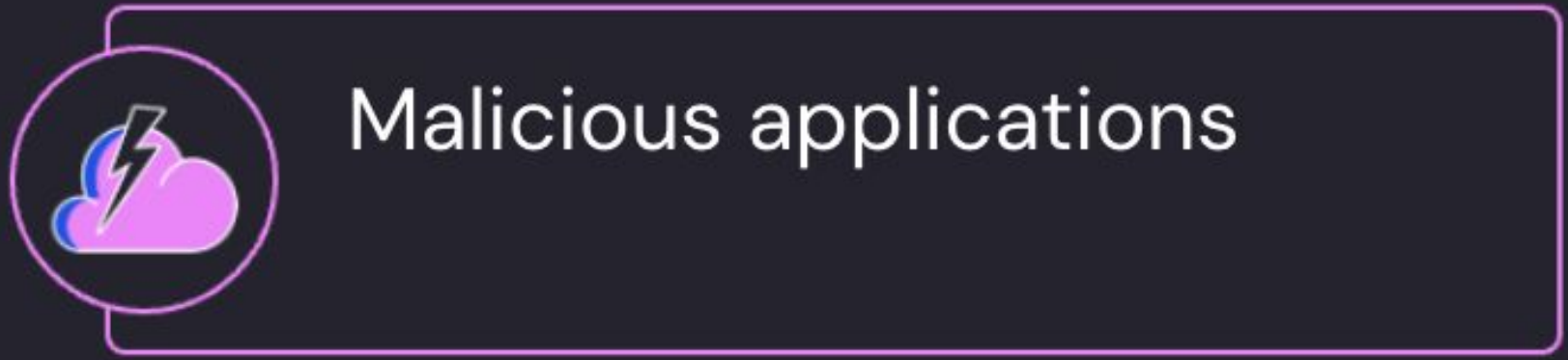
Malicious App

Legitimate App Misused (LoLApps)

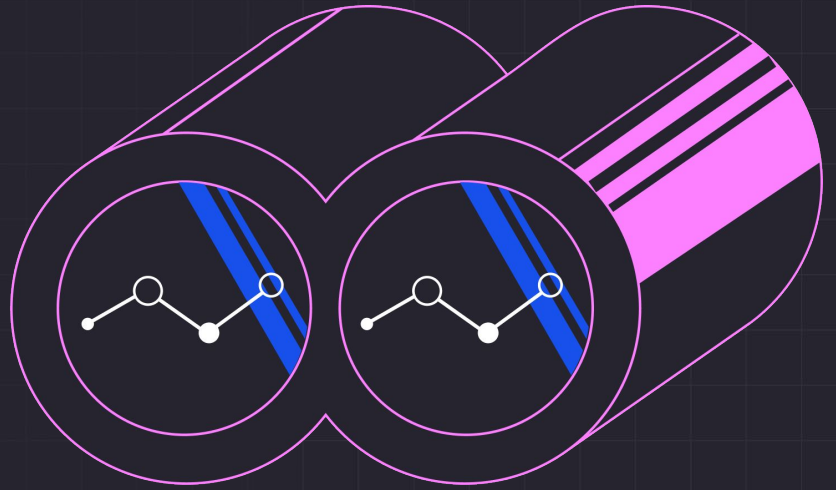
Overprivileged/Leaked Creds of App

Compromised App (Supply Chain)

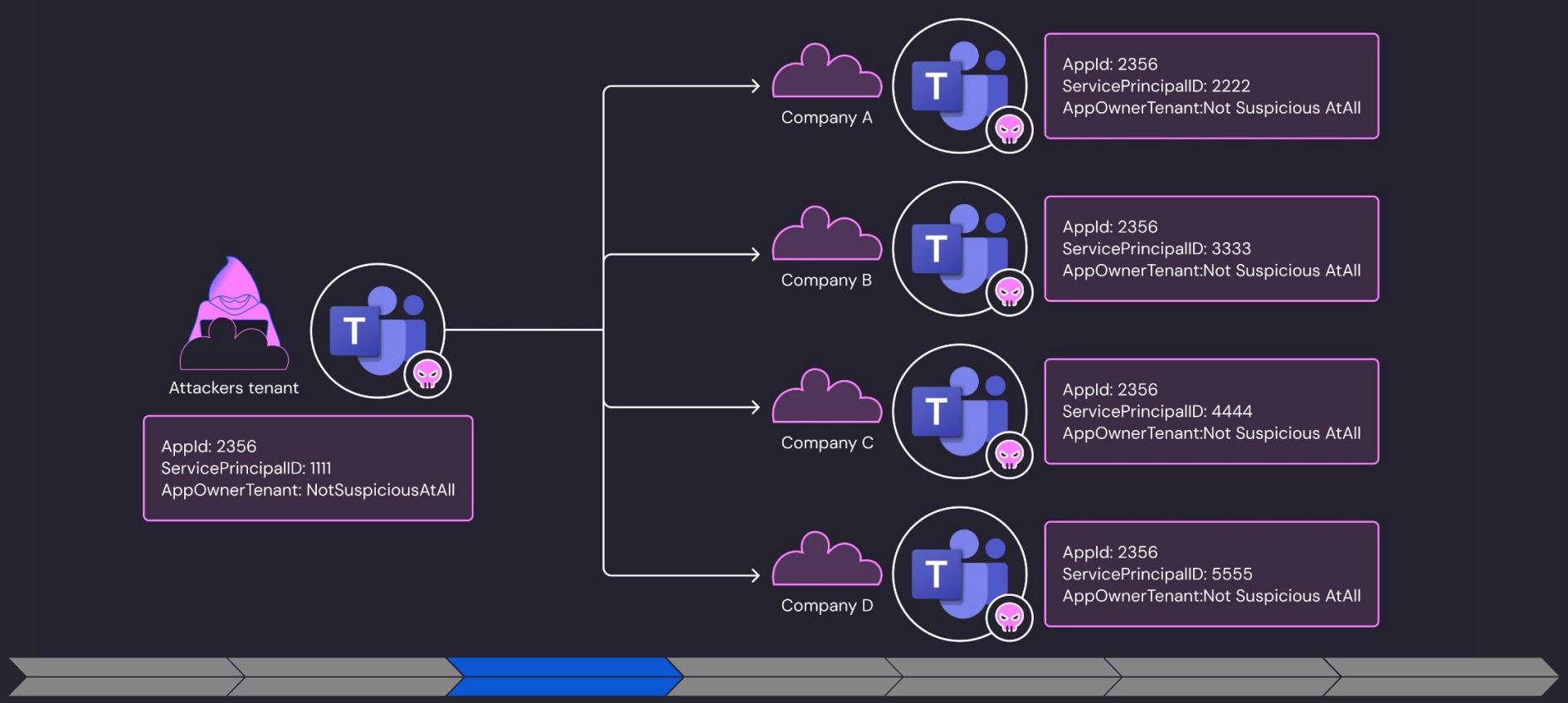
What's Next?



WIZ Research



Malicious Apps


Attackers tenant
AppId: 2356
ServicePrincipalID: 1111
AppOwnerTenant: NotSuspiciousAtAll
Company A
AppId: 2356
ServicePrincipalID: 2222
AppOwnerTenant:Not Suspicious AtAll
Company B
AppId: 2356
ServicePrincipalID: 3333
AppOwnerTenant:Not Suspicious AtAll
Company C
AppId: 2356
ServicePrincipalID: 4444
AppOwnerTenant:Not Suspicious AtAll
Company D
AppId: 2356
ServicePrincipalID: 5555
AppOwnerTenant:Not Suspicious AtAll

Applications Fields

LEGITIMATE APP:

App ID: 0d2fa037-dc1a-4153-80e5-bd30a17fb247,
App owner Tenant id:
237e701c-327f-4cad-a5a1-ddda2412d89d9,
Consent Date: 2025-09-05T14:09:03.000Z,
Creation Date: 1970-01-01T00:00:00.000Z,
Homepage: https://docusign.com,
App name: Docusign for Outlook,
Reply URL:
https://services.dev.docusign.net/integrations-office/v1.0/App/eSignature,
Verified publisher: Docusign,
Verified publisher ID: 2290474,
App owner name: Docusign
App owner domain: docusign.com

MALICIOUS APP:

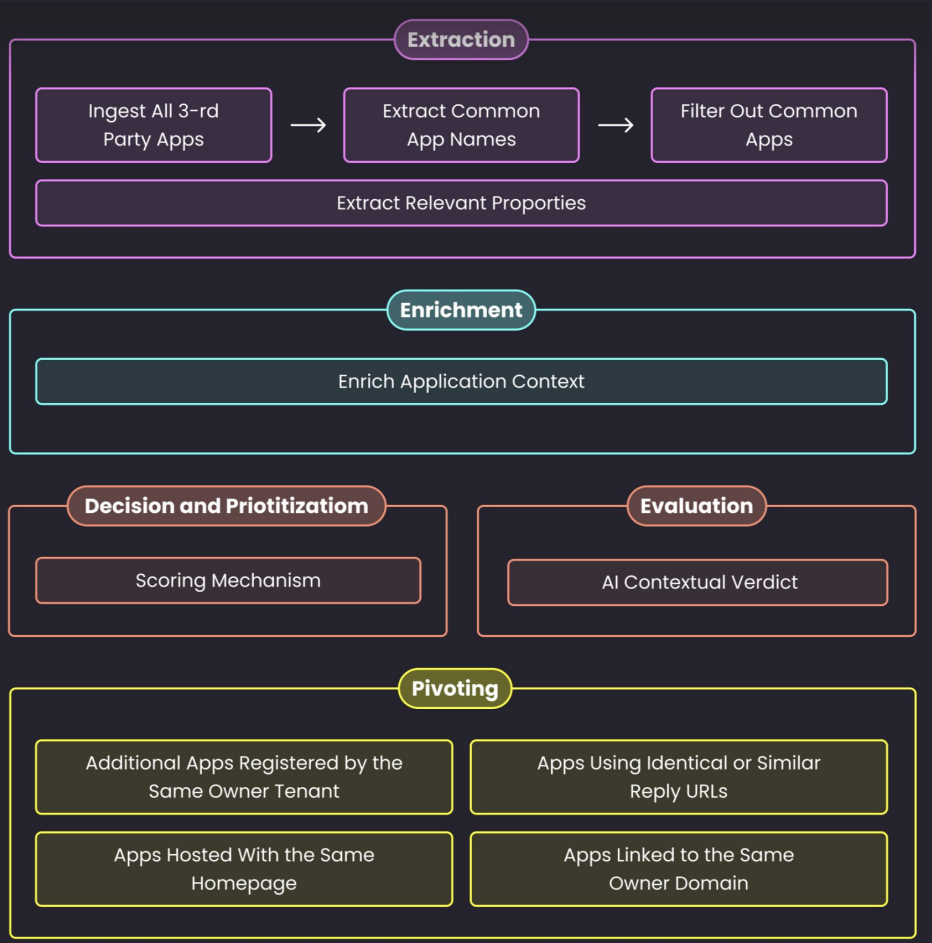
App ID: 22c606e8-7d68-4a09-89d9-c3c563a453a0,
App owner Tenant id:
34a773f5-d756-4912-9585-2f64d52d935e,
Consent Date: 2025-03-10T17:57:24.000Z,
Creation Date: 1970-01-01T00:00:00.000Z,
Homepage:
App name: Docusign,
Reply URL:
https://synapaketsteamworkspace.myclickfunnels.com/share-docus,
Verified publisher:
Verified publisher ID:
App owner name: Jackssons INC
App owner domain: jackssons.com

