

Business Email Compromise

Prevent - Detect - Respond



Threat Vectors [consolidated]

- Unpatched Vulnerabilities
- Misconfiguration
- Identity Attacks

“9 out of 10 data breaches start with Phishing”

PM	149	<u>ActivatePositions.csv</u>
AM	Directory	<u>Archived</u>
AM	Directory	<u>aspnet client</u>
PM	54,169	<u>Department.csv</u>
PM	3,536,968	<u>Employee Export.csv</u>
PM	199	<u>Ethnicity.csv</u>
M	897,514	<u>InsertDepartmentHours.csv</u>
M	51,545	<u>InsertLocationHours.csv</u>
M	57,256	<u>JobCodes.csv</u>

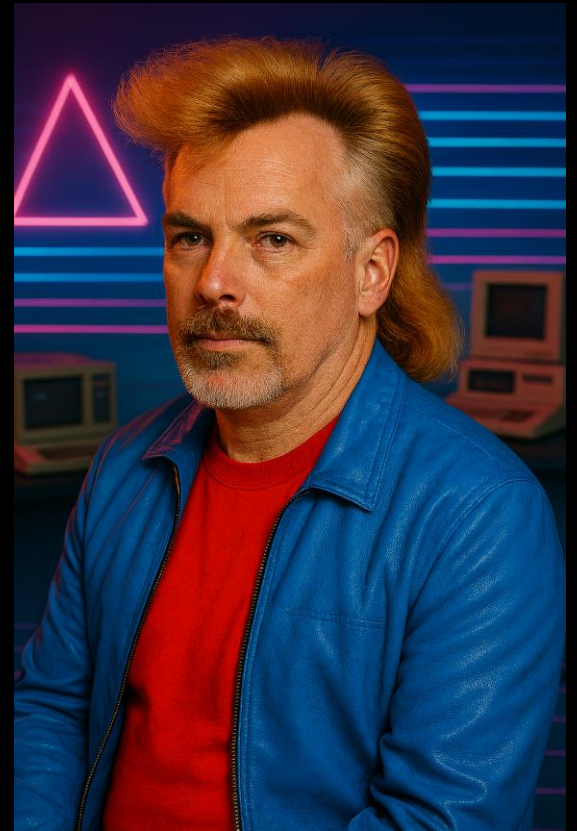
	27,328	<u>JobCodes.csv</u>
M	27,242	<u>InsertDepartmentHours.csv</u>
M	27,242	<u>InsertLocationHours.csv</u>

The BEC Kill Chain [simplified]

1. Invoke Trust and/or Trigger Emotional Response
 2. Override Decision-Making w/Call to Action
 3. Manipulate Identity/Actions for Financial Gain
 4. Use Compromised Identity to Invoke Trust
- [... REPEAT ...]

“you can’t stop 2 seconds of stupid”

🎵 “Things can only get ~~better~~ worse.” 🎵
~ *Patterson Jones*



Agenda

- Prevention Strategies
- Detect/Respond
- M365 Tips & Tricks
- Resources
- *Appendix* [Anatomy of a BEC]





“strive for perfection...
come within a quarter inch”

Patterson Cake
Incident Response Contrarian

Prevention Strategies

know your enemy and yourself

The BEC Kill Chain [simplified]

1. Invoke Trust and/or Trigger Emotional Response
 2. Override Decision-Making w/Call to Action
 3. Manipulate Identity/Actions for Financial Gain
 4. Use Compromised Identity to Invoke Trust
- [... REPEAT ...]

“you can’t stop 2 seconds of stupid”

The BEC Kill Chain [simplified]

1. Invoke Trust and/or Trigger Emotional Response

It's probably coming from someone they know/trust.

You're probably not fixing this one directly.

2. Override Decision-Making w/Call to Action

3. Manipulate Identity/Actions for Financial Gain

4. Use Compromised Identity to Invoke Trust

[... REPEAT ...]

~~“you can't stop 2 seconds of stupid”~~
but you should still try!

Your enemy and yourself ...

1. Invoke Trust and/or **Trigger Emotional Response**
 2. Override Decision-Making w/Call to Action
 3. Manipulate Identity/Actions for Financial Gain
 4. Use Compromised Identity to Invoke Trust
- [... REPEAT ...]

Tell them a story! [funny ... happy ... sad]

Make it personal/relatable!

Be succinct!

“May I have your ...”

Credit Card Number? **No!**

Social Security Number? **No!**

Username/Password? **No!**

GUARD THESE THINGS LIKE YOUR FUTURE DEPENDS ON IT
Because it does!

The BEC Kill Chain [simplified]

1. Invoke Trust and/or Trigger Emotional Response

2. Override Decision-Making w/Call to Action

Multi-Factor-Auth is your due diligence.

Multi-Factor-Auth is NOT a silver bullet.

3. Manipulate Identity/Actions for Financial Gain

4. Use Compromised Identity to Invoke Trust

[... REPEAT ...]

MFA = One layer of Defense in Depth

The BEC Kill Chain [simplified]

1. Invoke Trust and/or Trigger Emotional Response
 2. Override Decision-Making w/Call to Action
 3. Manipulate Identity/Actions for Financial Gain
 - ***Implement Multi-Factor-Workflow for ALL IMPORTANT transactions.***
 4. Use Compromised Identity to Invoke Trust
- [... REPEAT ...]

IMPORTANT = \$, \$\$, \$\$\$, \$\$\$\$?

The BEC Kill Chain [simplified]

1. Invoke Trust and/or Trigger Emotional Response
2. Override Decision-Making w/Call to Action
3. Manipulate Identity/Actions for Financial Gain
4. Use Compromised Identity to Invoke Trust

Monitor for post-exploitation indicators.

[... REPEAT ...]

Newly Created Inbox-Rules with Short/Unusual Names
Bulk Outbound Mail Messages (especially with links)

~~“you can’t stop 2 seconds of stupid”~~
but you should still try!

