



Azure Conditional Access Policies A World of Wonders

Paul Barbé / Matthieu Barjole

About us



Paul Barbé

Red teamer

@b-paul.bsky.social



Matthieu Barjole

Red teamer

@matthieub.bsky.social

Book your training! Azure intrusion for red teamers

Black Hat USA 2025 - Aug 2 / **Hexacon 2025** - Oct 6

Agenda



- **Conditional Access Policies**
- **Application discovery**
- **Statistics and bypass opportunities**

OAuth 2.0

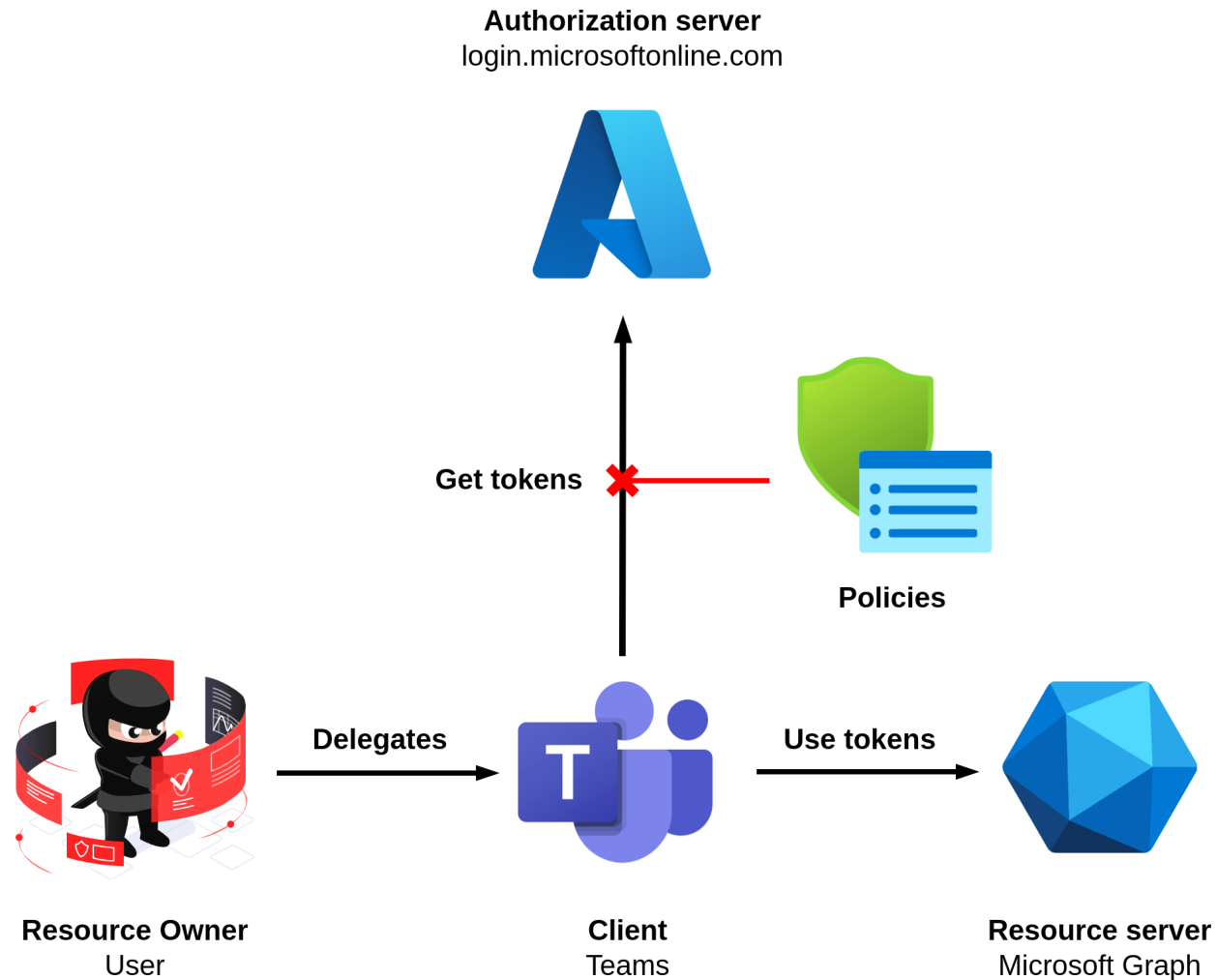
Microsoft applications



- **Everything is application** in Microsoft's world
 - Client, resource / API identified by GUIDs
 - Main API called **Microsoft Graph**
 - Entra ID + M365 services
 - 600+ scopes (`User.ReadWrite.All` , `Mail.Read`)
 - Other service-specific APIs
 - Exchange, SharePoint, Teams
 - Considered **first-party** (implicit consent)

Conditional Access Policies

Overview



Enforced by authorization server

- On **access token request** (any flow)
- Condition access with **context** (signals)



Identity



Location



Applications



Risk

Require **additional controls**



MFA



Password reset



Device compliant



Block

Conditional Access Policies

Application groups

- **Ease administration**

- Wraps multiple applications / scopes
- Often used to require MFA

- **If/else blackbox**

- Clients, resources, scopes?
- Which ones?