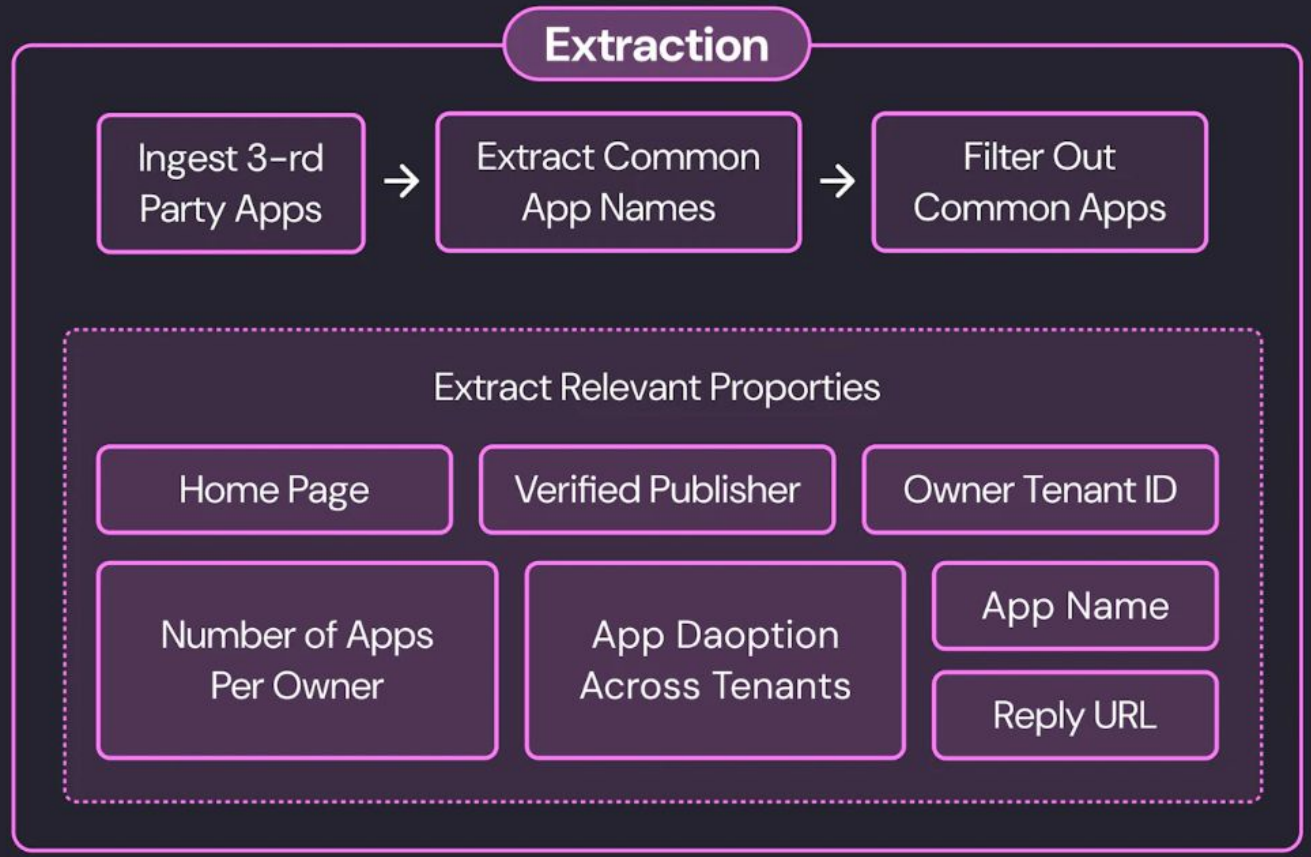
WIZ

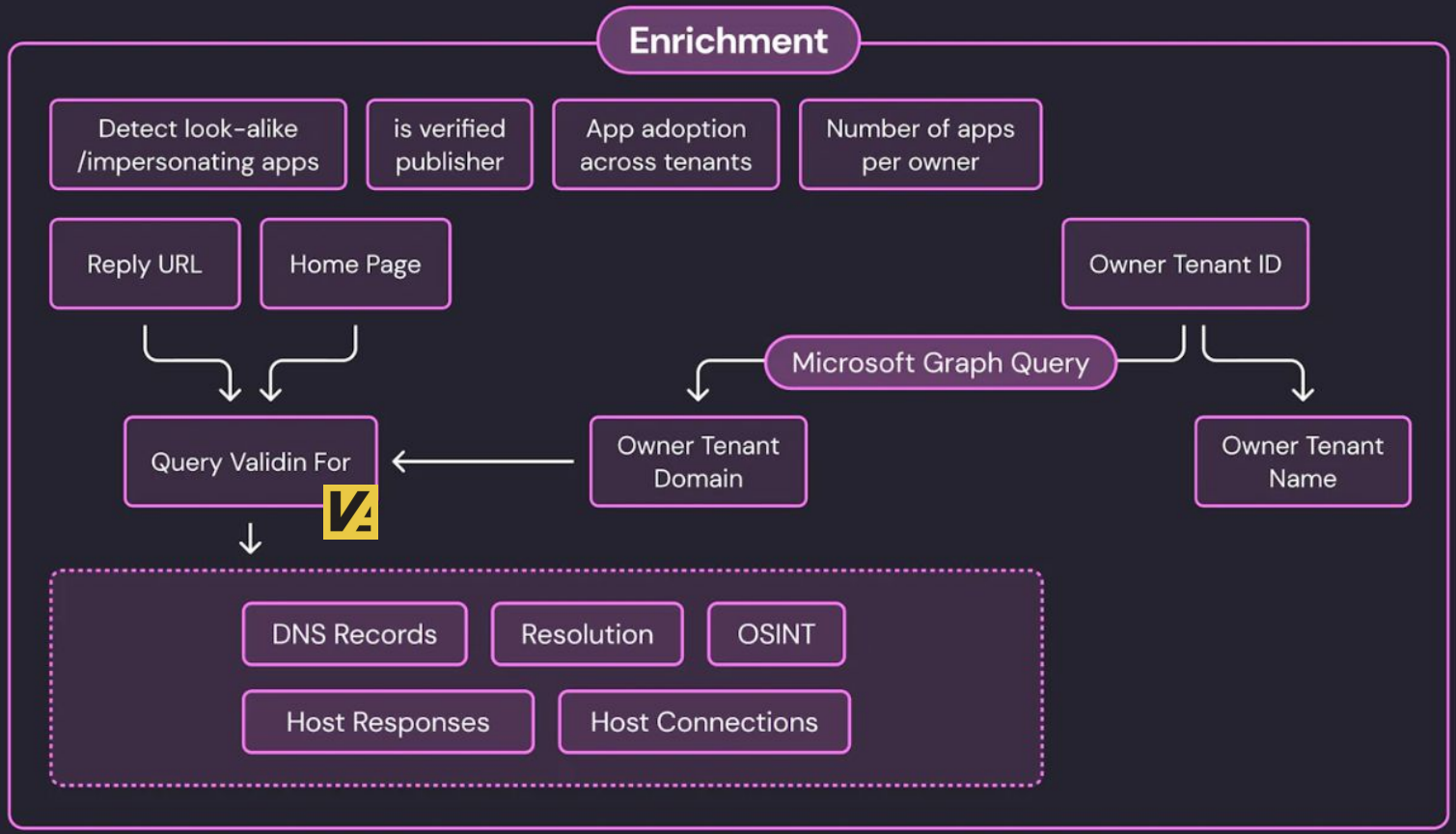
So How do We Detect This?

- Legitimate flow
- No malware / no exploit
- Looks like normal application usage
- Blends in with thousands of apps