Detection & Response

simple...effective...repeatable

Threat Report ["the wild"]

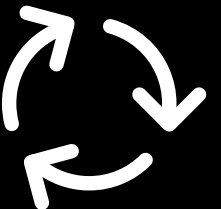
- BEC Standard Operating Procedures
- BEC "Identifiers" (UEBA)
- M365 Investigative Tips

[... "the weeds" ...]

BEC SoP [“the wild”]

- Observes User Behavior (often a few days to two weeks)
- Explores M365 Content
- Impersonates User in \$\$\$ Transactions
- Hides Actions From User (Inbox-Rules)*
 - Favorite Name = “.”
 - Moves mail to “unused” folder, e.g. “RSS Feeds”
- Registers M365 Applications (Search/Steal Data)
- Impersonates User to Phish Contacts

*[Find the Rule → Find the \$\$\$ Target]



BEC Investigative Questions [???

- Have we been compromised?
- If yes, then:
 - What accounts have been impacted?
 - What unauthorized access occurred?
 - What unauthorized actions occurred?

“that, Detective Spooner, is the right question!”



M365 Identifiers [UEBA]

- Username/Password
- Browser/OS [User-Agent String]
- Source IP Address
- MFA Type/Device
- Session Cookie

“what differentiates you from me?”



M365 Identifiers [UEBA]

- ~~Username/Password~~
- Browser/OS [User-Agent String]
- Source IP Address
- ~~MFA Type/Device~~
- ~~Session Cookie~~

“what differentiates the User from the TA?”



BEC Investigative Questions [???

- Have we been compromised? – Yes
[Firefox/Linux ... Netherlands]
- If yes, then:
 - What accounts have been impacted?
 - What unauthorized access occurred?
 - What unauthorized actions occurred?



“that, Detective Spooner, is the right question!”



M365 Investigative Tips

simple...effective...repeatable

BECUEBA – Entra ID [“have we been compromised”]

#1 Acquisition – SIGN-IN LOGS:

Entra Admin\Sign-In Logs ...

- Add all “Columns”
- Set Date to Max Range [note 100K max entries]
- Download in CSV & JSON [x6 each]

7 to 30 days retention!!!



BECUEBA – Entra ID [“have we been compromised”]

[Home](#) > [Haven Information Security, LLC](#) > [Users](#)



Users | Sign-in logs

Haven Information Security, LLC



Download



Export Data Settings



Troubleshoot



Refresh



Columns



Got feedback?



All users



Audit logs



Sign-in logs



Diagnose and solve problems



Deleted users



Password reset



User settings



Bulk operation results



New support request

Date : **Last 7 days**

Show dates as : **UTC**



Add filters

User sign-ins (interactive)

User sign-ins (non-interactive)

Date (UTC)	↑↓	Request ID	User	↑↓	Username	↑↓	Application	↑↓
4/13/2025, 7:27:03 AM		55286b0e-4f43-4214...	Patterson Cake		pc@securecake.com		Azure Portal	
4/13/2025, 7:25:16 AM		3e436c6e-eeac-4efc-...	Patterson Cake		pc@securecake.com		Azure Portal	
4/12/2025, 6:24:39 AM		c7f85616-8148-4cf7-...	Patterson Cake		pc@securecake.com		Office 365 Exchange ...	
4/8/2025, 6:40:08 PM		79cebbbb-5667-4c1...	Benjamin Cake		bcake@haven-usa.c...		One Outlook Web	
4/6/2025, 2:01:34 PM		681562b0-96d1-44c...	Patterson Cake		pc@securecake.com		Office 365 Exchange ...	
4/6/2025, 2:01:33 PM		5bc8bc93-bba3-43d...	Patterson Cake		pc@securecake.com		Office 365 Exchange ...	
4/6/2025, 2:01:11 PM		ae8b671a-457c-440f...	Patterson Cake		pc@securecake.com		Office 365 Exchange ...	

BECUEBA – Entra ID [”have we been compromised”]

#2 – Acquisition – AUDIT LOGS:

- Entra Admin\Audit Logs ...
 - Add all “Columns”
 - Set Date to Max Range [note 250K max records]
 - Download in CSV & JSON [x1 each]

7 to 30 days retention!!!



BECUEBA – Entra ID [“have we been compromised”]

#3 Investigation – SECURITY REPORTS:

- Entra Admin\Security ...
 - Risky Users
 - Risky Sign-Ins

Risk state : 2 selected

Status

Risk state

☒ At risk

☒ Confirmed compromised

☒ Remediated

☒ Dismissed

☒ Confirmed safe

Apply

Sign-in Type : 2 selected

Sign-in Type

☒ Interactive

☒ Non-interactive

Apply

Status : Active

Status

☒ Deleted

☒ Active

Apply

Manage

Identity Secure Score

Named locations

Authentication methods

Multifactor authentication

Certificate authorities (classic)

Public key infrastructure (Preview)

Report

Risky users

Risky workload identities

Risky sign-ins

IMPORTANT

Date (UTC)	Application	IP address	Location	Risk state	Risk level (Detection type(s)
2024-08-07T13:38:23Z	OfficeHome	13.57.246.62	San Jose, California, US	Remediated	Low	Unfamiliar sign-in properties
2024-08-07T13:38:19Z	OfficeHome	13.57.246.62	San Jose, California, US	Remediated	Low	Unfamiliar sign-in properties, Atypical travel
2024-08-06T20:57:22Z	Office 365 Exchange Online	3.80.218.146	Ashburn, Virginia, US	Remediated	Medium	Unfamiliar sign-in properties
2024-08-06T20:57:20Z	Office 365 Exchange Online	3.80.218.146	Ashburn, Virginia, US	Dismissed	Medium	Unfamiliar sign-in properties, Atypical travel
2024-08-06T19:10:47Z	OfficeHome	54.163.19.39	Ashburn, Virginia, US	Remediated	Medium	Unfamiliar sign-in properties, Atypical travel

BECUEBA – Entra ID

[”have we been compromised” – “what unauthorized access occurred”]

#4 Investigation – SIGN-INS:

- ~~Username/Password~~
- Browser/OS [User-Agent String]
- Source IP Address
- ~~MFA Type/Device~~
- ~~Session Cookie~~

