Tokens of the Kingdom

@rustla

I'm Russ / @rustla

Penetration Tester at Trustwave

Previous Quests:

- BSides Perth

  (2021)

- WACTF challenge dev

  (2019, 2020, 2022)

- SecTalks Perth

  (2022, 2023)

Summary

Introduction to Tokens

+ Overview of OAuth
+ Token types
+ Scopes, audiences, consent

Looting with Tokens

+ Where to find tokens
+ What you can do with tokens
+ Ideas to detect and prevent token replay

TOKENS?

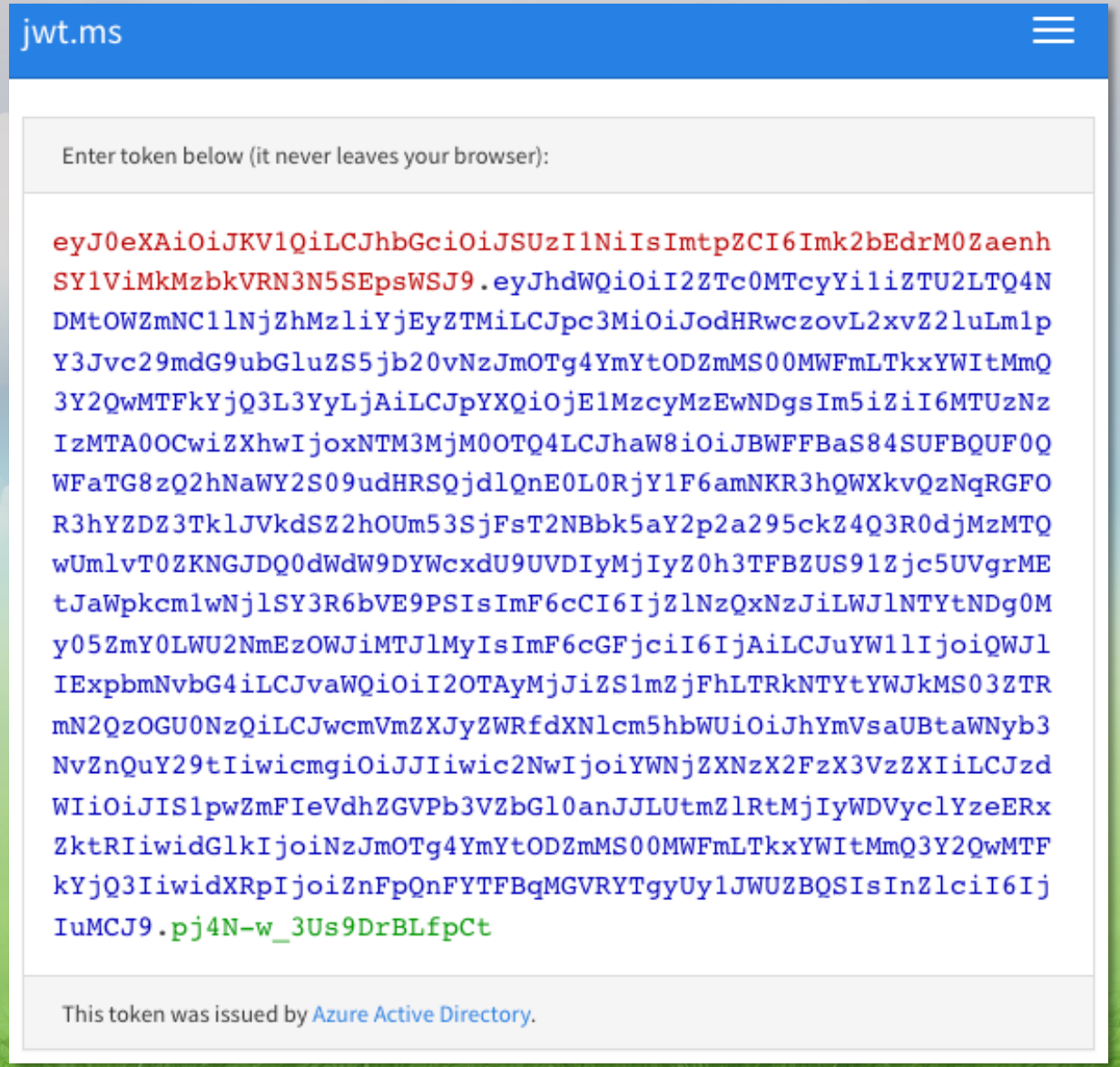
Issued to Clients by Identity Providers

Grant access to Resources (e.g. OneDrive, SharePoint, Azure)

OAuth Spec