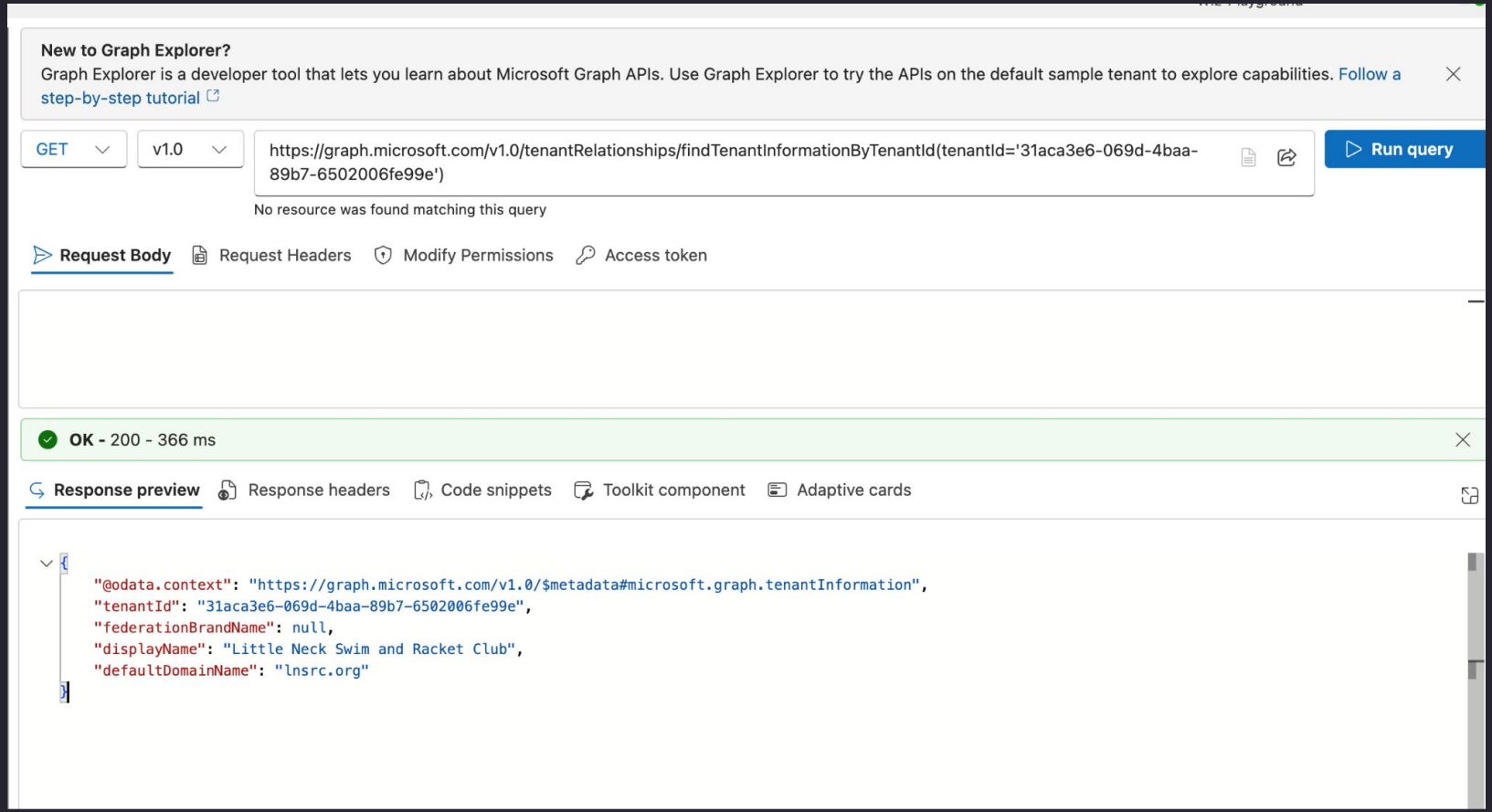
From Abuse to Detection

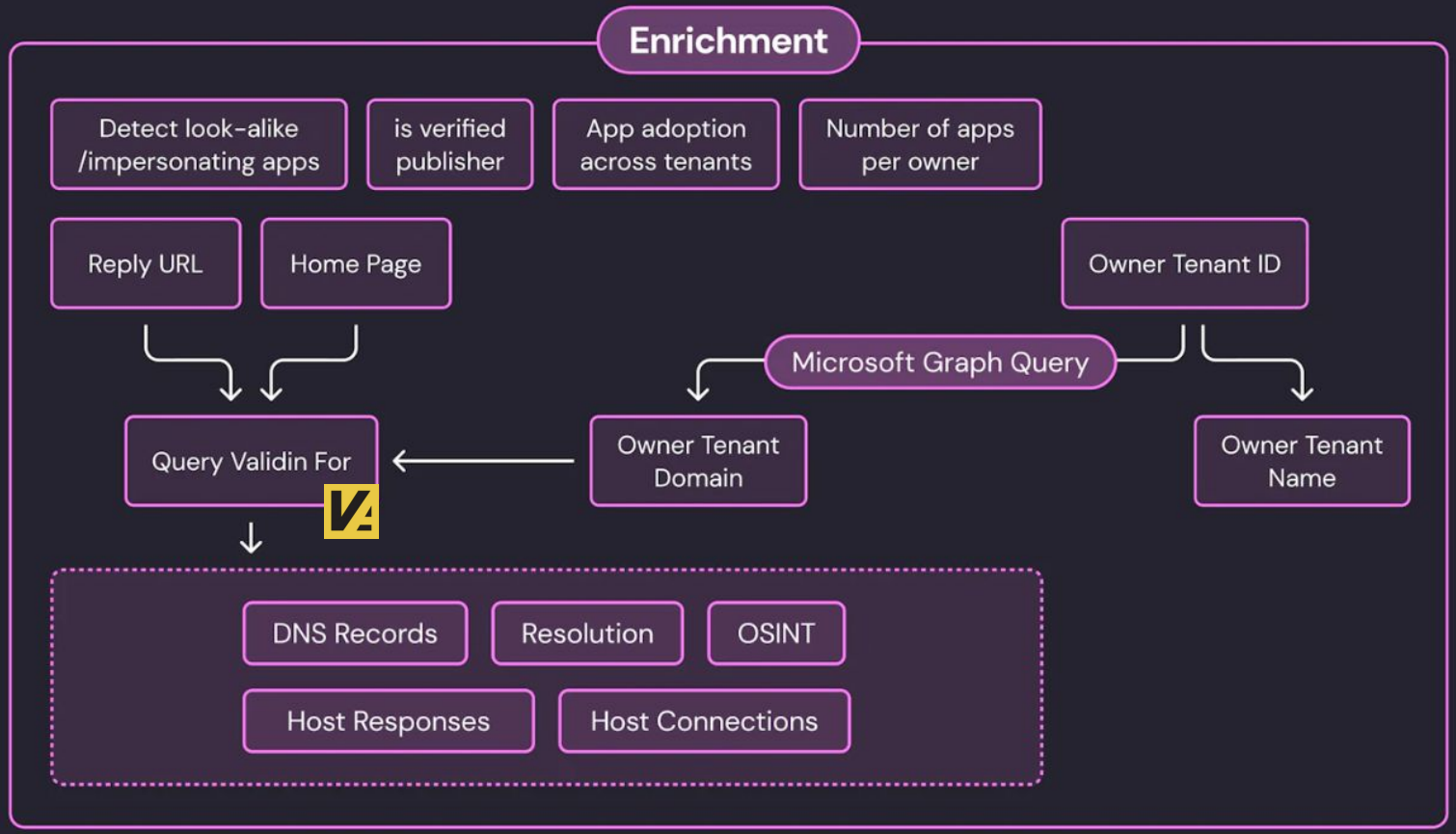



Extraction
Ingest 3-rd Party Apps
Extract Common App Names
Filter Out Common Apps
Extract Relevant Proporties
Home Page
Verified Publisher
Owner Tenant ID
Number of Apps Per Owner
App Daoption Across Tenants
App Name
Reply URL


Enrichment
Detect look-alike /impersonating apps
is verified publisher
App adoption across tenants
Number of apps per owner
Reply URL
Home Page
Owner Tenant ID
Microsoft Graph Query
Query Validin For
Owner Tenant Domain
Owner Tenant Name
DNS Records
Resolution
OSINT
Host Responses
Host Connections

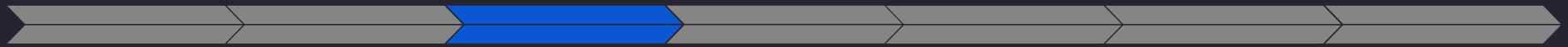
Owner tenant context – Graph API

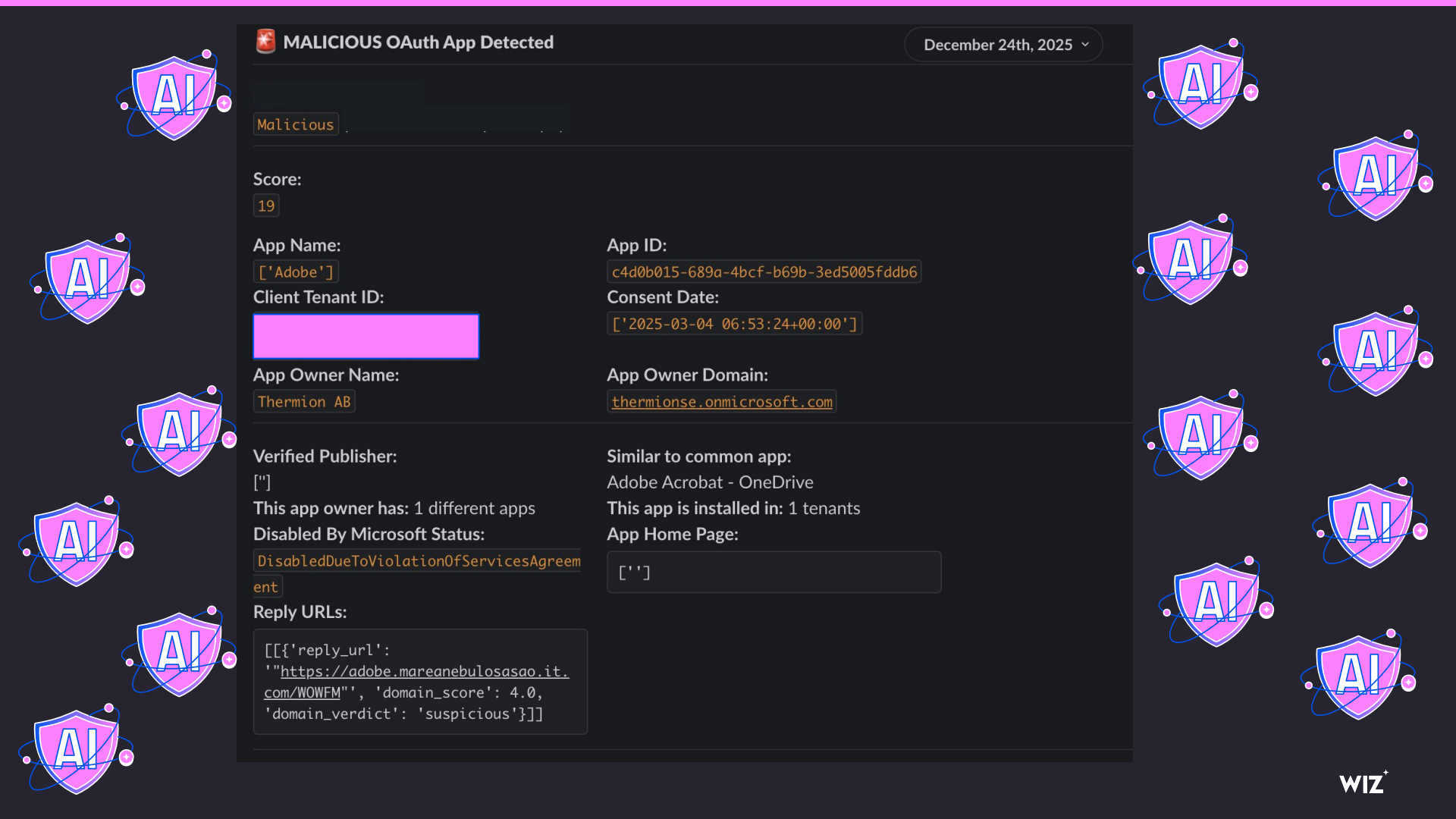



Enrichment
Detect look-alike /impersonating apps
is verified publisher
App adoption across tenants
Number of apps per owner
Reply URL
Home Page
Owner Tenant ID
Microsoft Graph Query
Query Validin For
Owner Tenant Domain
Owner Tenant Name
DNS Records
Resolution
OSINT
Host Responses
Host Connections