Select what this policy applies to

Resources (formerly cloud apps) ▼

Include

Exclude



None



All resources (formerly 'All cloud apps')



Select resources



Microsoft Admin Portals ⓘ



Office 365 ⓘ



Conditional Access Policies

Application groups

- **Office 365**

- Enforced on clients + resources
- Partially enforced on **Microsoft Graph**
 - **323/602 scopes** affected
 - **/.default** → blocked if affected scopes inside
 - **Native** OAuth scopes → gives all non-affected scopes
 - `email`, `profile`, `openid`, etc.



Office 365

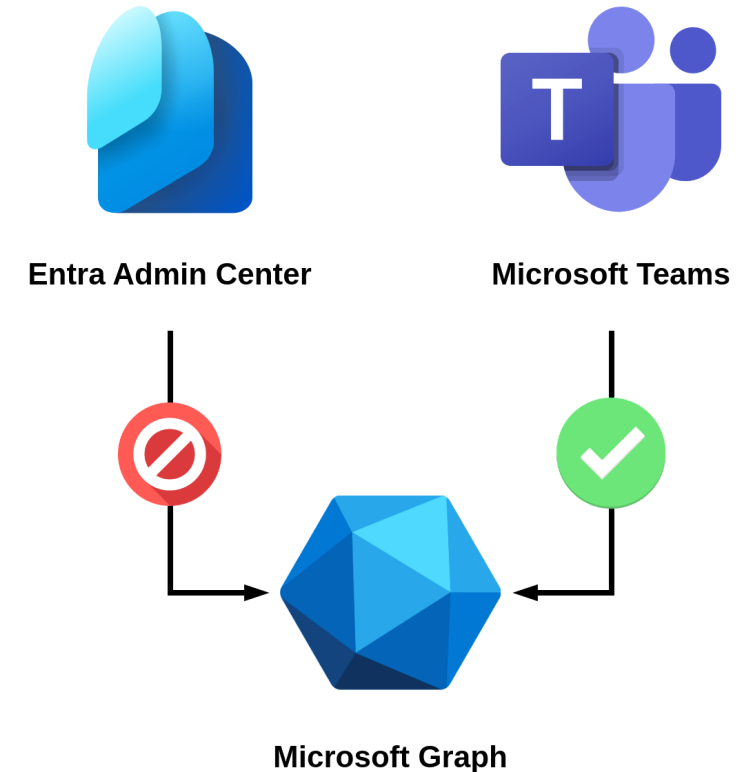
```
Calendars.Read  
Contacts.Read  
Files.Read  
Group.Read.All  
Mail.Read  
Notes.Create  
Team.ReadBasic.All  
TeamMember.Read.All  
[...]
```

Conditional Access Policies

Application groups

- **Microsoft Admin Portals**

- Enforced on clients + resources
- Not enforced on **Microsoft Graph** scopes
 - Common misunderstanding
 - Many benign apps with dangerous scopes
 - **Bypass opportunities**



Application discovery

Application discovery

Status

- **Microsoft (almost) does not document anything**
 - **First party** applications
 - **Scopes** on Microsoft Graph and service-specific APIs
 - **Memberships** in applications groups
 - Existing work ([ROADTools](#), [GraphPreConsentExplorer](#)) but no sources nor methodology
- **Objectives**
 - Provide discovery methodology and tooling
 - Find most legitimate applications providing bypass opportunities

Application discovery

GUIDS

■ Sources

- Existing work
- Audited environments (service principals, sign-in logs)
- SDKs
- Microsoft services enumeration (DNS/HTTP)

```
$ az ad sp create --id 'c44b4083-3bb0-49c1-b47d-974e53cbdf3c'  
{  
  "accountEnabled": true,  
  "appId": "c44b4083-3bb0-49c1-b47d-974e53cbdf3c",  
  "appOwnerOrganizationId": "f8cdef31-a31e-4b4a-93e4-5f571e91255a",  
  "displayName": "Azure Portal",  
  "replyUrls": [  
    "https://startups.portal.azure.com/auth/login/",  
  ]  
[...]
```

