

# TOKENS OF THE KINGDOM

@rustla



eyJ0eXAiOiJKV1



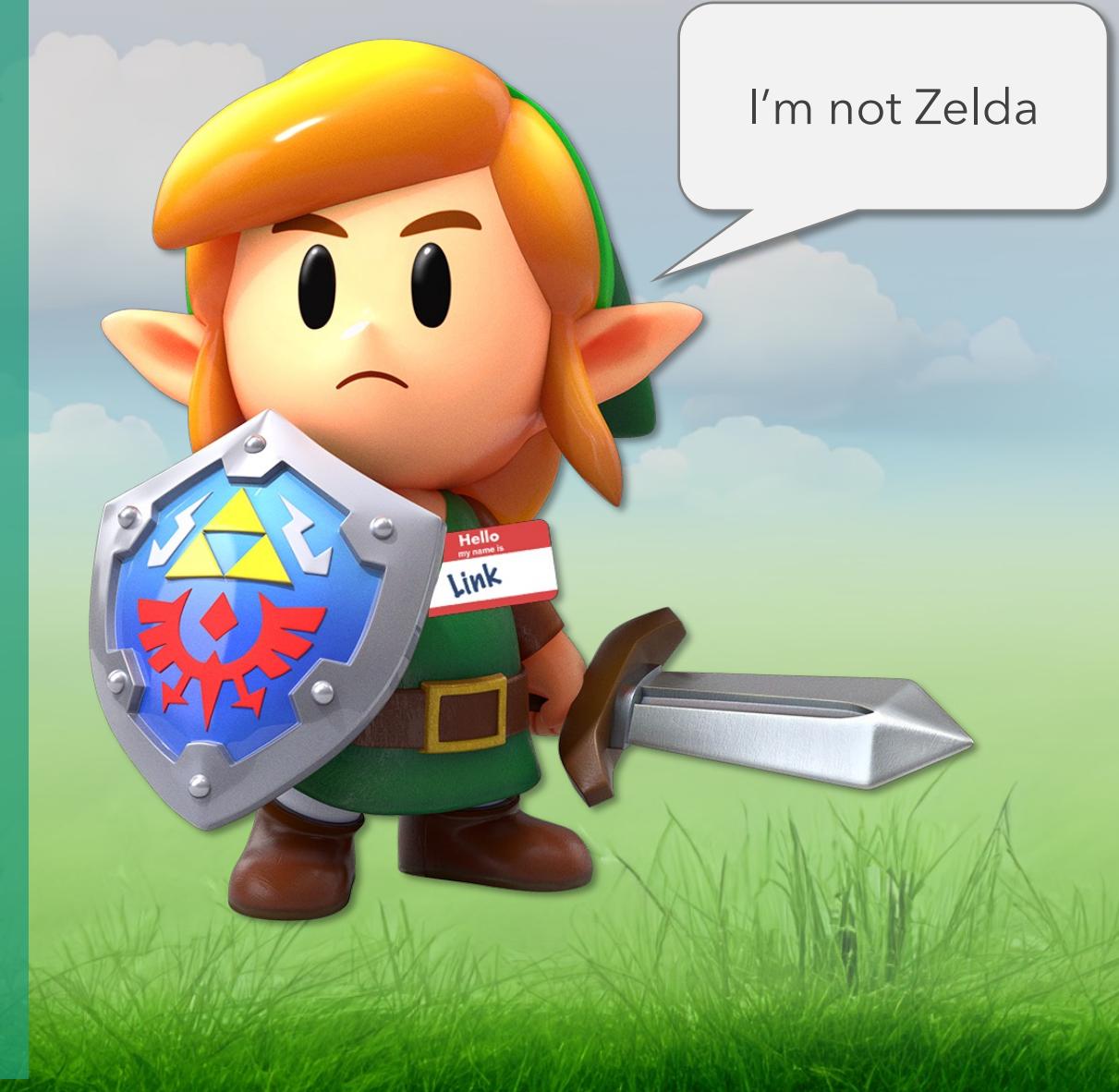
# H

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

jwt.ms

Enter token below (it never leaves your browser):