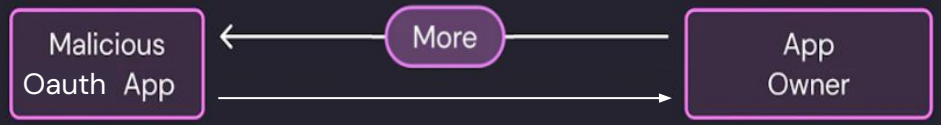
#3 Decision

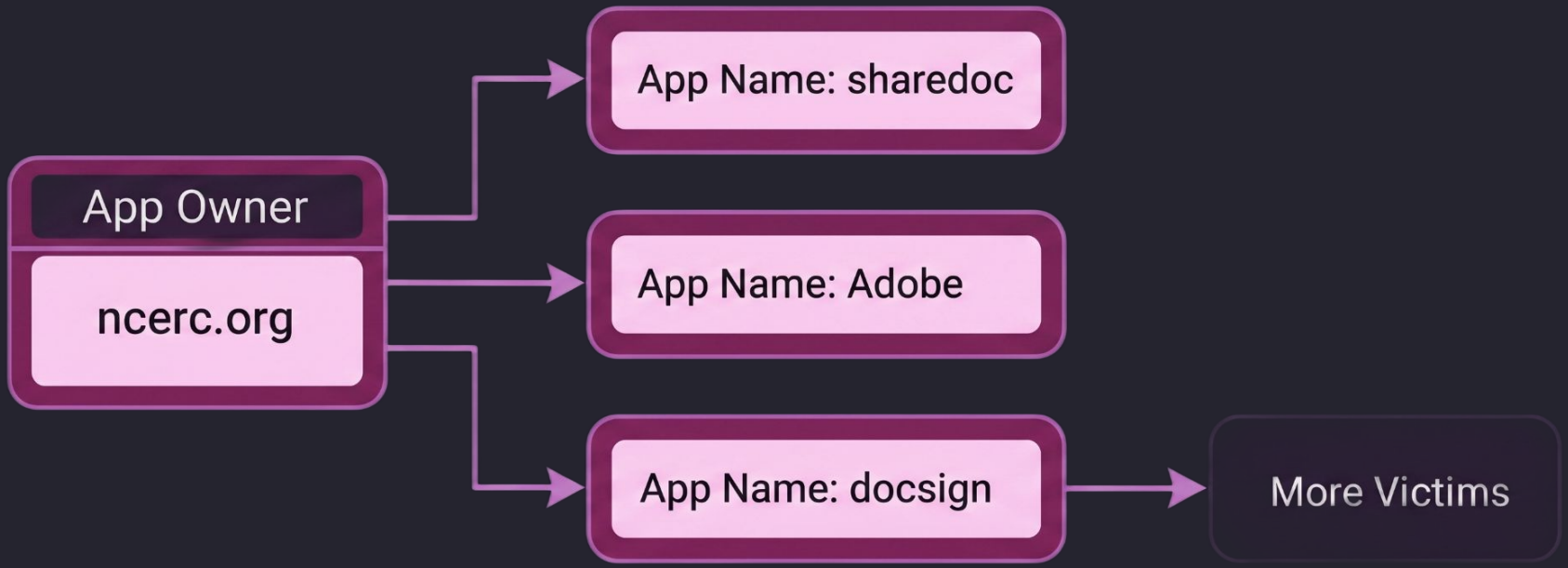
- Weighted scoring
- No single magic indicator
- Reduce noise




MALICIOUS OAuth App Detected
December 24th, 2025
Malicious
Score:
19
App Name:
['Adobe']
App ID:
c4d0b015-689a-4bcf-b69b-3ed5005fddb6
Client Tenant ID:
Consent Date:
['2025-03-04 06:53:24+00:00']
App Owner Name:
Thermion AB
App Owner Domain:
thermionse.onmicrosoft.com
Verified Publisher:
['']
Similar to common app:
Adobe Acrobat - OneDrive
This app owner has: 1 different apps
This app is installed in: 1 tenants
Disabled By Microsoft Status:
DisabledDueToViolationOfServicesAgreement
App Home Page:
['']
Reply URLs:
[[{'reply_url': '"https://adobe.mareanebulosasao.it.com/WOWFM"', 'domain_score': 4.0, 'domain_verdict': 'suspicious'}]]

Pivoting




App Owner
ncerc.org
App Name: sharedoc
App Name: Adobe
App Name: docsign
More Victims

Detections

User Granted Consent To Malicious Application

User Authenticated To Malicious Application

Results

Campaign evidence

19 distinct OAuth apps in the early-2025 campaign

7 additional legacy malicious apps dating back to 201

Shared infrastructure:

Examples from the IOCs:

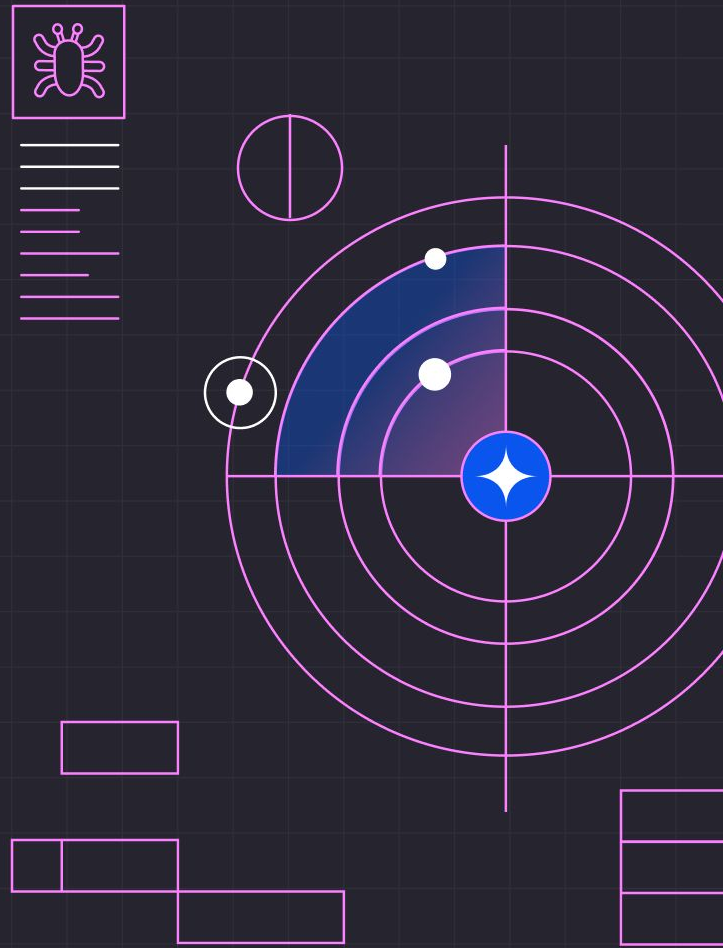
- Same owner domain - ncerc.org
- Shared owner tenant

Name	App ID	Owner ID	Owner domain	Reply URIs
DocuSign	a3903ccd-ec81-4264-8f6a-a7d4cd395fd5	e297c7b7-297d-4261-a849-e11e0f2bb10f	cooltekinc.com; cooltekllc.com; cooltekllc.onmicrosoft.com	["https://myworkspacefea7ffc776.myclickfunnels.com/httpsoutlookofficecom"]
Adobe	c52517b0-46eb-4d61-975a-771d9978dac0	a205f03e-e6ab-412e-a1f9-360f848b3705	anchorsgordon.com; anchorsgordon.onmicrosoft.com	["https://kimharrysteamworkspace.myclickfunnels.com/sharedfil"]
adobe	b0d8ea55-bc29-436c-9f8b-f8829030261d	0648fcb2-de2a-4a11-bd97-872c9b1a452b	damiongosamemorialfo.onmicrosoft.com; dgm-f.org	["https://workspacesteamworkspace.myclickfunnels.com/offices--af295"]
Users	21f81c9e-475d-4c26-9308-1de74a286f73	69168d16-9597-47a2-a4eb-a81900185529	fpwd.com; netorgft8261298.onmicrosoft.com	["https://myworksspace.myclickfunnels.com/office365com--5b652"]
sharedoc	48cb1fac-7195-47b3-98b2-fe3562bee75c	619849e9-5192-4c3f-b0f3-8469980c3958	nceconomicresourcecouncil.onmicrosoft.com; ncerc.org	["https://nmcunhasteamworkspace.myclickfunnels.com/secured-sharepoint-document"]

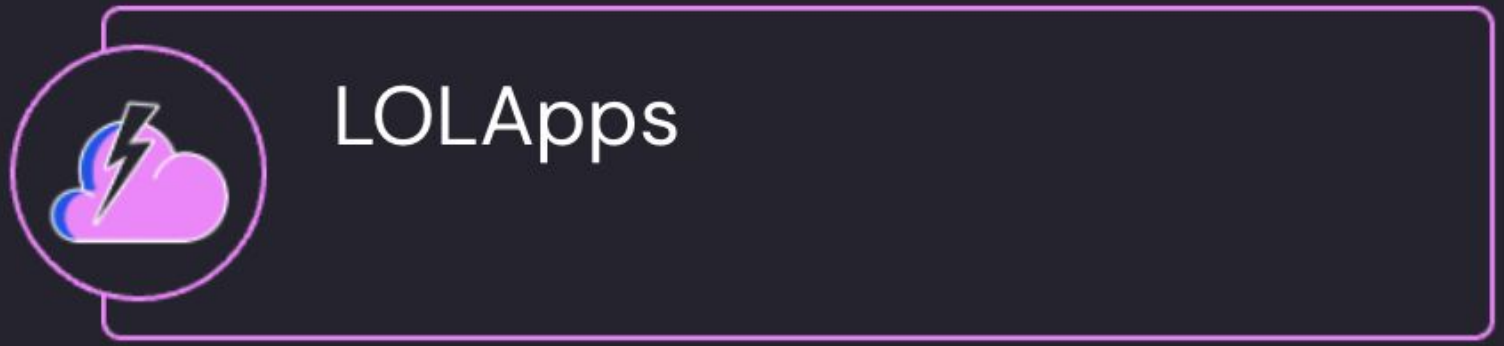
2019 vs 2025

Feature	2019	2019	2025
App Name	SharePoint Cloud	O365 Access	DocuSign
Target Brand	Microsoft	Microsoft	Third-Party (DocuSign/Adobe)
Reply URL	sharepoint.microzoftonline.com	officemtr.com:8081/office	ynapaletsteamworkspace.myclickfunnels.co
Stealth Level	Moderate (Visual)	Low	High (Contextual)

Sharing IOCs it’s important!