Application discovery

GUIDS

- **From audited environments:** service principals + sign-in logs

```
$ sqlite3 roadrecon.db 'select appOwnerTenantId,appId,appDisplayName from ServicePrincipals'
f8cdef31-a31e-4b4a-93e4-5f571e91255a|00000001-0000-0000-c000-000000000000|Azure ESTS Service
f8cdef31-a31e-4b4a-93e4-5f571e91255a|00000002-0000-0000-c000-000000000000|Windows Azure Active Directory
[...]
```

```
$ jq sign-in-interactive.json
{
  "appId": "1fec8e78-bce4-4aaf-ab1b-5451cc387264",
  "appDisplayName": "Microsoft Teams",
  "resourceId": "00000003-0000-0000-c000-000000000000",
  "resourceDisplayName": "Microsoft Graph",
  "appliedConditionalAccessPolicies": [
    {
      "displayName": "MFA for Office365",
      "result": "reportOnlyInterrupted",
      "conditionsSatisfied": "application,clientType",
      "includeRulesSatisfied": [
        {
          "conditionalAccessCondition": "application",
          "ruleSatisfied": "appId"
        }
      ]
    }
  ]
}
```

```
$ jq sign-in-noninteractive.json
{
  "appId": "1fec8e78-bce4-4aaf-ab1b-5451cc387264",
  "appDisplayName": "Microsoft Teams",
  "resourceId": "00000003-0000-0000-c000-000000000000",
  "resourceDisplayName": "Office 365 SharePoint Online",
  "scopes": [
    "Container.Selected",
    "MyFiles.Write",
    "Sites.FullControl.All",
    "Sites.Manage.All",
    "User.ReadWrite.All"
  ]
}
```

Application discovery

GUIDs

■ Results

- GUID list
- 20+ Microsoft tenants

```
$ wc -l first-party-applications.lst  
1887
```

```
$ cat microsoft-tenants.lst  
f8cdef31-a31e-4b4a-93e4-5f571e91255a Microsoft Services  
b4c546a4-7dac-46a6-a7dd-ed822a11efd3 Office 365  
72f988bf-86f1-41af-91ab-2d7cd011db47 Microsoft  
2132228a-d66e-401c-ab8a-a8ae31254a36 PIM SAFE PROD  
[...]
```

Application discovery

Tokens harvesting

- **Client-side and public authentication flows**

- Implicit flow
- Authorization code flow / PKCE (SPA)
- Password flow (ROPC)
- Device code

- **Refresh token flow**

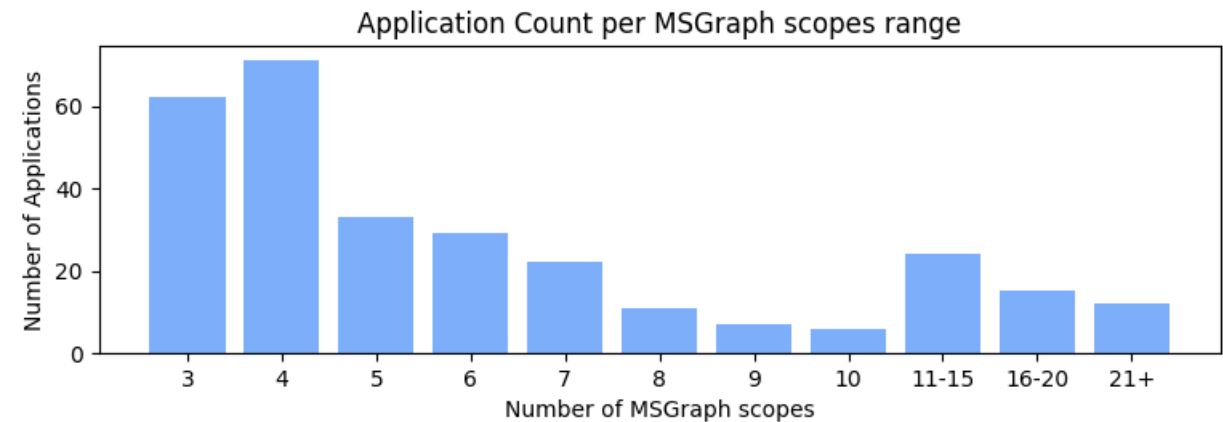
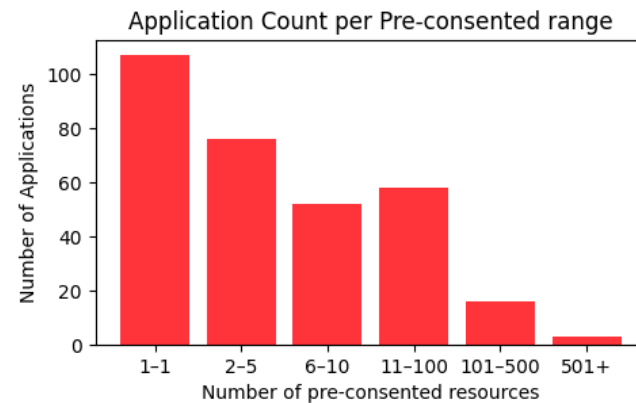
- FOIC & Brokers (wip)