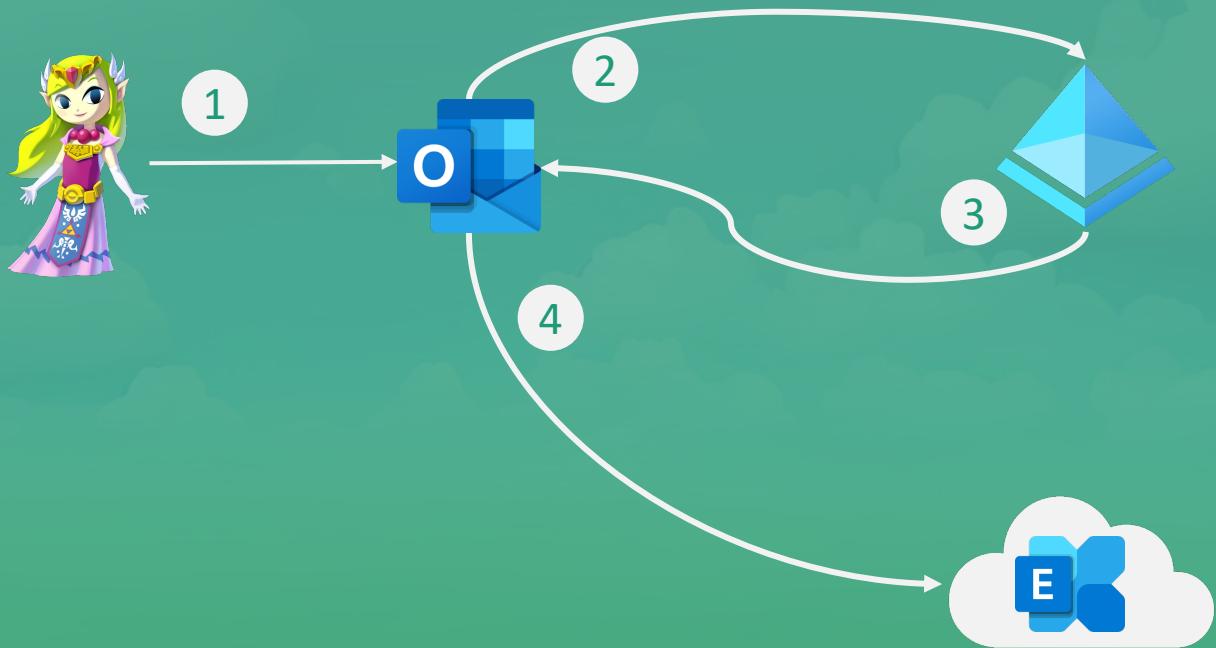
```
eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiIsImtpZCI6Imk2bEdrM0ZaenhSY1ViMkMzbkVRN3N5SEpsWSJ9.eyJhdWQiOiI2ZTc0MTcyYiIzTU2LTQ4NDMtOWZmNC1lNjZhMzliYjEyZTMiLCJpc3MiOiJodHRwczovL2xvZ2luLmlpY3Jvc29mdG9ubGluZS5jb20vNzJmOTg4YmYtODZmMS00MWFmLTkxyWIItMmQ3Y2QwMTFkYjQ3L3YyLjAiLCJpYXQiOjE1MzcyMzEwNDgsIm5iZiI6MTUzNzIzMta0OCwiZXhwIjoxNTM3MjM0OTQ4LCJhaW8iOiJBWFFBaS84SUFBQUF0QWFaTG8zQ2hNaWY2S09udHRSQjdlQnE0L0RjY1F6amNKR3hQWXkvQzNqRGFOR3hYZDZ3Tk1JVkdSz2hOUm53SjFsT2NBbk5aY2p2a295ckZ4Q3R0djMzMTQwUmlvT0ZKNGJDQ0dWdW9DYWcxdu9UVDIyMjIyZ0h3TFBZUS91Zjc5UVgrMETJaWpkcm1wNj1SY3R6bVE9PSIsImF6cCI6IjZ1NzQxNzJiLWJ1NTYtNDg0My05ZmY0LWU2NmEzOWJiMTJlMyIsImF6cGFjciI6IjAiLCJuYW1IjoiQWJ1IEpbmNvbG4iLCJvaWQiOii2OTAyMjJiZS1mZjFhLTRkNTYtYWJkMS03ZTRmN2QzOGU0NzQiLCJwcmVmZXJyZWRfdXNlc5hbWUiOijhYmVsaUBtaWNyb3NvZnQuY29tIiwigioiJJiIwic2NwIjoiYWNjZXNzX2FzX3VzzXIiLCJzdWIIoiJIS1pwZmFIeVdhZGVPb3VZbGl0anJJLUtmZ1RtMjIyWDVyclYzeERxZktRIiwidGlkIjoiNzJmOTg4YmYtODZmMS00MWFmLTkxyWIItMmQ3Y2QwMTFkYjQ3IiwidXRpIjoiZnFpQnFYTFBqMGVRYTgyUylJWUZBQSIsInZlcii6IjIuMCJ9.pj4N-w_3Us9DrBLfpCt
```