8/21/2024, 7:43:47 PM	pc@securecake.com	Office 365 Exchange ...	Success	44.223.33.132	Ashburn, Virginia, US	Linux ←	Chrome 118.0.0
8/21/2024, 7:17:30 PM	pc@securecake.com	OfficeHome	Interrupted	44.223.33.132	Ashburn, Virginia, US	Windows10	Chrome 127.0.0
8/17/2024, 4:04:57 PM	pc@securecake.com	Office365 Shell WCS...	Success	172.221.112.235	Grand Junction, Colo...	Windows10	Edge 127.0.0
8/17/2024, 4:04:57 PM	pc@securecake.com	Office365 Shell WCS...	Success	172.221.112.235	Grand Junction, Colo...	Windows10	Edge 127.0.0

BECUEBA – Entra ID

[”what unauthorized access/actions occurred”]

#5 Investigation – AUDIT LOGS:

- ‘Update User’ [MFA changes?]
 - StrongAuthenticationUserDetails ... NewValue
- ‘Add Service Principal’ [App Registrations?]
 - DisplayName ... NewValue
- ‘Add App Role Assignment Grant to User’ [App Registrations?]
 - ServicePrincipal ... ID

2024-08-12T15:55:06	Core Directory	UserManagement	Reset user password	Success	User	
2024-08-09T14:13:57	Core Directory	UserManagement	Add app role assignment grant to user	Success	ServicePrincipal	eM Client
2024-08-06T21:16:29	Core Directory	UserManagement	Update user	Success	User	

Unified Audit Log (UAL)

[“what unauthorized access/actions occurred”]

#6 Acquisition – UAL:

- Purview*
- PowerShell*
- Graph API

Unified Audit Log (UAL) – PSA

Audit Log Record Type [RecordType]

- Exchange Admin [1]
- Entra Id Events [8]
- Security Compliance Alerts [40]

<https://dub.sh/m365-recordtype>

Purview – Compliance “Audit”

Date and time range (UTC) *

Start

Apr 01

00:00

End

Apr 13

00:00

Keyword Search

Enter the keyword to search for

Admin Units

Choose which Admin Units to search for

Search

Clear all

Activities - friendly names

Choose which activities to search for

Activities - operation names

i

Enter operation values, separated by commas

Record Types

Select the record types to search for

Search name

BEC Investigation 04152025

Users

PC Patterson Cake X Add the users whose au...

File, folder, or site

i

Enter all or a part of the name of a file, website, o...

Workloads

Enter the workloads to search for

↓ Export

Date (UTC) ↓	IP Address ↓	User ↓	Record Type ↓	Activity ↓
Apr 12, 2025 6:40 PM	2603:10b6:408:227::13	pc@securecake.com	ExchangeItemAggregated	Accessed mailbox items
Apr 12, 2025 6:01 PM	194.78.149.132	pc@securecake.com	ExchangeItemAggregated	Accessed mailbox items
Apr 12, 2025 7:30 AM	194.78.149.132	pc@securecake.com	ExchangeItemAggregated	Accessed mailbox items

Unified Audit Log (UAL)

[“what unauthorized access/actions occurred”]

#6 Acquisition & Analysis – UAL:

- PowerShell→SOF-ELK [up to 365 days retention]
 - ‘New-InboxRule’ ... Name:Name,Value; FromAddressContainsWords

<https://git.new/m365-bec>

Resources

<https://www.blackhillsinfosec.com/blog>

1: wrangling-the-m365-ual-with-powershell-and-sof-elk-part-1-of-3

2: wrangling-the-m365-ual-with-powershell-and-sof-elk-part-2-of-3

3: wrangling-the-m365-ual-with-powershell-and-sof-elk-part-3-of-3

<https://git.new/m365-bec>

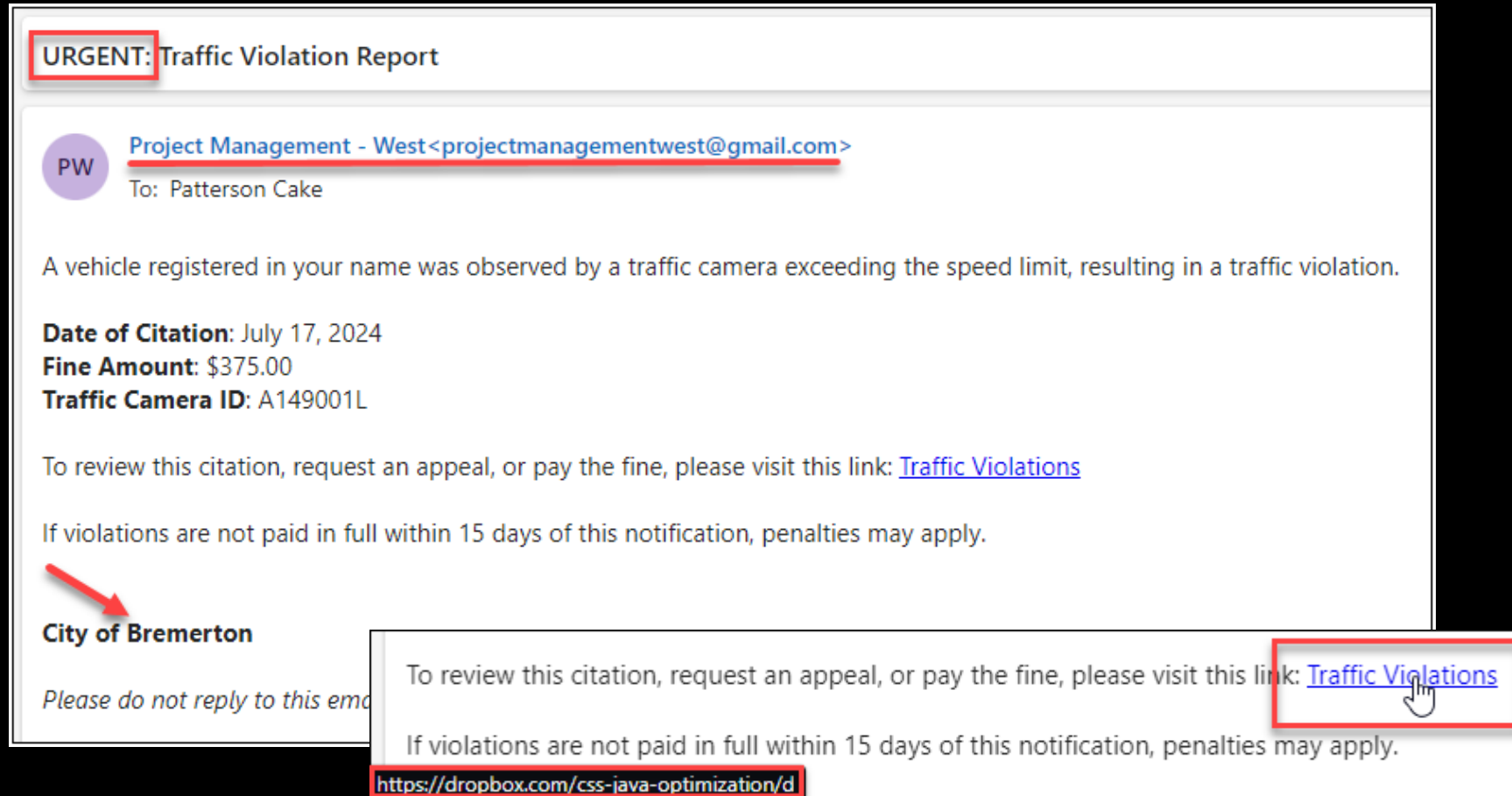
PWYC Workshop – M365 BEC - October 17, 2025 [4 Hour]