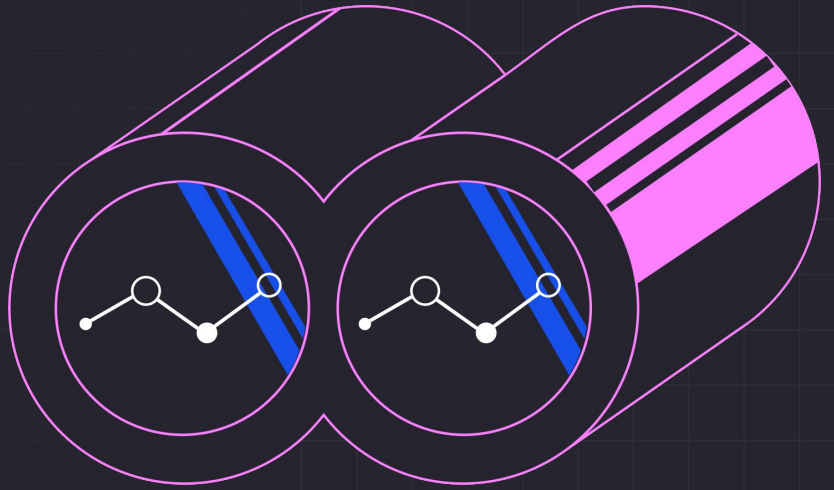


What's Next?



