

## **Hacking Azure AD Identities**

@DrAzureAD

https://linkedin.com/in/nestori



### Dr Nestori Syynimaa Senior Principal Security Researcher Secureworks® CTU™ *Twitter/Mastodon:*

@DrAzureAD@infosec.exchange



MICROSOFT MOST VALUABLE Security Researcher ESTD. 2022

VOLUME

@DrAzureAD

#### **AADInternals**

- Admin & hacking toolkit for Azure AD & Microsoft 365
- Open source:
  - https://github.com/gerenios/aadinternals
  - https://aadinternals.com/aadinternals
- MITRE ATT&CK
  - https://attack.mitre.org/software/S0677/

Groups That Use	This Soft	ware

ID	Name	References
G0016	APT29	[5]



#### Contents

- How does the cloud work?
- Introduction to identities
- Attack scenarios
- Demos





# How does the cloud work

## How does the cloud work? 1/2



Secureworks

Source: Secureworks

## How does the cloud work? 2/2

- Identity provider (Azure AD)
  - Knows about the client & user what is told to it (proof-ofidentity!)
- Service provider (Azure AD, Azure, M365, etc.)
  - Trusts identity provider
  - Only does what client tells it to do
  - Knows about the client & user what identity provider tells it (claims in bearer token)



## Introduction to identities

## Introduction to identities



Source: Secureworks

#### **OAuth terminology**

- Identity provider (Azure AD)
  - Authorization Server
- Service provider (Azure AD, Azure, M365, etc.)
  - Resource Server
- User (member, guest)
  - Resource Owner
- Application
  - OAuth Client

#### **OAuth 2.0 authorization flow**



Cobb, Ryan, Larcher-Gore, Anthony, & Syynimaa, Nestori. (2022). Family Matters: Abusing Family Refresh Tokens to gain Unauthorised Access To Microsoft Cloud Services - Exploratory Study of Azure Active Directory Family of Client IDs. Paper presented at the ICEIS - 24th International Conference on Enterprise Information Systems.

#### **Azure AD Token types**

Token	Standard	Purpose	Lifetime
id_token	OpenID Connect	User identification	1 h
access_token	OAuth2	User (identification and) authorization	1 h
refresh_token	OAuth2	For requesting new access_token	Not limited, must be used once in 90 days

https://docs.microsoft.com/en-us/azure/active-directory/develop/active-directory-configurable-token-lifetimes

#### Typical Azure AD Access Token payload [redacted]

```
{
    "aud": "https://outlook.office365.com",
    "iss": "https://sts.windows.net/c5ff949d-2696-4b68-9e13-055f19ed2d51/",
    "exp": 1646991788,
    "appid": "d3590ed6-52b3-4102-aeff-aad2292ab01c",
    "oid": "47bd560e-fd5e-42c5-b51b-ce963892805f",
    "scp": "user_impersonation",
    "tid": "c5ff949d-2696-4b68-9e13-055f19ed2d51",
    "upn": "user@company.com",
}
```

Value	Description
aud	Audience (resource server)
iss	Issuer or the token (authorization server)
scp	Scope (API)



@DrAzureAD

#### **Proof of identity**

Proof of identity	User	Device	App/client
Username + password (ROPC)	Х		Х
Authenticator	Х		
FIDO2	Х		
Kerberos ticket (Seamless SSO)	Х		
SAML token (federated identity)	Х		
Primary Refresh Token (PRT)	Х	Х	
Refresh token	Х	(X)	
Windows Hello for Business	Х	Х	
Certificate	Х	Х	Х
Temporary Access Pass (TAP)	Х		

#### Secureworks

## Attack scenarios

#### Stealing proof-of-identity

- Phishing
  - Man-in-the-middle (MITM) / adversary in-the-middle (AITM)

- Device Code
- Token theft
  - Steal from a browser
  - Steal from a computer
  - PRT

#### Spoofing proof-of-identity

- SAML tokens (federated identity)
- Kerberos tickets (Seamless SSO)
- Device certificates
- CBA certificates
- Pass-through Authentication (PTA)

#### **Attack scenarios**

Cloud	On-prem	Endpoint
Phishing	Identity federation	Token theft
MITM/AITM	Seamless SSO	
Device certificates	CBA	
	PTA	



## **Demo time!**

## Thank you!