Anatomy of M365 BEC

know your enemy...step-by-step

Anatomy of a Business Email Compromise

#1: Trigger an emotional response with call to action



[... "someone you know" ...]

URGENT: Traffic Violation Report



Project Management - West<projectmanagementwest@gmail.com>

To: Patterson Cake

A vehicle registered in your name was observed by a traffic camera exceeding the speed limit, resulting in a traffic violation.

Date of Citation: July 17, 2024

Fine Amount: \$375.00

Traffic Camera ID: A149001L

To review this citation, request an appeal, or pay the fine, please visit this link: [Traffic Violations](#)

If violations are not paid in full within 15 days of this notification, penalties may apply.



City of Bremerton

Please do not reply

To review this citation, request an appeal, or pay the fine, please visit this link: [Traffic Violations](#)

If violations are not paid in full within 15 days of this notification, penalties may apply.

<https://dropbox.com/css-java-optimization/d>

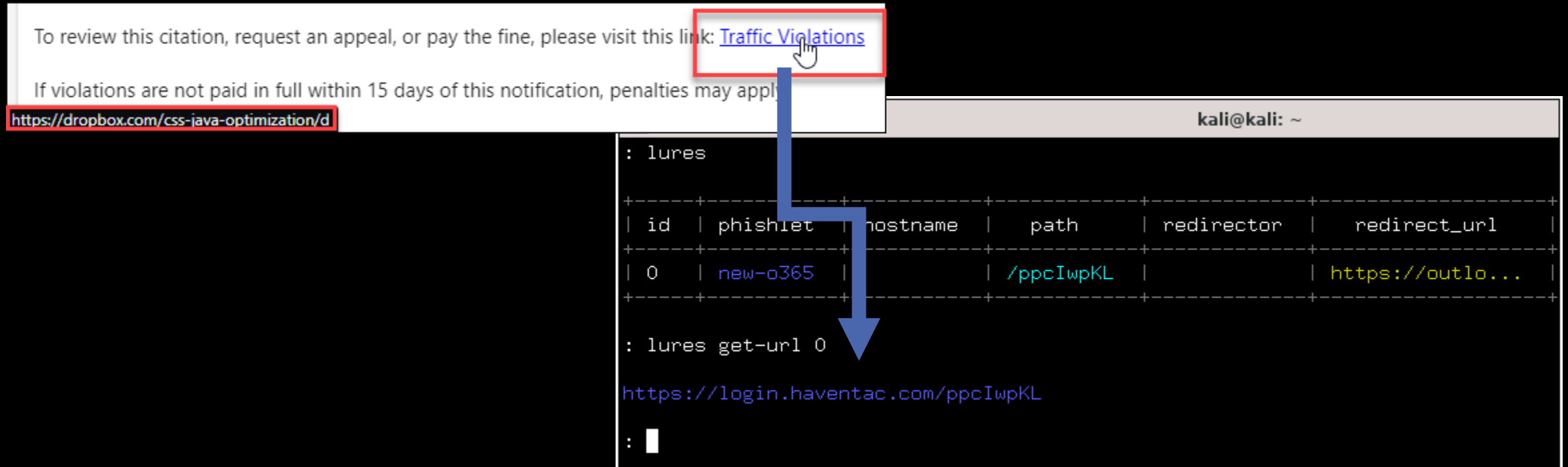
Anatomy of a Business Email Compromise

#2: User clicks malicious link to “Evil Proxy”

To review this citation, request an appeal, or pay the fine, please visit this link: [Traffic Violations](#)

If violations are not paid in full within 15 days of this notification, penalties may apply.

