# Identity based attack paths in Azure and Azure AD

**Cody Burkard** 

Principal Security Architect cody@o3c.no | +47 482 77 939

**Identity Day Norway** 16.03.2023





### About me

- Cody Burkard
- Partner and Principal Consultant O3
   Cyber
- Security testing and cloud security architecture
- Security researcher Offensive primitives in Azure











Identity-centric attack primitives





### A brief introduction to attack paths

### What is an "attack path"?



### What is an "attack path"?



### Also an attack path...

### **Alternative attack path**



### **Azure AD technical background**

### **Azure Active Directory**

- Cloud-based directory services and IAM platform
- Microsoft Online Apps and Azure
- SSO to SaaS
- Custom integration via Identity Platform



### **How Azure AD Works**

- Organizations have a unique tenant
- Directory objects:
  - Users
  - Groups
  - Service Principals
  - Application Objects
  - Devices
- To manage a tenant you need an Azure AD Role assigned to your user

Home >						
Weboxo   Overview     Azure Active Directory						
*	🕂 Add 🗸 🗔 Ma	inage tenants [] What's new 🛛 📑 Preview feature	es 🛛 🗖 Got feedba	ick? 🗸		
i Overview						
Preview features	Microsoft Entra	Microsoft Entra has a simpler, integrated experience for managing all your Identity and Access Management needs. Try the new Microsoft Entra admin center!				
X Diagnose and solve problems	Overview Monito	Overview Monitoring Properties Recommendations Tutorials				
Manage						
🚨 Users	Search your tenant					
A Groups	Basic information					
External Identities						
2. Roles and administrators	Name	Weboxo	Users	4		
Administrative units	Tenant ID	d22295c2-ed7e-4662-9c6c-b7346f740f8b	Groups	1		
🚸 Delegated admin partners	Primary domain	Weboxo.onmicrosoft.com	Applications	4		
Enterprise applications	License	Azure AD Free	Devices	0		
Devices						
III. App registrations	Alerts					
Identity Governance	• • •					
Application proxy	Upcoming IPv6 deployment Organizations that use named locations in		Upcoming MFA Server deprecation Please migrate from MFA Server to Azure AD Multi-			
Custom security attributes (Preview)	Conditional action as so impact.	Access or Identity Protection must take on as possible to avoid any service	Factor Authentication by September 2024 to avoid any service impact.			
Licenses	Learn more 🖸		Learn more 🖸			
Cross-tenant synchronization						

#### **Azure AD in Azure Portal**

### How Azure AD Works - Roles

- Azure AD Roles contain permissions to modify objects in the Microsoft Online ecosystem.
- Administration of Azure AD and M365 with limited permissions
- Principle of least privilege
  - Limit Global Admins

Microsoft Azure		D 🛱 🗘 🏟 🕐	A dwriter@weboxo.or weboxo (weboxo.onmi	imic cros
ome > Weboxo   Roles and administra	tors >			
Roles and administr	ators   All roles			>
*	🕂 New custom role  🗊 Delete custom role 🞍 Download assi	nments 🜔 Refresh 🛛 🖾 Preview features 📄 🞘 Got feedback?		
All roles				
Diagnose and solve problems	Io create custom roles, your organization needs Azure AD Premium	1 or P2. Start a free trial. →		
ctivity	(i) Your Role: Global Reader			
Access reviews	Administrative roles			
Audit logs	Administrative roles are used for granting access for privileged actions access to manage other parts of Azure AD not related to application c	in Azure AD. We recommend using these built-in roles for delegating access to manage broad application configuratio infiguration. Learn more.	n permissions without grantin	g
Bulk operation results	Learn more about Azure AD role-based access control			
oubleshooting + Support				
New support request	Search by name or description Add filters			
ren support request	Role	↑↓ Description	Туре ↑↓	·
	Application Administrator	Can create and manage all aspects of app registrations and enterprise apps.	Built-in	
	Application Developer	Can create application registrations independent of the 'Users can register applications' setting.	Built-in	
	🗌 🍰 Attack Payload Author	Can create attack payloads that an administrator can initiate later.	Built-in	
	Attack Simulation Administrator	Can create and manage all aspects of attack simulation campaigns.	Built-in	
	Attribute Assignment Administrator	Assign custom security attribute keys and values to supported Azure AD objects.	Built-in	
	📃 🍰 Attribute Assignment Reader	Read custom security attribute keys and values for supported Azure AD objects.	Built-in	
	📃 🍰 Attribute Definition Administrator	Define and manage the definition of custom security attributes.	Built-in	
	🗌 🍰 Attribute Definition Reader	Read the definition of custom security attributes.	Built-in	
	Authentication Administrator	Can access to view, set and reset authentication method information for any non-admin user.	Built-in	
	Authentication Extensibility Administrator	Customize sign in and sign up experiences for users by creating and managing custom authentication extensions.	Built-in	
	Authentication Policy Administrator	Can create and manage the authentication methods policy, tenant-wide MFA settings, password protection policy, and verifiable credentials.	Built-in	
	Azure AD Joined Device Local Administrator	Users assigned to this role are added to the local administrators group on Azure AD-joined devices.	Built-in	
	🗌 🍰 Azure DevOps Administrator	Can manage Azure DevOps organization policy and settings.	Built-in	

**Azure AD Roles** 

### **Under the hood**

What happens when you click save?