- Access Tokens - Grant access
- Refresh Tokens - Fetch new access tokens

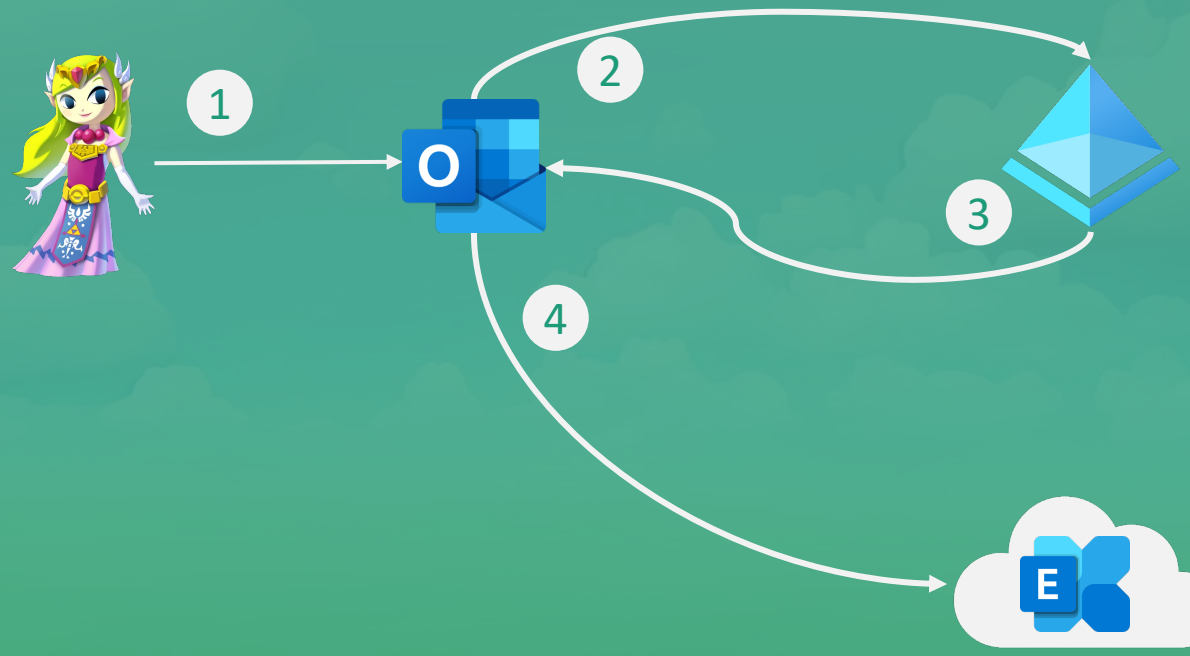
Example Access Token



OAuth Roles

OAuth Role	Kingdom-specific Examples
Authorisation Server (Identity Provider)	~~Azure AD (AAD)~~ Entra ID
Client (Application)	Outlook Client, Teams Client, Azure CLI, etc
Resource Server (APIs)	M365 services, Graph APIs, etc
Resource Owner (User)	End-user

OAuth Flow



1. User Auths to Client App
2. Client App Auths and Requests Access
3. Auth Server sends token to Client App
4. Client App requests resource w/ token

What's in a Token?