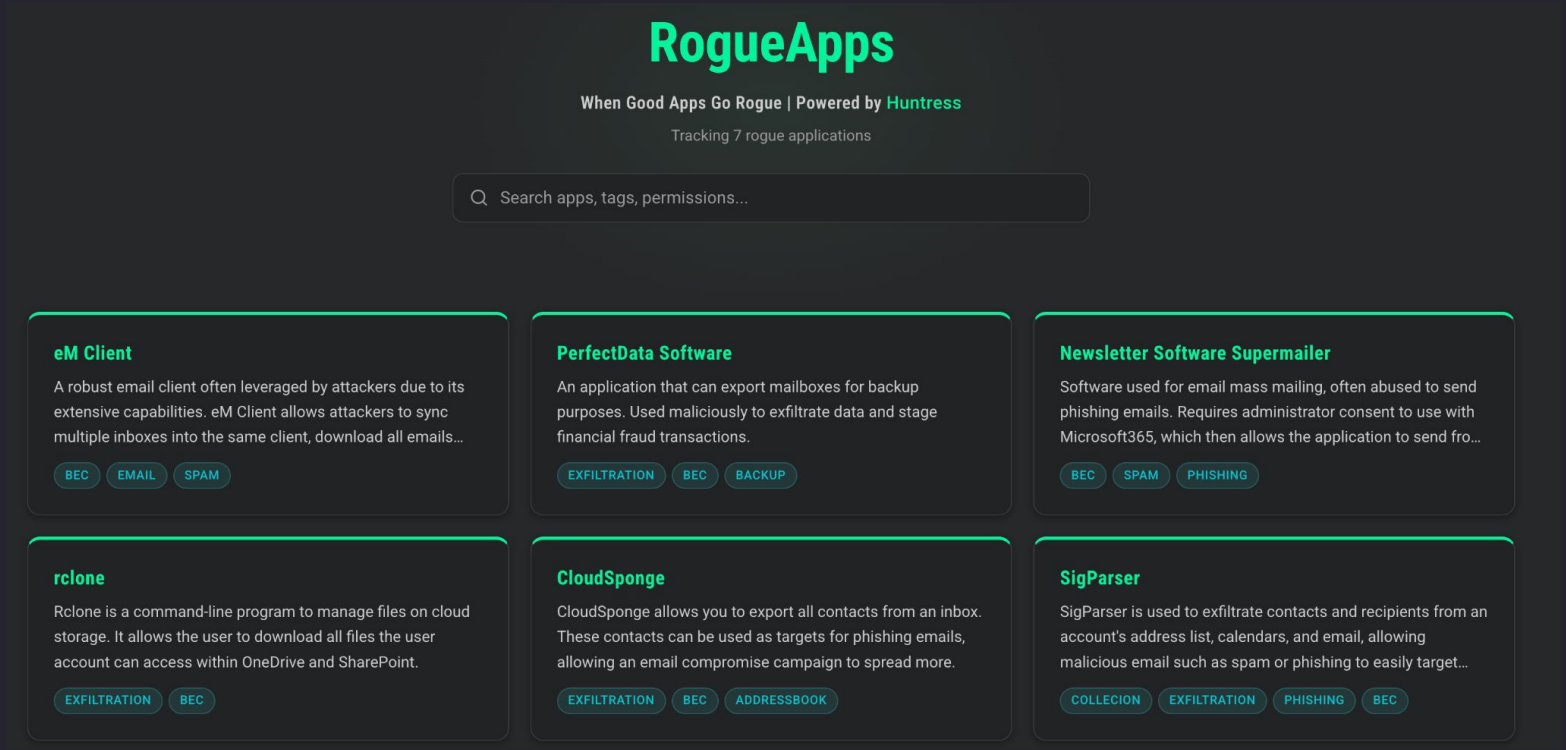
WIZ Research

LOLApps

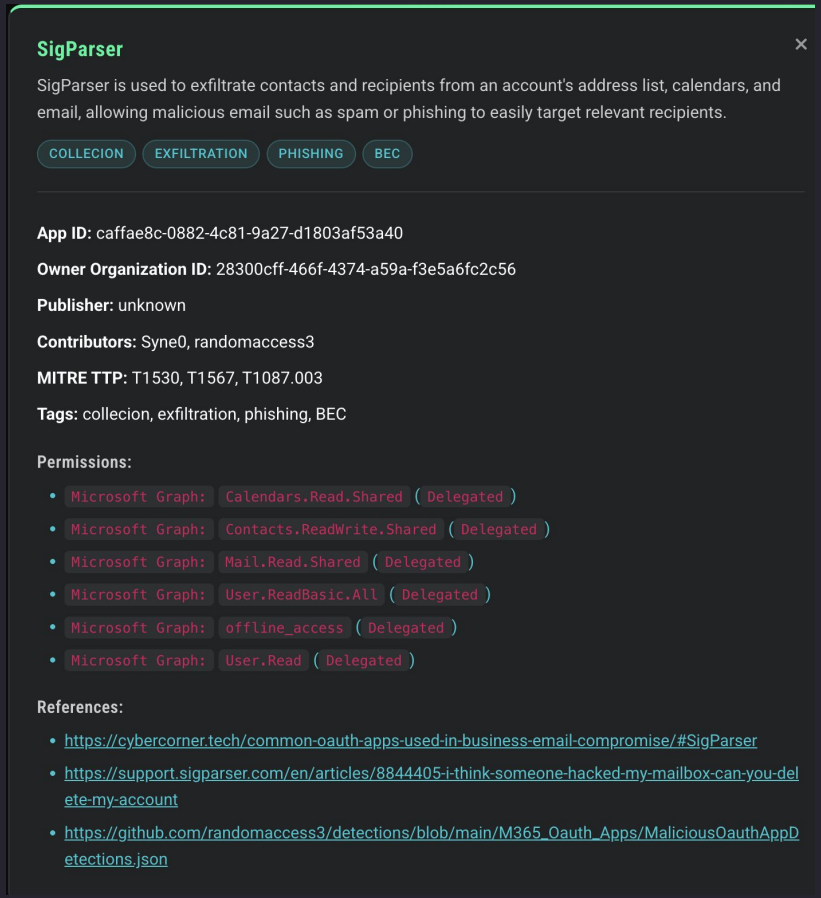


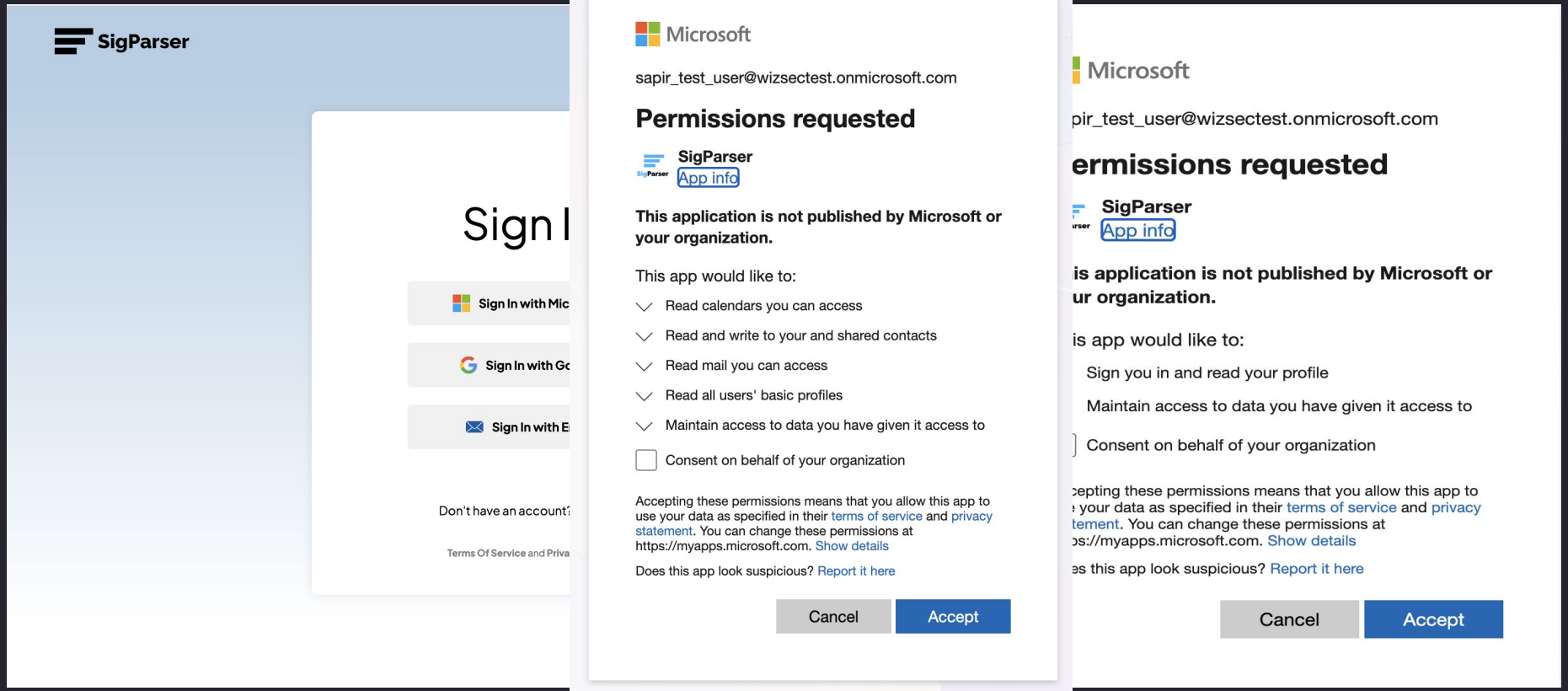
Abuse common app

Huntress: https://huntresslabs.github.io/rogueapps/



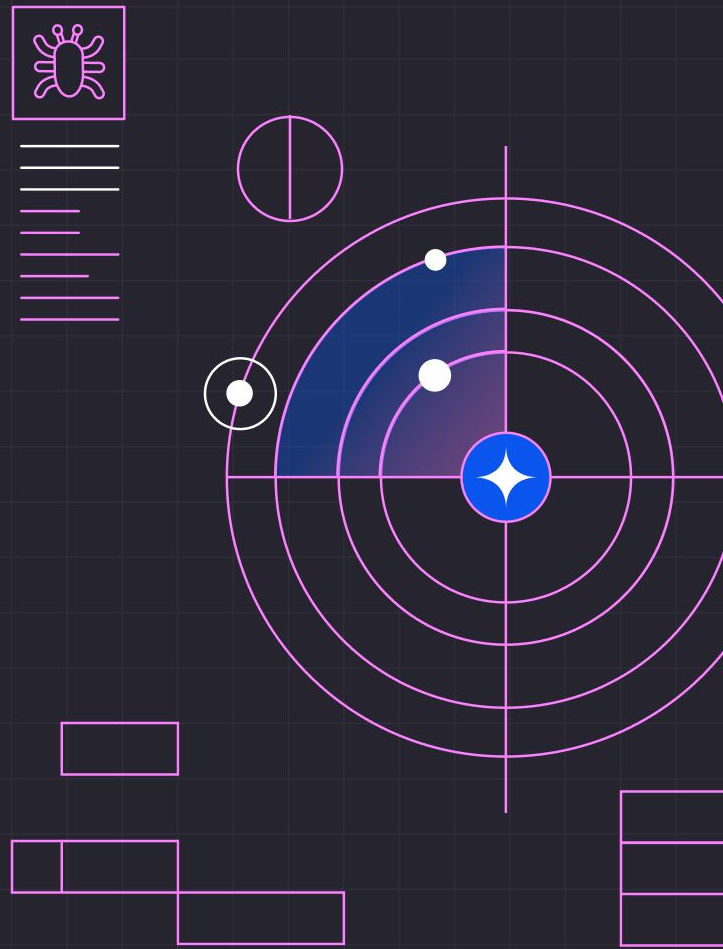
SigParser


SigParser
SigParser is used to exfiltrate contacts and recipients from an account's address list, calendars, and email, allowing malicious email such as spam or phishing to easily target relevant recipients.
COLLECION
EXFILTRATION
PHISHING
BEC
App ID: caffae8c-0882-4c81-9a27-d1803af53a40
Owner Organization ID: 28300cff-466f-4374-a59a-f3e5a6fc2c56
Publisher: unknown
Contributors: Syne0, randomaccess3
MITRE TTP: T1530, T1567, T1087.003
Tags: collecion, exfiltration, phishing, BEC
Permissions:
Microsoft Graph: Calendars.Read.Shared (Delegated)
Microsoft Graph: Contacts.ReadWrite.Shared (Delegated)
Microsoft Graph: Mail.Read.Shared (Delegated)
Microsoft Graph: User.ReadBasic.All (Delegated)
Microsoft Graph: offline_access (Delegated)
Microsoft Graph: User.Read (Delegated)
References:
https://cybercorner.tech/common-oauth-apps-used-in-business-email-compromise/#SigParser
https://support.sigparser.com/en/articles/8844405-i-think-someone-hacked-my-mailbox-can-you-delete-my-account
https://github.com/randomaccess3/detections/blob/main/M365_Oauth_Apps/MaliciousOauthAppDetections.json

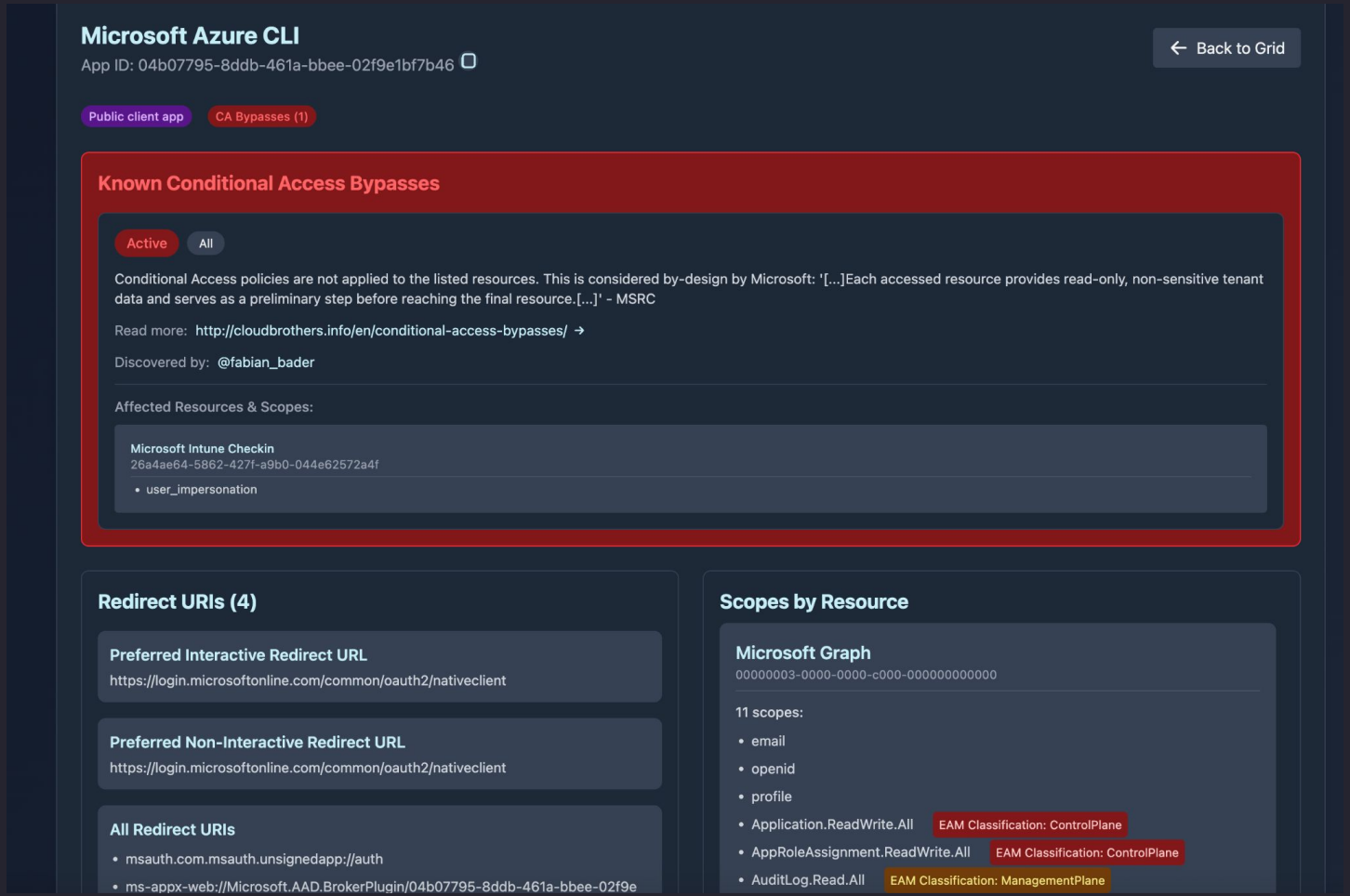

SigParser
Sign I
Sign In with Mic
Sign In with Go
Sign In with E
Don't have an account?
Terms Of Service and Priva
Microsoft
sapir_test_user@wizsectest.onmicrosoft.com
Permissions requested
SigParser
App info
This application is not published by Microsoft or your organization.
This app would like to:
Read calendars you can access
Read and write to your and shared contacts
Read mail you can access
Read all users' basic profiles
Maintain access to data you have given it access to
Consent on behalf of your organization
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
Does this app look suspicious? Report it here
Cancel
Accept
Microsoft
pir_test_user@wizsectest.onmicrosoft.com
ermissions requested
SigParser
App info
is application is not published by Microsoft or ur organization.
is app would like to:
Sign you in and read your profile
Maintain access to data you have given it access to
Consent on behalf of your organization
cepting these permissions means that you allow this app to your data as specified in their terms of service and privacy tement. You can change these permissions at os://myapps.microsoft.com. Show details
es this app look suspicious? Report it here
Cancel
Accept