This token was issued by [Azure Active Directory](#).

# 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/8IAAAAtAaZLo3ChMif6K0nttRB7eBq4/DccQzjcJGxPYy/C3jDaNGxD6wNIVGR ghNRnwJ1l0cAnNZcjvkoyrFxCttv33140Rio0FJ4bCCGVuoCag1u0TT22222gHwLPYQ/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-KfftTm222X5rrV3xDqfKQ", "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



link@castlehyrule.onmicrosoft.com

## Permissions requested



This application is not published by Microsoft.

This app would like to:

- ✓ Sign you in and read your profile
- ✓ Read all users' basic profiles
- ✓ Create, read, update, and delete your tasks and task lists

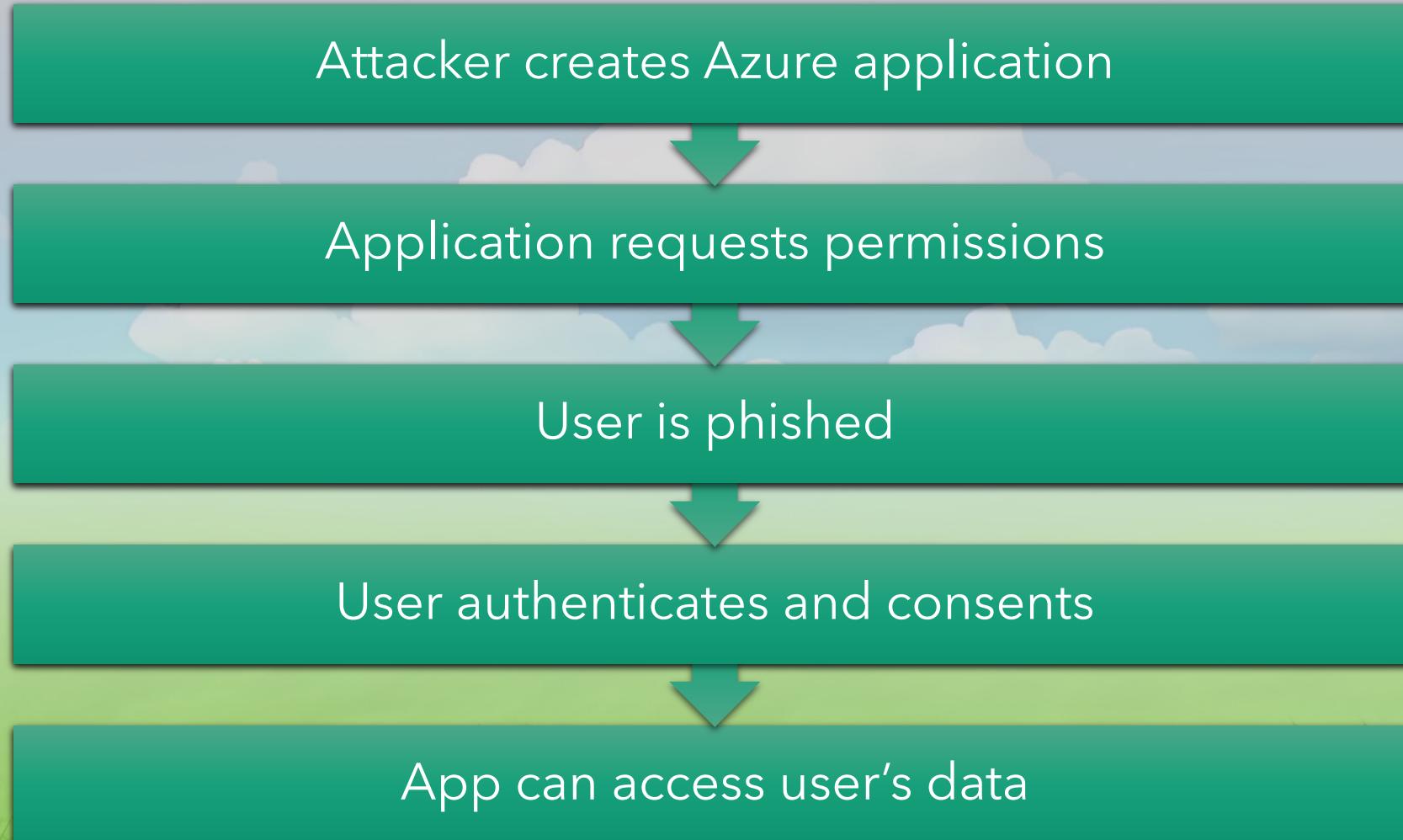
Accepting these permissions means that you allow this app to use your data as specified in their Terms of Service and Privacy Statement. You can change these permissions at <https://myapps.microsoft.com>. [Show details](#)