AAD OAuth access tokens are typically JWTs

JWTs include:

- Header (inc. signature algorithm)
- Payload Claims (information about the user)
- Signature (signature to prevent tampering)

Decoded Access Token

Decoded Token | Claims


```
{
  "typ": "JWT",
  "alg": "RS256",
  "kid": "i6lGk3FZzxRcUb2C3nEQ7syHJlY"
}.{
  "aud": "6e74172b-be56-4843-9ff4-e66a39bb12e3",
  "iss": "https://login.microsoftonline.com/72f988bf-86f1-41af-91ab-
2d7cd011db47/v2.0",
  "iat": 1537231048,
  "nbf": 1537231048,
  "exp": 1537234948,
  "aio":
"AXQAi/8IAAAAtAaZLo3ChMif6KOnttRB7eBq4/DccQzjcJGxPYy/C3jDaNGxXd6wNIIVGR
ghNRnwJ1lOcAnNZcjvkoyrFxCttv33140RioOFJ4bCCGVuoCag1uOTT22222gHwLPYQ/uf7
9QX+0KIijdrmp69RctzmQ==",
  "azp": "6e74172b-be56-4843-9ff4-e66a39bb12e3",
  "azpacr": "0",
  "name": "Abe Lincoln",
  "oid": "690222be-ff1a-4d56-abd1-7e4f7d38e474",
  "preferred_username": "abeli@microsoft.com",
  "rh": "I",
  "scp": "access_as_user",
  "sub": "HKZpfaHyWadeOouYlitjrI-KffTm222X5rrV3xDqfKQ",
  "tid": "72f988bf-86f1-41af-91ab-2d7cd011db47",
  "uti": "fqiBqXLPj0eQa82S-IYFAA",
  "ver": "2.0"
}.[Signature]
```

Relevant Payload Claims

Claim	Name	Description
aud	Audience	Resources the token can be used for
iss	Issuer	~~AAD~~ Entra ID Tenant ID that issued the token
exp	Expiry	Time (epoch) the token expires
scp	Scope	Permission given over the Resource APIs

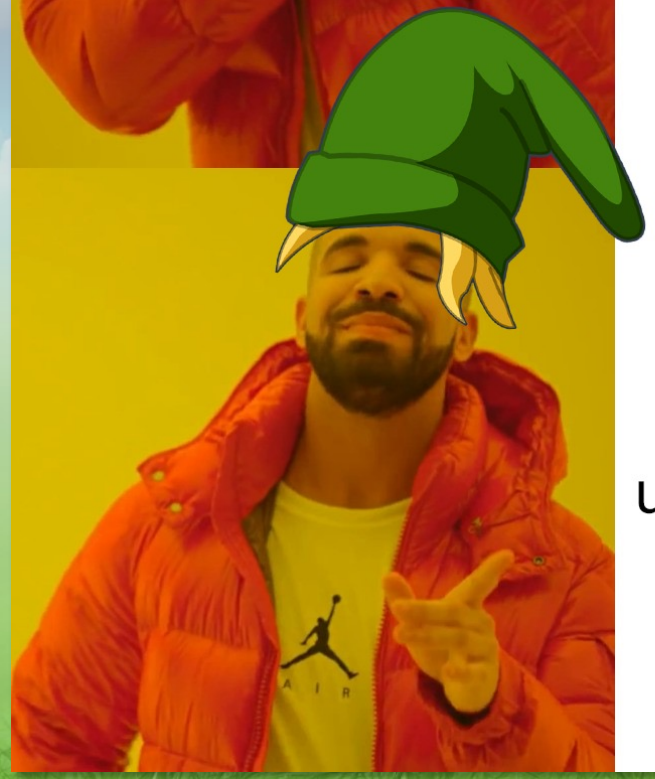
Scopes

Client Apps act on behalf of a user (delegated)

Scopes limit what a token can do with the resource e.g.