LOLApps: Flavour #2

Microsoft First-Party Applications

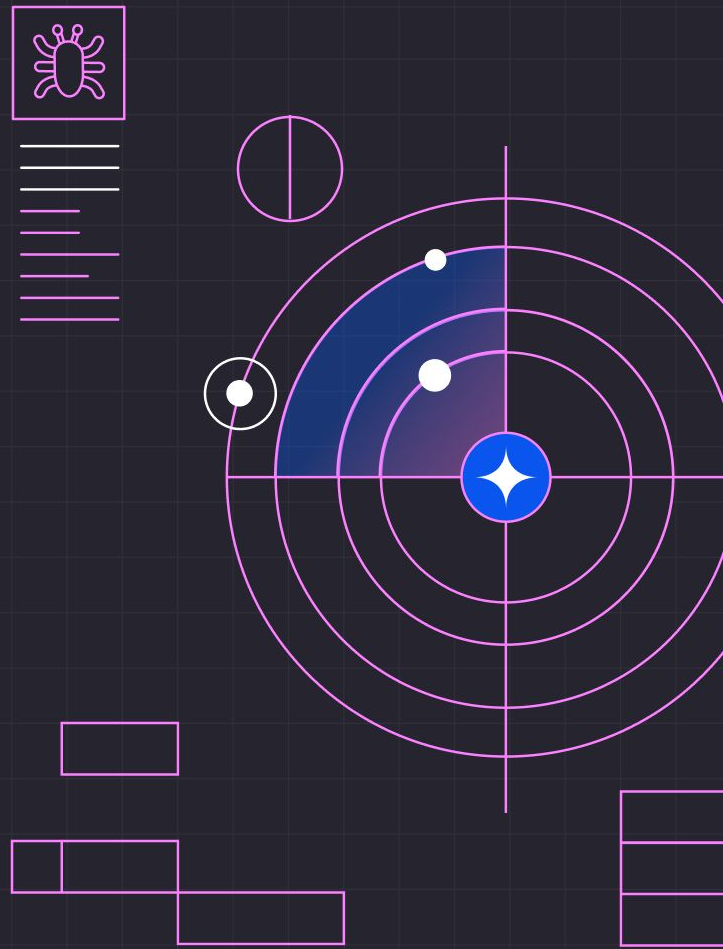


The Real LOLApps

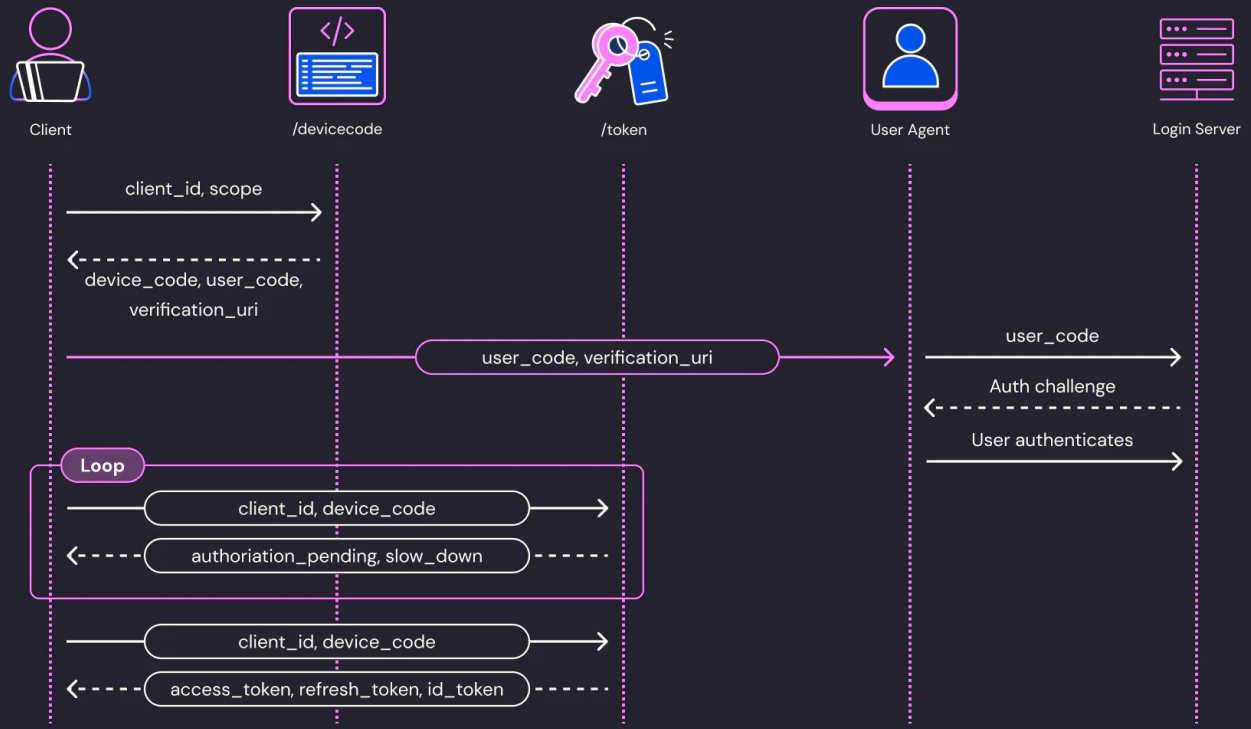


The Tactical Shift

Stolen Passwords -> Phishing

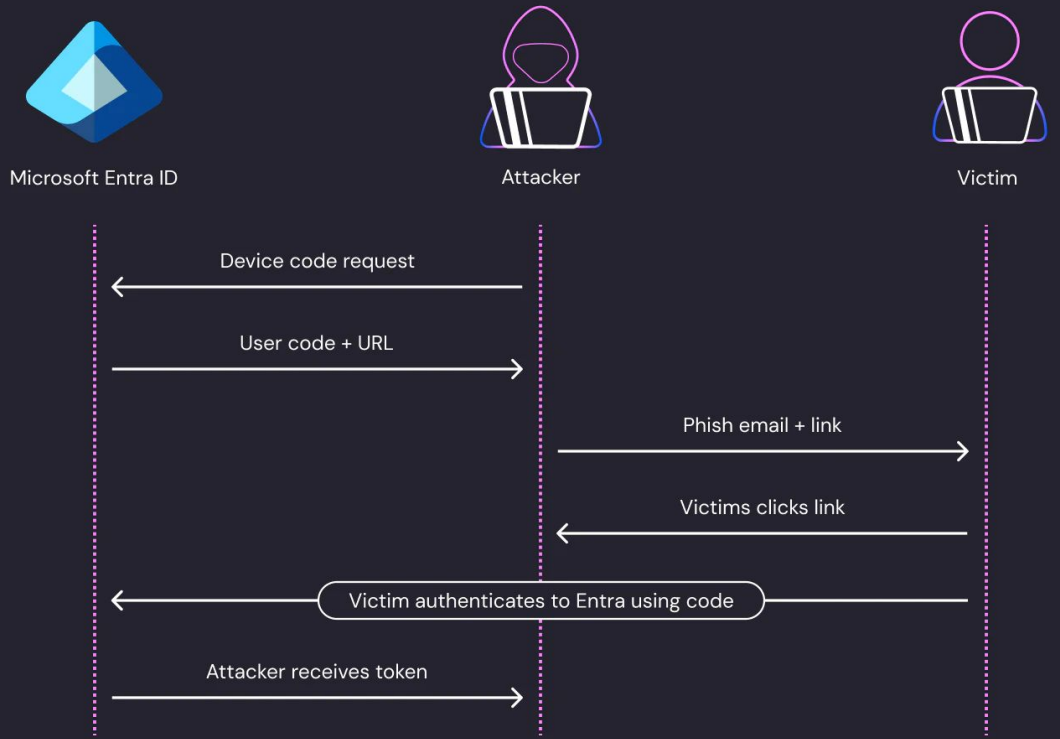


Device Code Flow



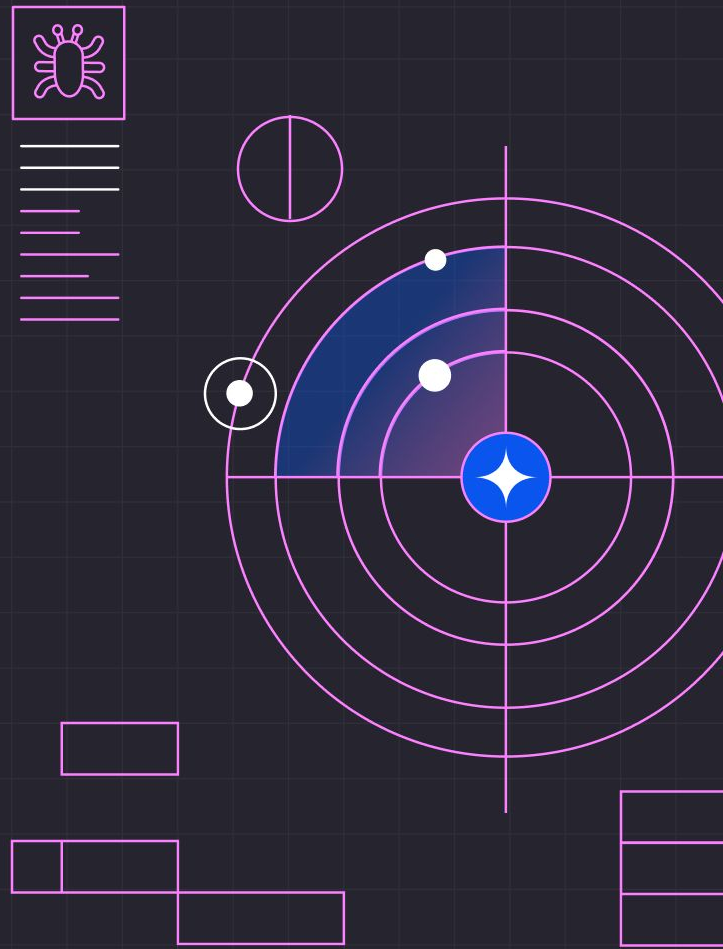
WIZ Research

Device code Phishing



WIZ Research

Detections



Questions You Should Ask Yourself

01

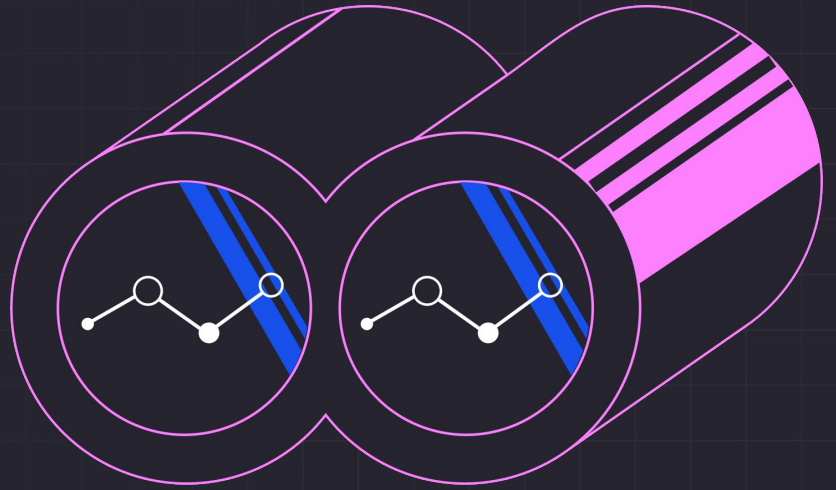
Is this app common in my organization?

02

Does the authentication to this app look suspicious?