Does this app look suspicious? [Report it here](#)

Cancel

Accept

# ILLICIT CONSENT GRANT



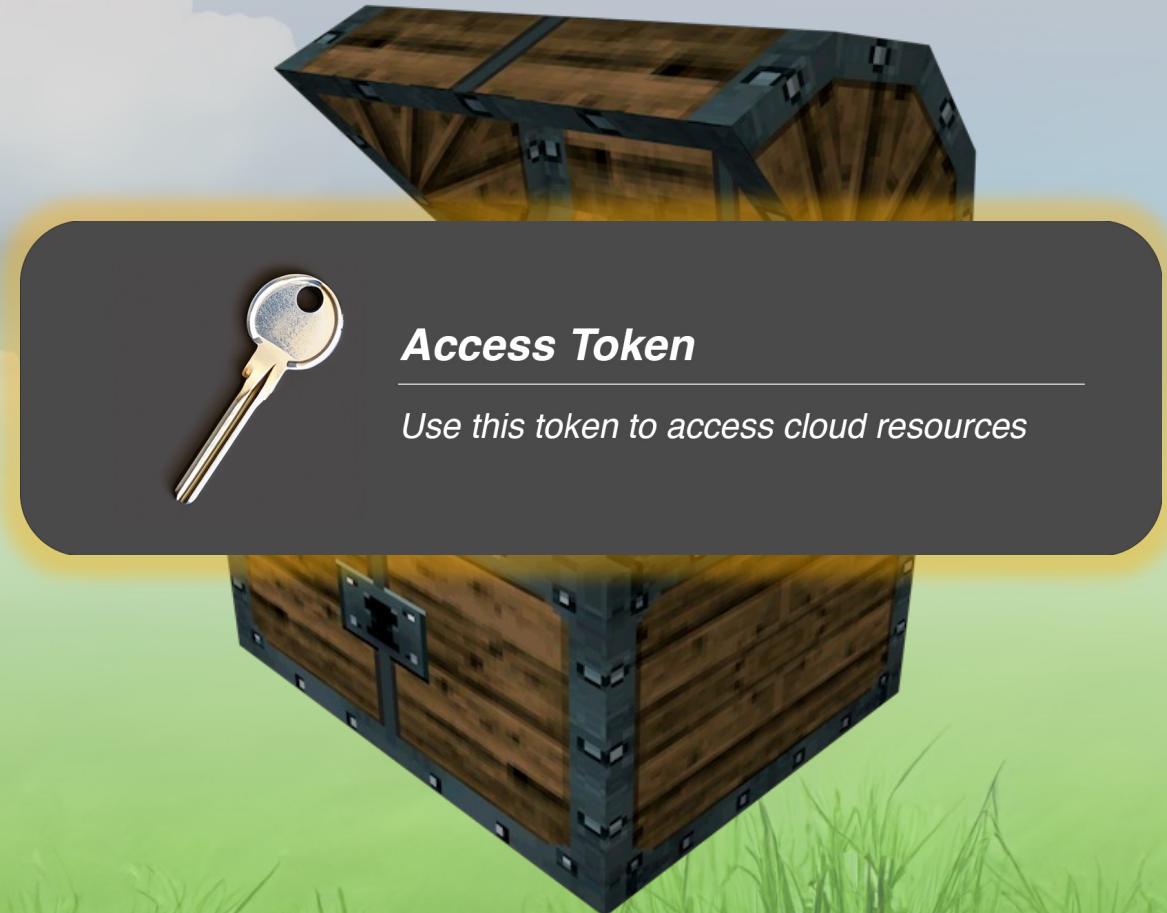
# **ILLICIT CONSENT GRANT DEMO (1/2)**

# **ILLICIT CONSENT GRANT