- Sub-set of permissions
- Everything the user can do (user_impersonation)

Scope:
User.Read



Scope:
user_impersonation

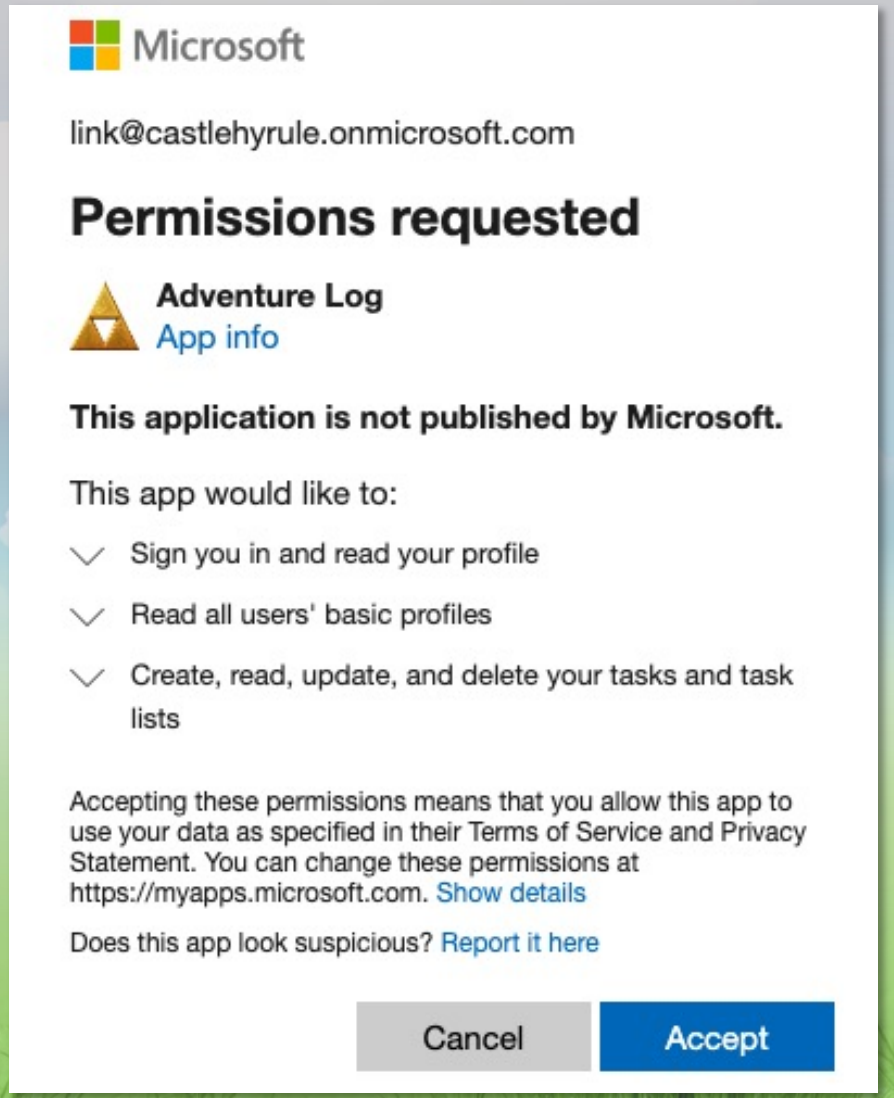
CONSENT

Scopes require consent

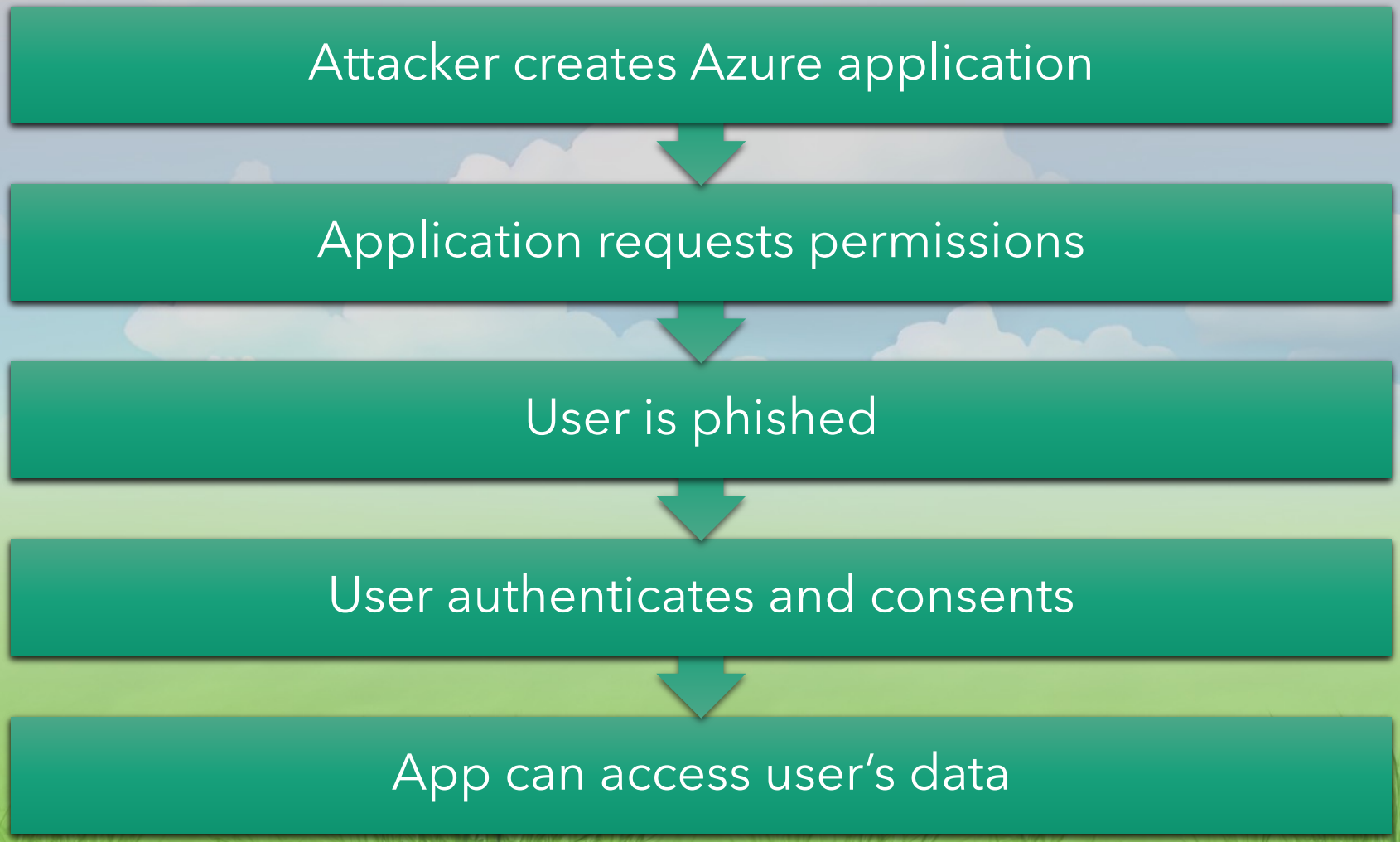
Consent prompt:

- Includes name of the app
- Warns it's not a Microsoft app
- Shows permissions requested

User must accept to use the app



Illicit Consent Grant



Illicit Consent Grant Demo (1/2)

Illicit Consent Grant Demo (2/2)

Getting Tokens

Where you may find:

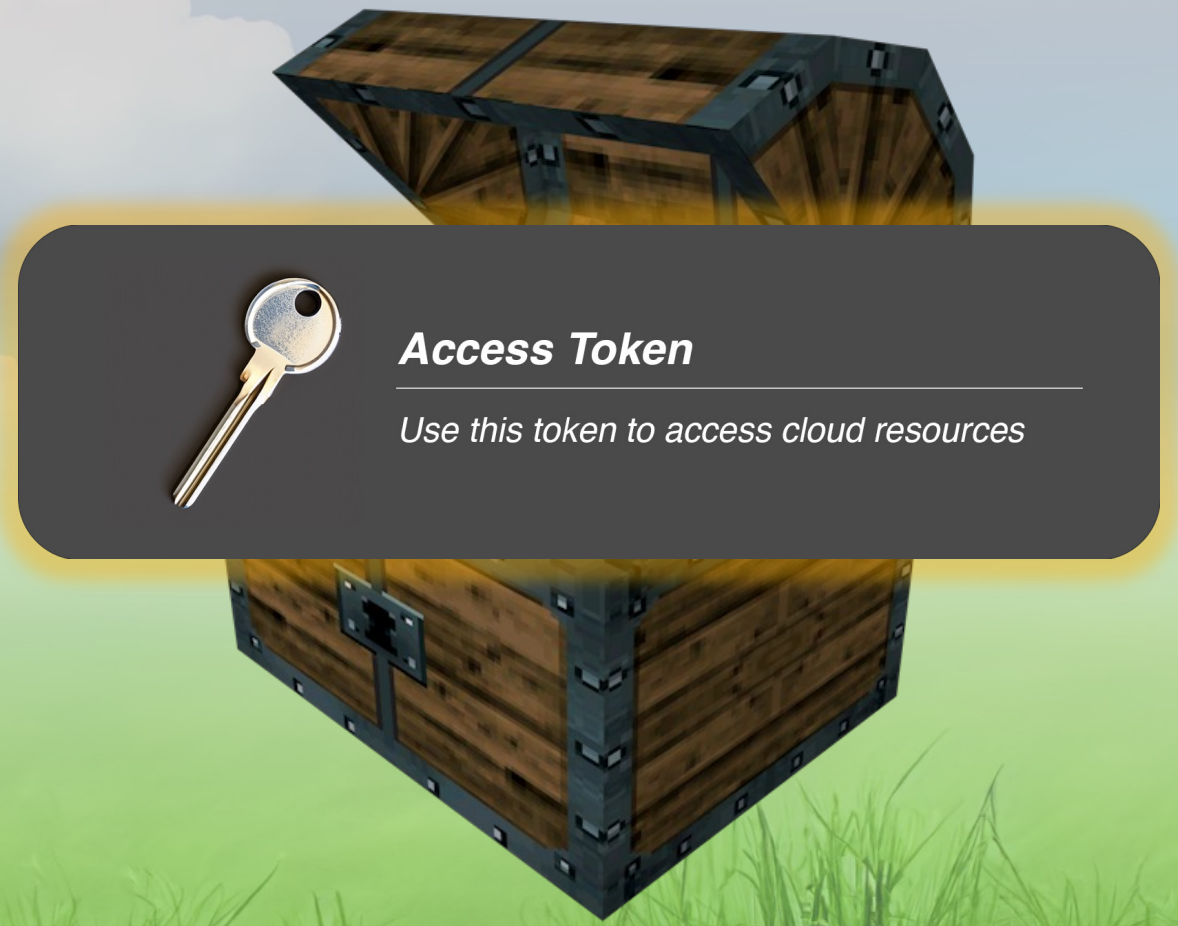
- On a compromised host

Looting Compromised Hosts Demo

Getting Tokens

Where you may find:

- On a compromised host
- Exploiting web app vulns



SPA Tokens

Refresh Tokens issued to Single Page App (SPA):

- Can be used to request additional tokens
- SPA must already have admin consent for new scope/tokens requested
- Have much shorter lifetime

Getting Tokens

Where you may find:

- On a compromised host
- Exploiting web app vulns
- Phishing

Device Code Phishing

Intended to login on devices with no keyboard

Attack Overview:

- Send the URL and code to a user
- They login
- You get their tokens

Device Code Phishing Demo

Got a Token, Now What?