<https://dropbox.com/css-java-optimization/d>

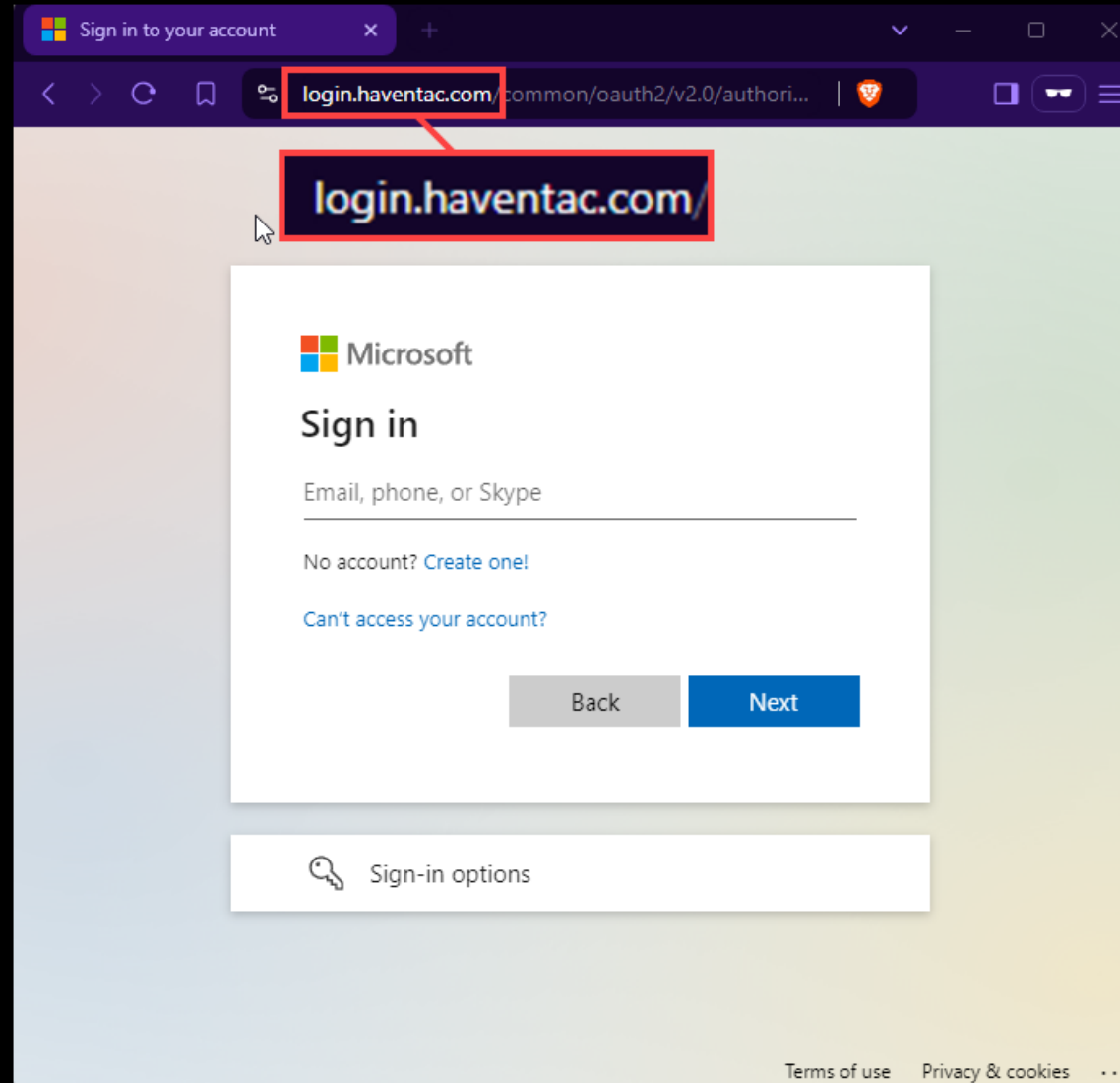


```
kali@kali: ~  
: lures  
+-----+-----+-----+-----+-----+-----+  
| id | phishlet | hostname | path | redirector | redirect_url |  
+-----+-----+-----+-----+-----+-----+  
| 0 | new-o365 | | /ppcIwpKL | | https://outlo... |  
+-----+-----+-----+-----+-----+-----+  
: lures get-url 0  
https://login.haventac.com/ppcIwpKL  
: █
```

[... “Man in the Middle” ...]

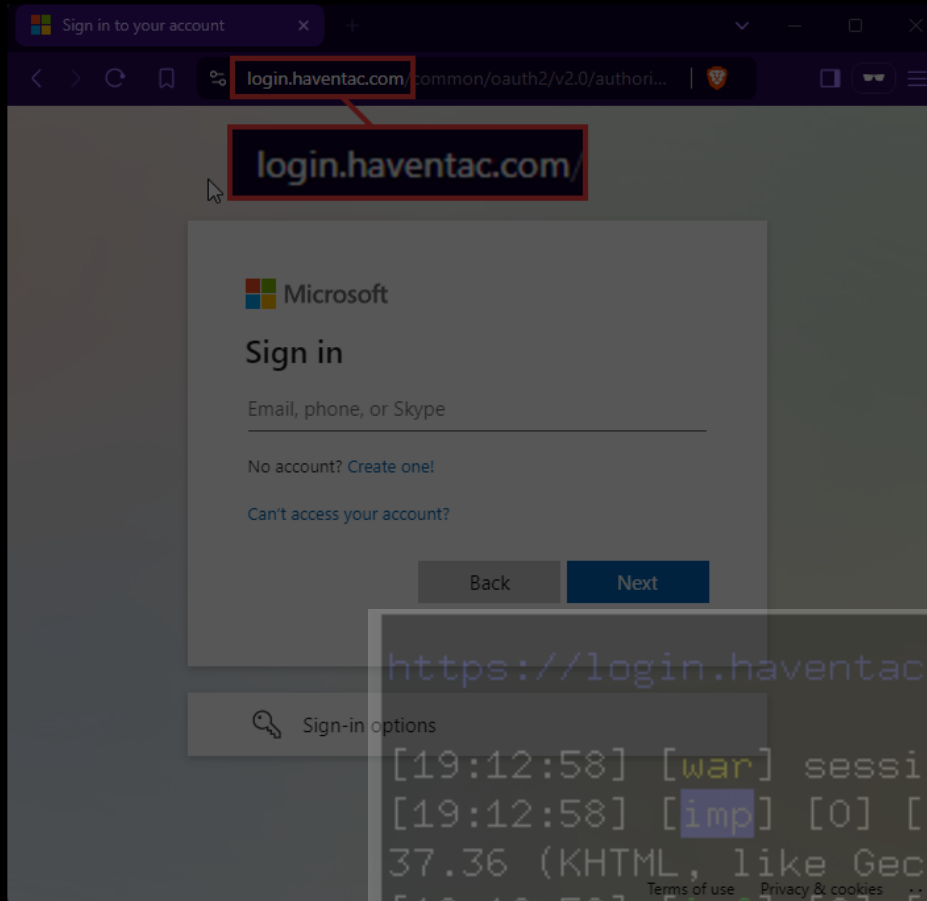
Anatomy of a Business Email Compromise

#3: User visits malicious M365 login



Anatomy of a Business Email Compromise

#3: User visits malicious M365 login



M365 IAM:

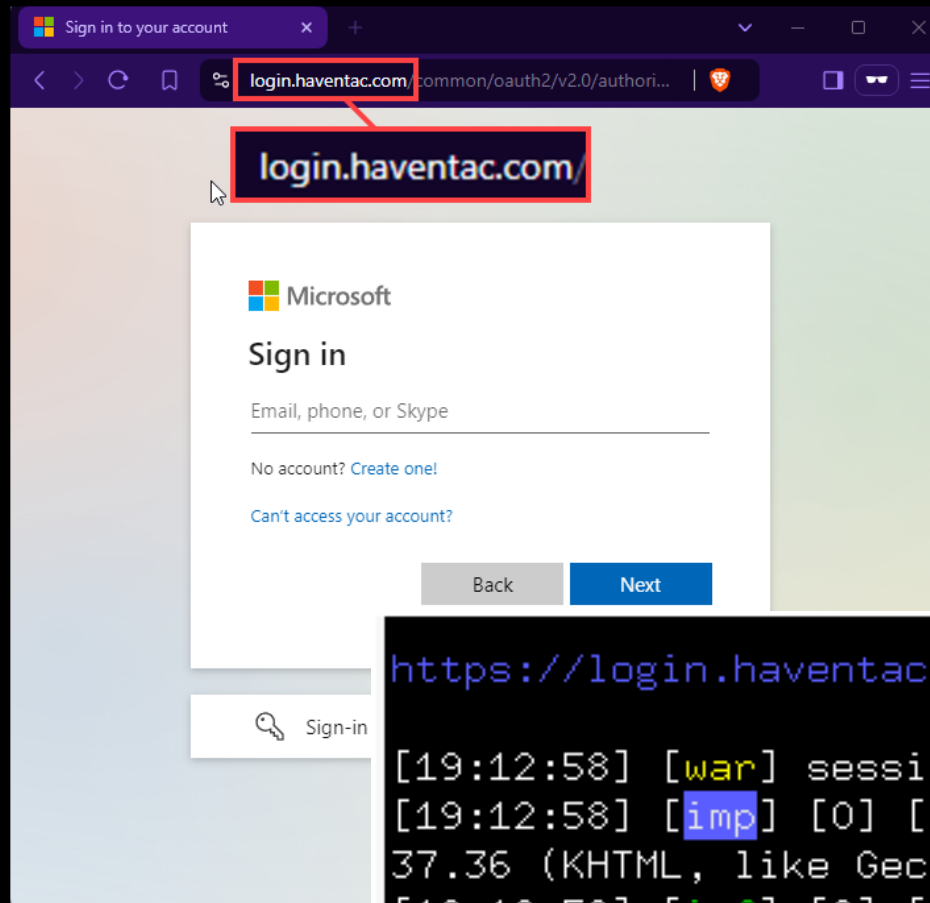
- a. Username/PW
- b. Device/Browser (User-Agent)
- c. MFA/Device
- d. Session Cookie
- e. Source IP

https://login.haventac.com/ppcIwpKL

```
[19:12:58] [war] session cookie not found: https://login.haventac.com/ppcIwpKL (1
[19:12:58] [imp] [0] [new-o365] new visitor has arrived: Mozilla/5.0 (Windows NT
37.36 (KHTML, like Gecko) Chrome/127.0.0.0 Safari/537.36 (172.221.112.235)
[19:12:58] [inf] [0] [new-o365] landing URL: https://login.haventac.com/ppcIwpKL
:
```