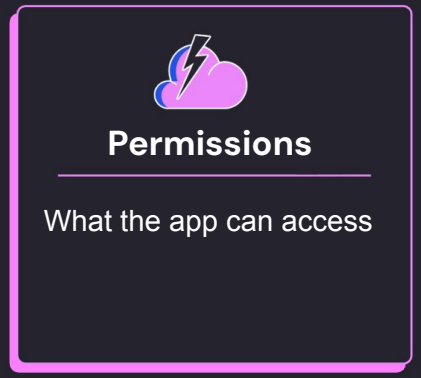
What's Next?

WIZ Research

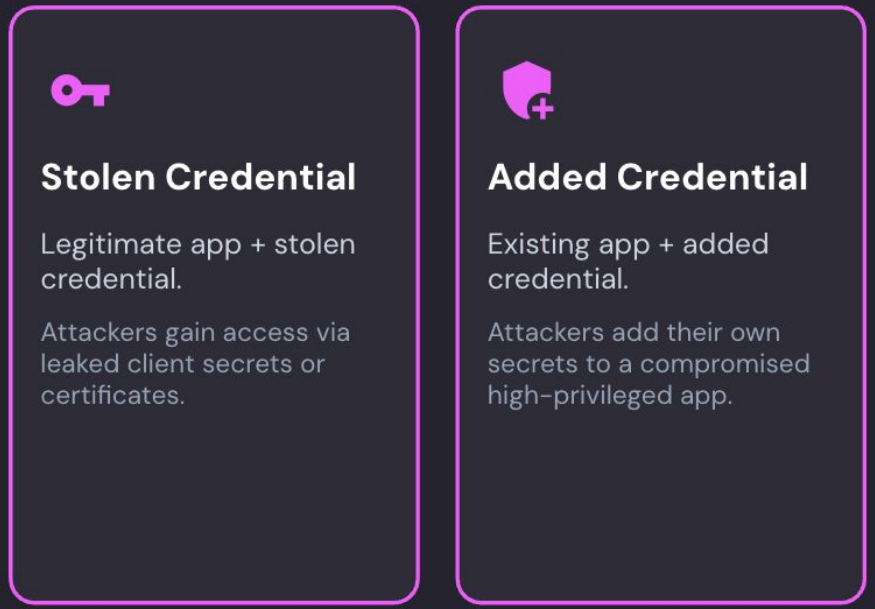


Permission and Credentials Abuse

Two sides of app access



Attack Patterns



Questions You Should Ask Yourself

Resources

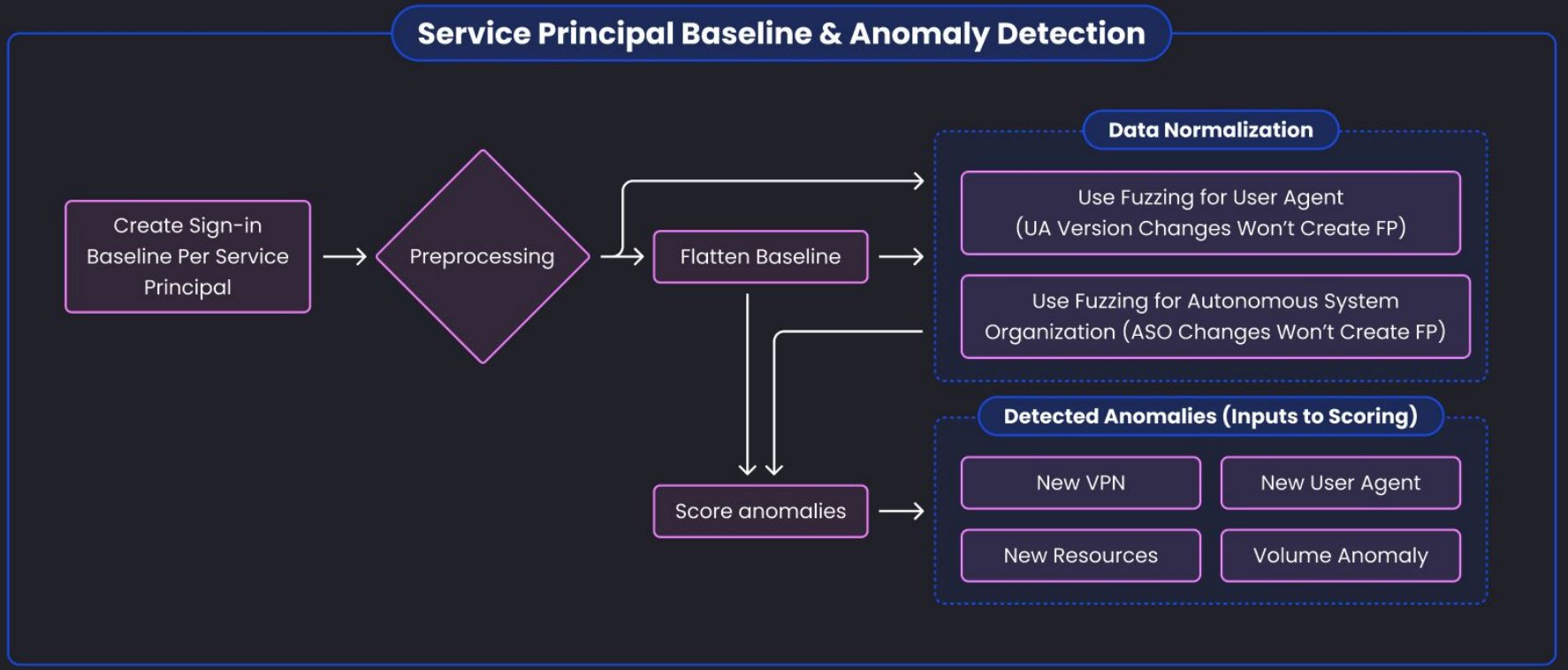
What does this app normally access?

Volume

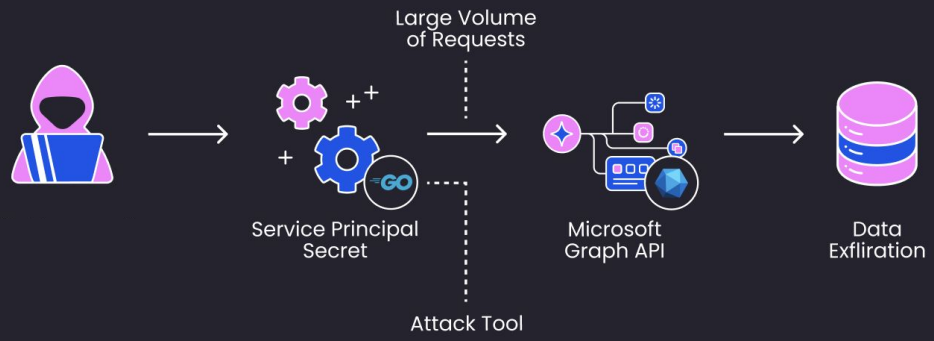
How broad is the activity of the app?

Execution context

How and from where is the app being used?


Service Principal Baseline & Anomaly Detection
Create Sign-in Baseline Per Service Principal
Preprocessing
Flatten Baseline
Score anomalies
Data Normalization
Use Fuzzing for User Agent (UA Version Changes Won't Create FP)
Use Fuzzing for Autonomous System Organization (ASO Changes Won't Create FP)
Detected Anomalies (Inputs to Scoring)
New VPN
New User Agent
New Resources
Volume Anomaly

Service Principal Anomalies – Findings



- New VPN
- New User Agent
- New Resources
- Volume Anomaly

WIZ Research

OAuth App Attack Path | OAuth Apps 101 | Malicious Apps | LOLApps | Permissions Abuse | Why is it hard? | Supply chain

Service Principal Anomalies – False Positives

Security products

Automated scans and protection agents often trigger false positive anomaly alerts during routine operations.

Debugging

Development activity and troubleshooting sessions can mimic suspicious behavior patterns.

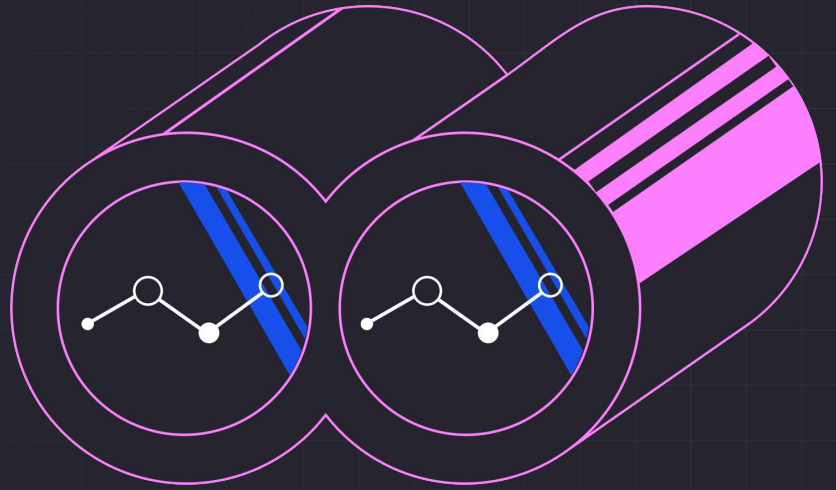
No baseline

Newly created principals or infrequent tasks lack historical data to establish "normal" behavior.

What's Next?

OAuth-based supply chain attacks

WIZ Research



Supply Chain

Supply Chain

Why is it hard?

Supply chain

Permissions abuse

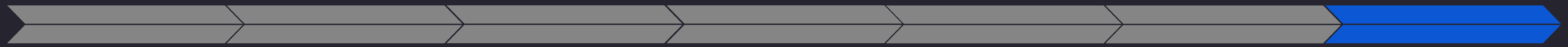
Supply Chain – TeamPCP Azure Collector

```
def _token_from_cli_cach
    cache_file = os.path
    if not os.path.exist
        return None
```

```
def _token_from_imds(resource):
    url = (
        "http://169.254.169.254/metadata/identity/oauth2/token"
```

```
def _collect_env_vars():
    keys = [
        "AZURE_CLIENT_ID", "AZURE_CLIENT_SECRET", "AZURE_TENANT_ID",
        "AZURE_CLIENT_CERTIFICATE_PATH", "AZURE_SUBSCRIPTION_ID",
    ]
    return {k: v for k in keys if (v := os.environ.get(k))}
```

Who is going to be next?



OAuth App Attack Path | OAuth Apps 101 | Malicious Apps | LOLApps | Permissions Abuse | Why is it hard? | Supply chain

Thank You for Listening!

- wiz.io/blog/tag/research
- threats.wiz.io
- https://www.wiz.io/blog/detecting-malicious-oauth-applications