Application discovery

Interesting results

- **10k authentications**
 - 336 clients to 1550 resources
- **MSGraph**: 306 clients
- **AADGraph**: 117 clients (EOL July 1st)

Client	Resources	Client	MSGraph scopes
Device Management Client	1524	Microsoft Office	39
Microsoft Authentication Broker	1510	Microsoft Outlook	26
Microsoft Azure PowerShell	683	One Outlook Web	26
Microsoft Azure CLI	477	OneNote	24
Microsoft Office	394	Microsoft Teams Admin Portal	24



Application discovery

Interesting results

- **2 first-party tenants**

- Microsoft Services

`f8cdef31-a31e-4b4a-93e4-5f571e91255a`

- Orgid Migrated Apps

`475130ab-62b5-4241-a9d3-47e37c9bc215`

- **Applications groups**

- **Microsoft Admin Portals:** 5 apps + broking
 - **Office 365:** 150 apps

- **Same scopes** but different groups

- `make.powerapps.com /`
`make.test.powerapps.com`

- `Application.ReadWrite.All`

Microsoft Graph

Scopes	Clients	0365	AdminPortals
Directory.AccessAsUser.All	7	2	0
Application.ReadWrite.All	13	1	0
Files.ReadWrite.All	28	N/A	0
Policy.ReadWrite.ConditionalAccess	1	0	0
User.ReadWrite.All	8	1	0

Alternative APIs

API	Scopes	Clients
ADlbizaUX	user_impersonation	7
Office 365 SharePoint Online	Multiple	68

Application discovery

Statistics

- Common usage from sign-in logs
 - Password spraying optimization

```
$ python3 application-usage.py
```

Use	Application ID	Application Name	Resource ID	Resource Name
---	-----	-----	-----	-----
20%	38aa3b87-[...]	Windows Sign In	00000002-[...]	Windows Azure Active Directory
18%	89bee1f7-[...]	Office365 Shell WCSS-Client	00000003-[...]	Microsoft Graph
9%	5e3ce6c0-[...]	Microsoft Teams Web Client	cc15fd57-[...]	Microsoft Teams Services
5%	00000002-[...]	Office 365 Exchange Online	00000002-[...]	Office 365 Exchange Online
4%	243c63a3-[...]	Office Online Core SSO	e03a13ee-[...]	Office Online Service
3%	08e18876-[...]	SharePoint Online Web Client	00000003-[...]	Microsoft Graph
3%	d3590ed6-[...]	Microsoft Office	00000002-[...]	Office 365 Exchange Online
3%	00000003-[...]	Office 365 SharePoint Online	00000003-[...]	Office 365 SharePoint Online
1%	1fec8e78-[...]	Microsoft Teams	cc15fd57-[...]	Microsoft Teams Services
1%	c0ab8ce9-[...]	M365ChatClient	fb8d773d-[...]	Enterprise Copilot Platform
1%	29d9ed98-[...]	Microsoft Authentication Brk	00000002-[...]	Windows Azure Active Directory
1%	4765445b-[...]	OfficeHome	4765445b-[...]	OfficeHome
1%	9199bf20-[...]	One Outlook Web	00000002-[...]	Office 365 Exchange Online
[...]				

Conclusion

Conclusion



■ **Misconception**

- Scope policies to identities, not apps
- Anyway, better set MFA for everyone, everywhere

■ **Black box**

- So many if/else it must be an AI
- Unexpected / undocumented behaviors

■ **Future work**

- **Consolidated results** soon on GitHub :)
- Third-party clients
- Native bypasses and exploitable APIs
(e.g. IntuneCP & device compliance from Dirk-Jan)

Thanks!



<https://www.linkedin.com/company/synacktiv>



<https://x.com/synacktiv>



<https://bsky.app/profile/synacktiv.com>



<https://synacktiv.com>