Anatomy of a Business Email Compromise

#3: User visits malicious M365 login

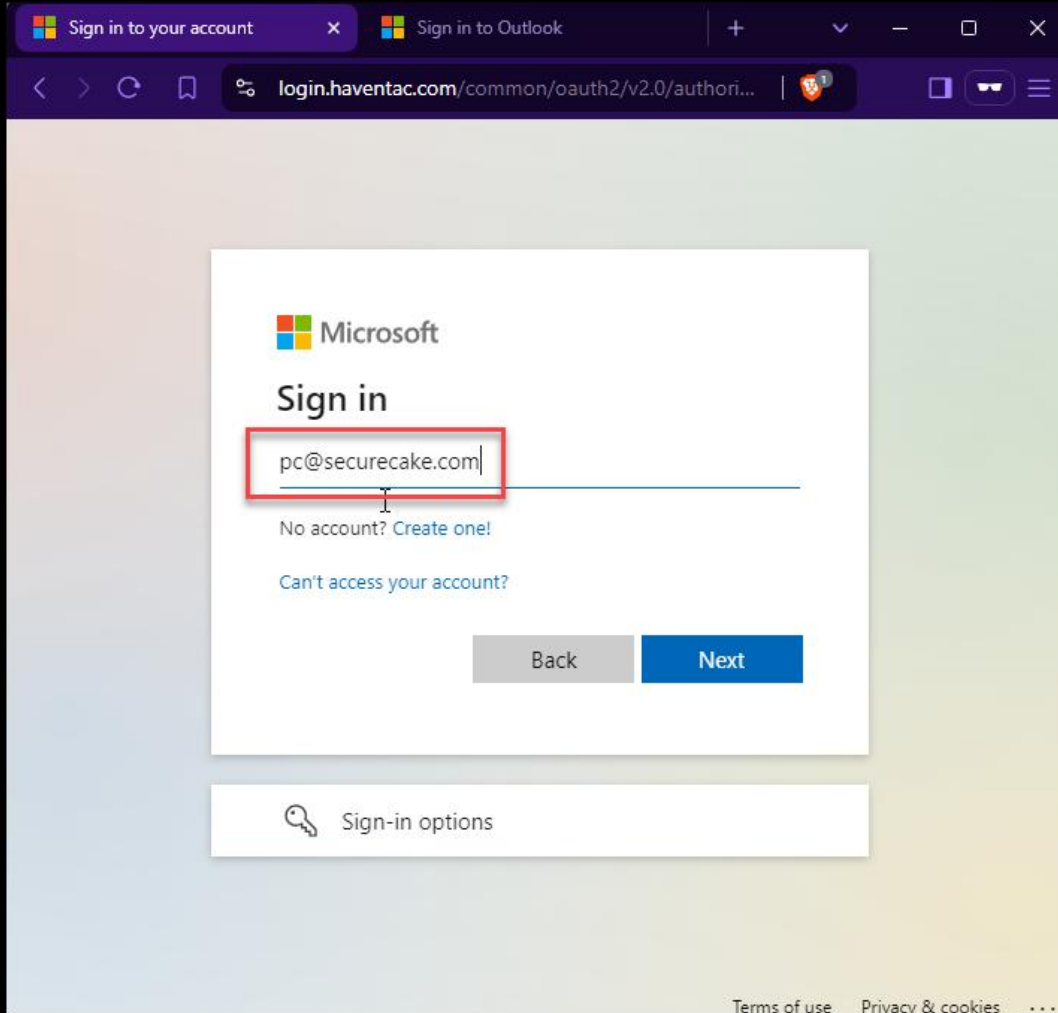


https://login.haventac.com/ppcIwpKL

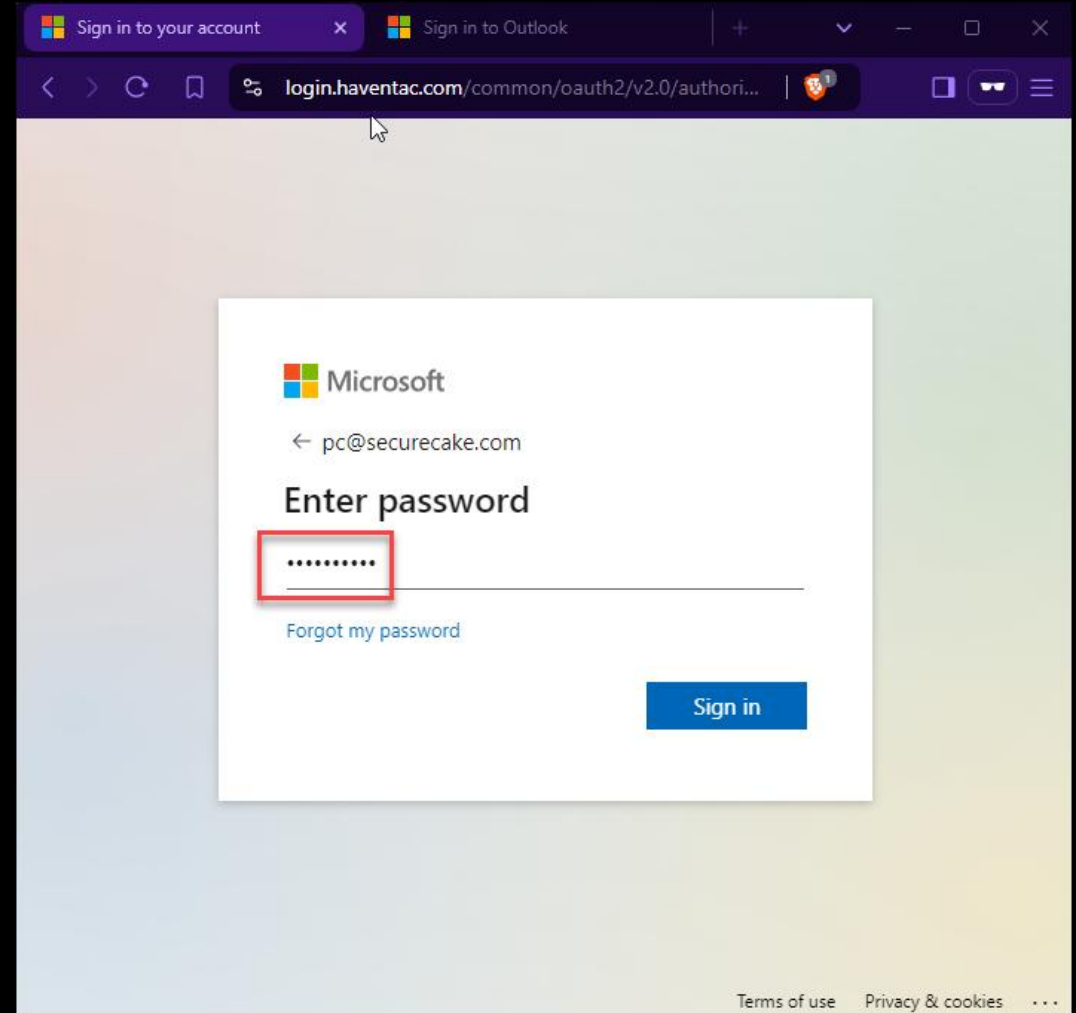
```
[19:12:58] [war] session cookie not found: https://login.haventac.com/ppcIwpKL (1
[19:12:58] [imp] [0] [new-o365] new visitor has arrived: Mozilla/5.0 (Windows NT
37.36 (KHTML, like Gecko) Chrome/127.0.0.0 Safari/537.36 (172.221.112.235)
[19:12:58] [inf] [0] [new-o365] landing URL: https://login.haventac.com/ppcIwpKL
: █
```

Anatomy of a Business Email Compromise

#4: User enters username and password



This screenshot shows the Microsoft sign-in page in a web browser. The browser's address bar displays the URL `login.haventac.com/common/oauth2/v2.0/authori...`. The page features the Microsoft logo and the heading "Sign in". A text input field contains the email address `pc@securecake.com`, which is highlighted by a red rectangular box. Below the input field, there are links for "No account? Create one!" and "Can't access your account?". At the bottom of the sign-in box are "Back" and "Next" buttons. A "Sign-in options" section is visible at the bottom of the page.