DEMO (2/2)**

# GETTING TOKENS

Where you may find:

- On a compromised host



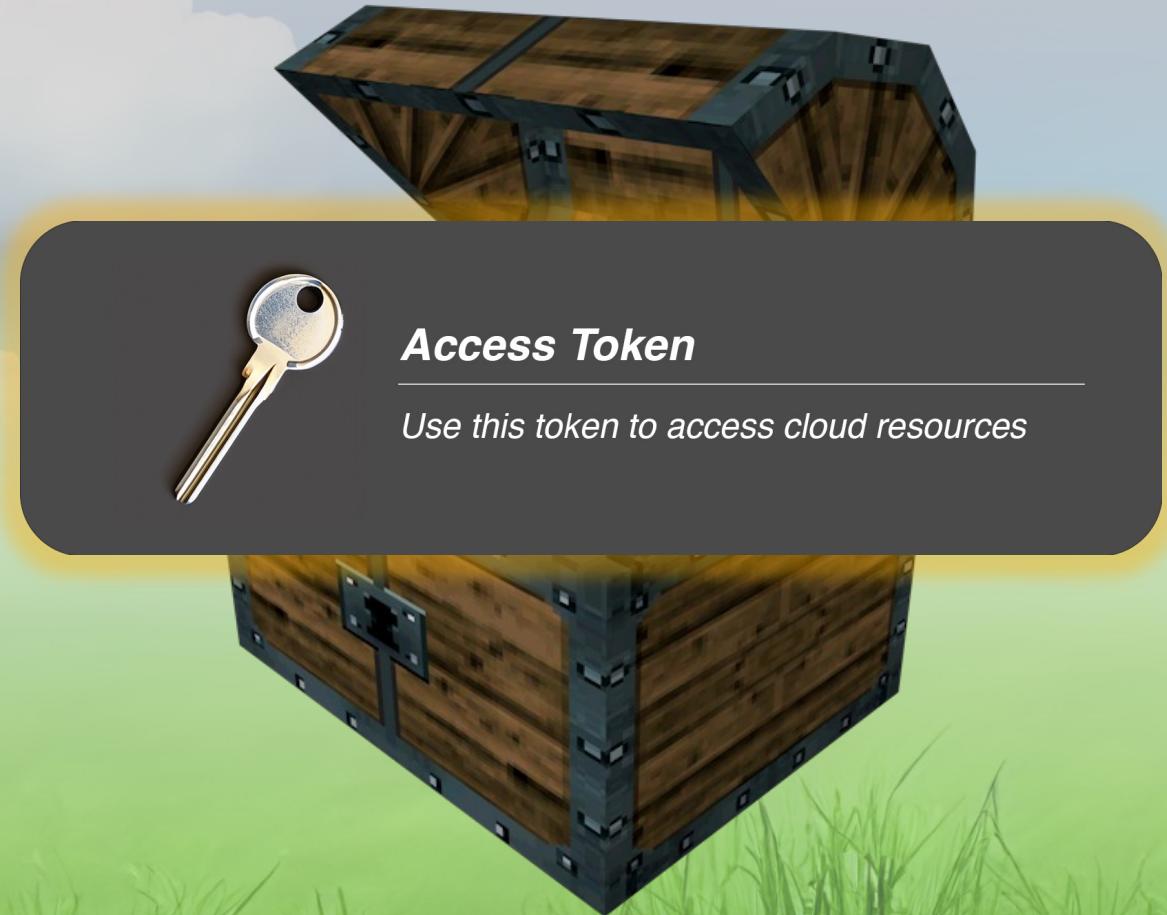


**LOOTING COMPROMISED HOSTS DEMO**

# GETTING TOKENS

Where you may find:

- On a compromised host
- Exploiting web app vulns



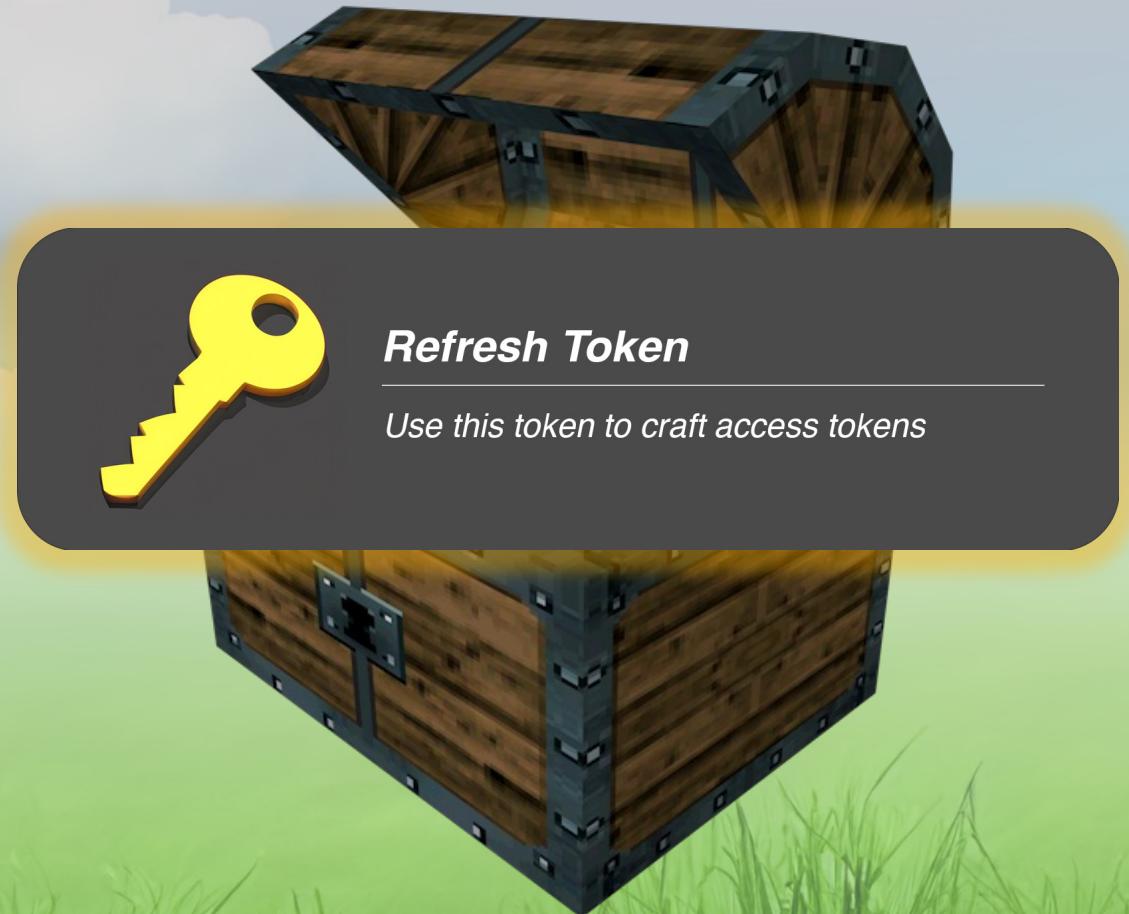
## **Access Token**

*Use this token to access cloud resources*

# 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

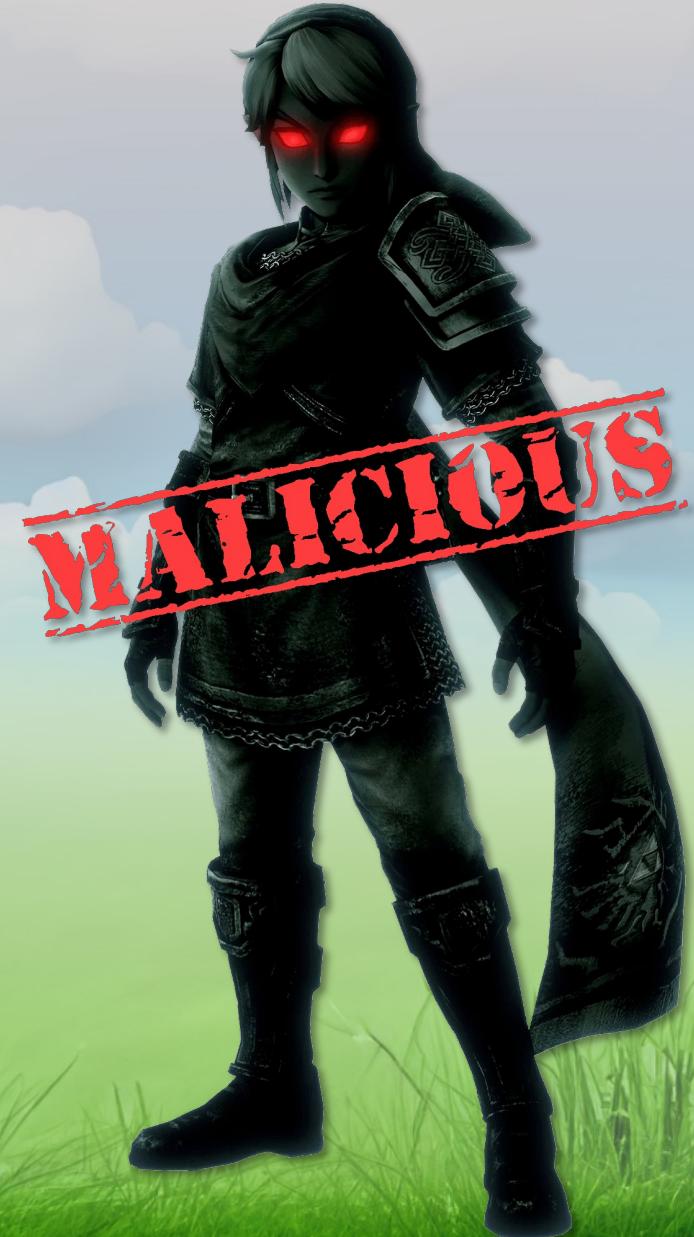


# DEVICE CODE PHISHING

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





A scenic landscape featuring a bright blue sky filled with fluffy white clouds. In the foreground, there is a lush, vibrant green field of tall grass.

**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



The background features a vibrant landscape with a clear blue sky filled with fluffy white clouds. Below the sky is a vast, bright green field of grass. In the foreground, there are several tufts of tall, detailed green grass.

**AZUREHOUND DEMO**

# GLOBAL ADMIN ‘DEMO’

Attack: Link -> Add Global Admin role

Oh no! Edge cases:

- PowerZure failing
- MS Azure PS failing

Troubleshoot:

- Checked source code
- Checked documentation
- Fixed request

The screenshot shows a REST client interface with two requests and their corresponding responses.

**Request 1:**

```
POST /beta/roleManagement/entitlementManagement/roleAssignment HTTP/1.1
Authorization: Bearer
```

**Response 1:**11 {
 "error": {
 "code": "BadRequest",
 "message": "Resource not found for the segment 'roleAssignment'.",

**Request 2:**

```
POST /v1.0/roleManagement/directory/roleAssignments HTTP/1.1
Authorization: Bearer
eyJ0eXAiOiJKV1QiLCJub25jZSI6InBxNEQ0Y2syVThTbFg4eHktMWZKYzFudWlt
jdiUm9meG11Wm9YcWJIWkdldyIsImtpZCI6Ii1LSTNR0W50Ujd1Um9meG11Wm9Yc
@odata.type": "#microsoft.graph.unifiedRoleAssignment",
```

**Response 2:**1 HTTP/1.1 201 Created

# 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](http://aka.ms/tokentheft)
- [aka.ms/tokentheftplaybook](http://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