POST https://graph.microsoft.com/v1.0/groups

■ Microsoft Azure	$\mathcal P$ Search resources, services, and docs (G+/)
Home > Weboxo   Groups > Groups   All groups >	
New Group	
Sot feedback?	
Group type * 🛈	
Security	$\checkmark$
Group name * ①	
newGroup	✓
Group description ①	
Enter a description for the group	
Membership type ①	
Assigned	$\sim$
Owners	
No owners selected	
Members	
No members selected	
· · · · · · · · · · · · · · · · · · ·	
Croat	

### **Azure AD management APIs**

### Create Group, update group, add user to group...



### **Azure AD Auth – User Access**



### What about machine to API?

- Directory Automation?
- Reading directory objects from apps?
- Updating objects such as Groups from a SaaS app?
- Requires a service principle



#### Service Principle Permissions

### **Azure AD Auth – Service Principles**



### **How Azure AD Works**

### In summary

- *Most* management requests now use *https://graph.microsoft.com* APIs
- To modify the directory, must authenticate to MS Graph APIs using some directory object
- Two authorization mechanisms that allows you to modify directory objects
  - Azure AD roles
  - Application permissions with service principals

### How can you abuse Azure AD?

### Initial Access - attacks

- Illicit Consent Grant Attacks?
- Password Spraying?
- Credential Stuffing?
- General password brute forcing?
- Traditional phishing tactics fake login page?
- Steal the tokens from browsers of victims (after initial compromise)?
- Dump and steal Primary Refresh Tokens (after initial compromise)?
- Leaked Service Principal Secret?

### How can you abuse Azure AD?

s?

### Initial Access - Attacks

- Illicit Consent Gr
- Password Sprayn.
- Credential Stuffing?
- General password b
- Traditional phis
- Steal the tokens fr . . owsers of vicu

## Not what this presentation is about

fter initial compromise)?

• Dump and steal Primary Refresh Tokens (after initial compromise)?

rake

• Leaked Service Principal Secret?

### **Azure AD attack primitives**

The basis of attack path analysis

### What is an "attack primitive"?



### **Attack Primitives – definition**

"A configuration state that may be abusable under certain conditions, but that is not a vulnerability"

### **Attack Primitives – definition**

- Allows the attacker to "change state" in one way or another
  - Privilege Escalation
  - Lateral Movement
  - Abuse technique
- Building blocks of an attack path

## **Speed Round**

### **Basic primitives**

### Abuse Azure AD Administrative Roles:

Azure AD Role	Primitive
Application Administrator	Assume Privileges of any Service Principle
Privileged Auth Administrator	Assign new Global Administrators
Groups Administrator	Assign self to privileged group
Hybrid Identity Administrator	Assign self as Owner to Application

### Abuse object ownership:

Object Ownership	Primitive
Application Object	Assume Privileges of the Application (multi tenant)
Service Principal	Assume Privileges of the Service Principle (single tenant)
Group	Assign self to group

## **Basic primitives - Applications**

Abuse Application Objects and Service Principals:

Graph Permission	Primitive
Application.ReadWrite.All	Assume Privileges of any Service Principle
DirectoryRole.ReadWrite.All	Assign new Global Administrators
Group.ReadWrite.All	Assign self to privileged group



### **Password reset primitives**

### Who can reset who's password?



Role that password can be reset	Password Admin	Helpdesk Admin	Auth Admin	User Admin	Privileged Auth Admin	Global Admin
Auth Admin			~		~	<b>v</b>
Directory Readers	1	~	~	~	~	<b>v</b>
Global Admin					~	✓*
Groups Admin				~	~	<b>v</b>
Guest Inviter	~	~	~	~	~	<b>v</b>
Helpdesk Admin		~		~	~	<b>v</b>
Message Center Reader		~	<ul> <li>✓</li> </ul>	~	✓	<b>v</b>
Password Admin	~	~	<ul> <li>✓</li> </ul>	~	~	<b>v</b>
Privileged Auth Admin					~	<b>v</b>
Privileged Role Admin					~	<b>v</b>
Reports Reader		~	~	~	~	<b>v</b>
User (no admin role)	~	~	~	<b>v</b>	✓	~
User (no admin role, but member or owner of a role-assignable group)					1	~
User Admin				~	~	✓
Usage Summary Reports Reader		~	~	~	~	<b>v</b>
All custom roles	<b>v</b>	~	~	~	~	~

https://learn.microsoft.com/en-us/azure/activedirectory/roles/permissions-reference#who-can-resetpasswords

## **ABAC primitives**

- Attribute-based access control new attack surface!
- Who controls the attribute?
  - Dynamic Group Abuse
  - Azure ABAC abuse
    - coming soon



Invite admin@o3c.no.maliciousdomain.com

## Data Plane "Bouncing"

- Secrets in Plaintext
- Cloud Shell Abuse
- Key Vault Secrets
- Automation Account Abuse
- Logic App Abuse
- Managed Identity Abuse



## **Application-level primitives**

- Abuse admin portals on SaaS apps
- Abuse application OAuth vulnerabilities
  - Poor validation of tokens
  - Improper validation of scope or roles
- Capture auth codes from Oauth Clients
  - Open Redirects
  - Subdomain takeover of redirectUrl domain

## **Other interesting primitives**

- Self-service signup flow in Azure AD
- Combine with traditional on-premise AD attack paths
  - Global admin in Azure may be a normal user on prem
- Bypass PIM with refresh tokens

## **Putting them together**

### Azure AD Attack Paths – example 1



### Azure AD Attack Paths – example 2



## **Closing Thoughts**

- Just because a primitive exists in your infra doesnt mean there is a security issue
- «IAM hygiene» does help to eliminate *unnecessary* attack paths
- «IAM hygiene» will not prevent attack paths from being introduced
  This is an entirely different topic
- Attack path analysis or testing may be worth including in IAM routines
- Research may yield interesting results in your unique setups



## 03C.N0