Depends on the token

Some options:

- Interact with APIs
- Retrieve new access tokens
- Get access tokens for different resources

Email Exfil Demo

Teams Exfil Demo

Manual API Requests

No tool? Create manual requests (Microsoft documentation is your friend)

```
searchresponse = requests.get("https://castlehyrule-
my.sharepoint.com/_api/v2.0/me/drive/items/root/search(q='" +
query + "')", headers=reqheaders)


getitemresponse = requests.get("https://castlehyrule-
my.sharepoint.com/_api/v2.0/me/drive/items/" + itemid +
"/content", headers=reqheaders)
```

OneDrive Exfil Demo

Accessing Azure

May also use tokens to interact with Azure resources

Depends on:

- Scope & audience of token
- Access the user has within Azure

AzureHound Demo

Global Admin "Demo"

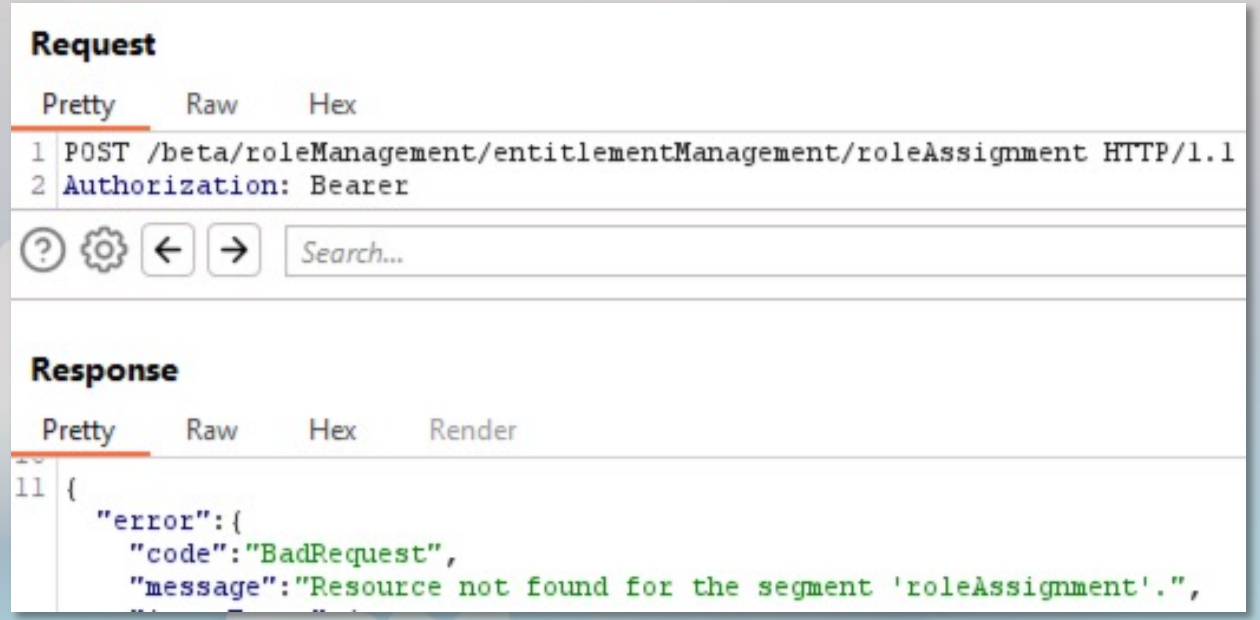
Attack: Link -> Add Global Admin role

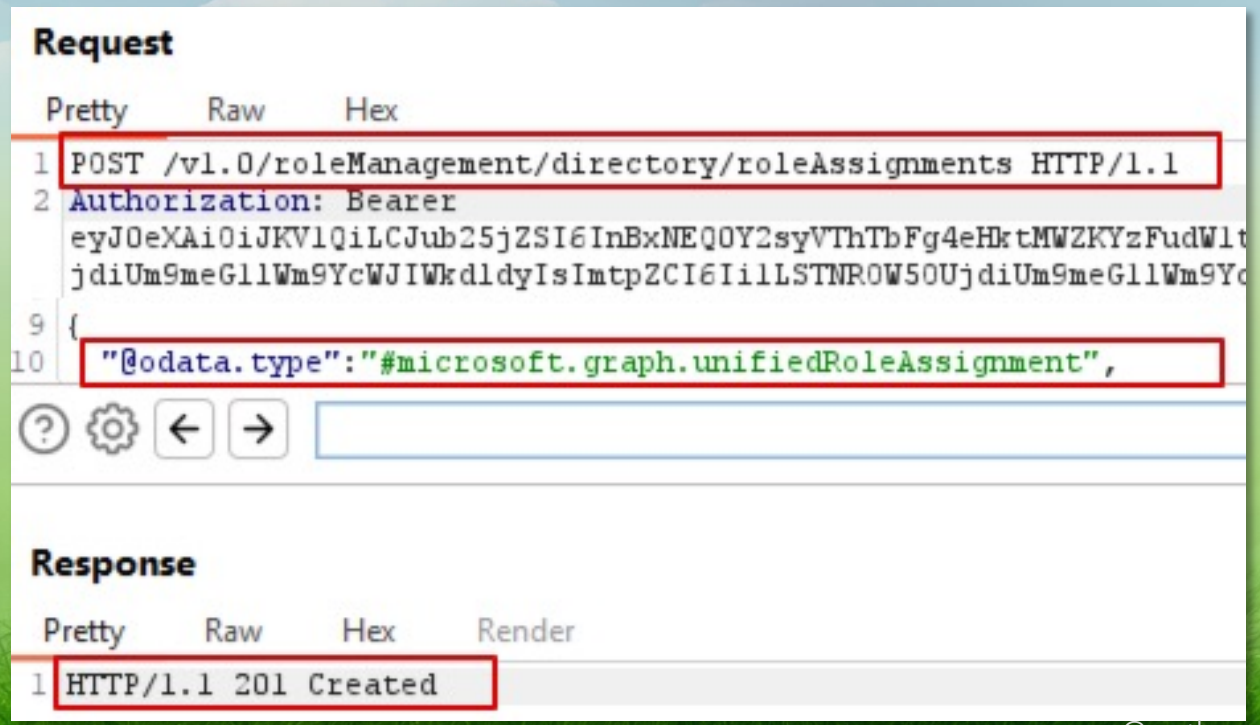
Oh no! Edge cases:

- PowerZure failing
- MS Azure PS failing

Troubleshot:

- Checked source code
- Checked documentation
- Fixed request





Detect / Prevent

Detect

- Refresh Tokens in Non-Interactive User Sign-Ins
- AAD Identity Protection “Anomalous Token” detection

Limit Replay

- Conditional Access to require compliant/joined device
- Continuous Access Evaluation to invalidate access tokens

Additional MS guidance

- aka.ms/tokentheft
- aka.ms/tokentheftplaybook

QUESTIONS?

Get in touch @rustla

Thanks to researchers (below) & artists
(for images borrowed/modified)

Tool	github.com/
365-Stealer	AlteredSecurity/365-Stealer
TokenTactics	rvrsh3ll/TokenTactics
OfficeTokens	trustedsec/CS-Remote-OPs-BOF
AADInternals	Gerenios/AADInternals
TeamFiltration	Flangvik/TeamFiltration
AzureHound	BloodHoundAD/AzureHound
BARK	BloodHoundAD/BARK
PowerZure	hausec/PowerZure