This screenshot shows the Microsoft sign-in page after the user has entered their username. The browser's address bar remains the same. The page now displays the heading "Enter password" and shows the email address `pc@securecake.com` with a back arrow. A password input field, represented by a series of dots and highlighted with a red rectangular box, is for the user to enter their password. Below the password field is a link for "Forgot my password". A "Sign in" button is located at the bottom right of the sign-in box. The "Sign-in options" section is no longer visible.

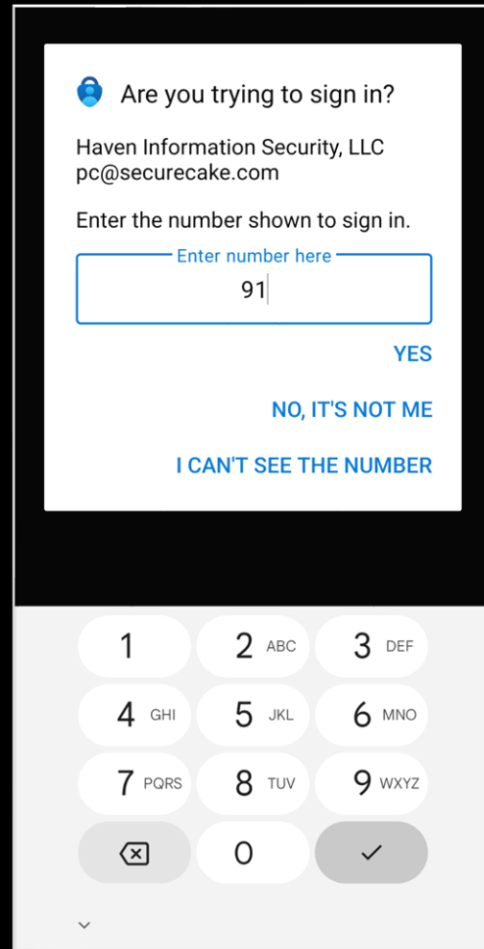
Anatomy of a Business Email Compromise

#5: “Evil proxy” captures username and password

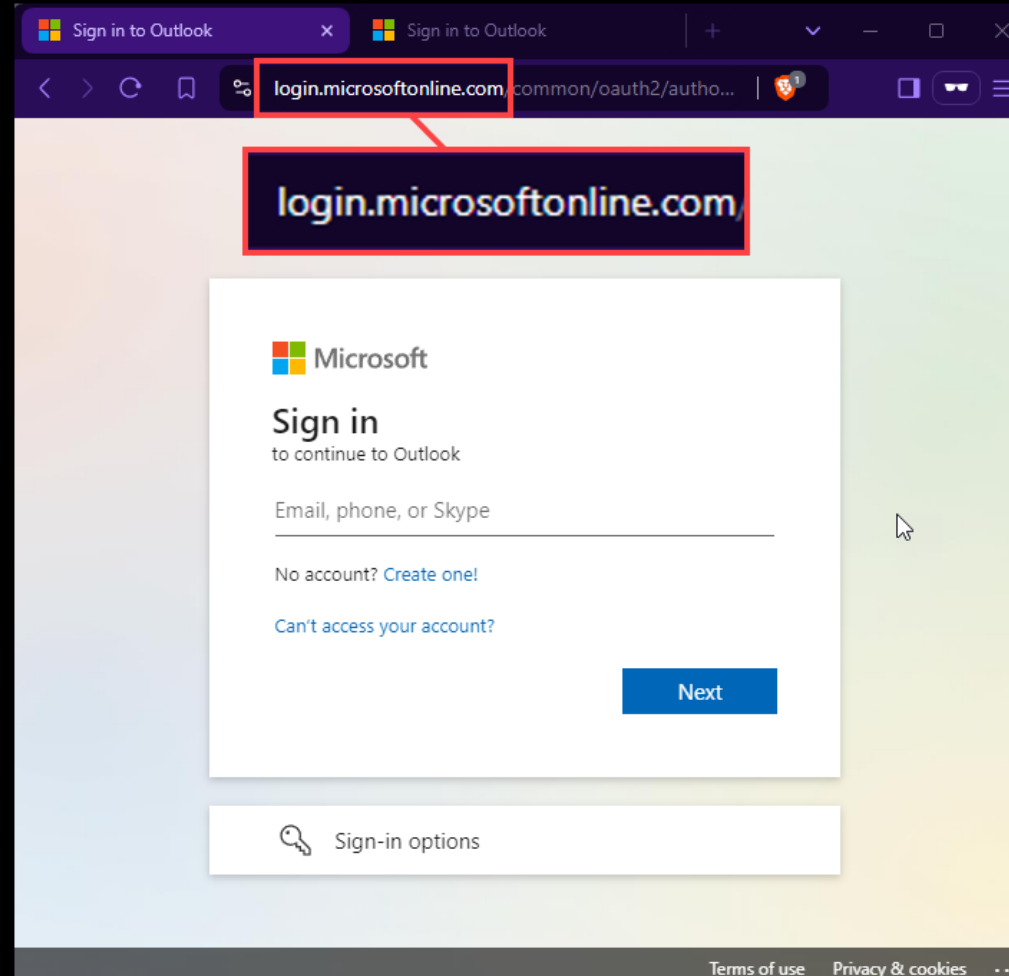
```
: lures get-url 0  
  
https://login.haventac.com/ppcIwpKL  
  
[19:12:58] [war] session cookie not found: https://login.haventac.com/ppcIwpKL (172.221.112.235) [new-o365]  
[19:12:58] [imp] [0] [new-o365] new visitor has arrived: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/127.0.0.0 Safari/537.36 (172.221.112.235)  
[19:12:58] [inf] [0] [new-o365] landing URL: https://login.haventac.com/ppcIwpKL  
[19:15:53] [+++] [0] Username: [pc@securecake.com]  
[19:15:53] [+++] [0] Username: [pc@securecake.com]  
[19:15:53] [+++] [0] Password: [Ns3cur3!?! ]  
: █
```

Anatomy of a Business Email Compromise

#6: If MFA is enforced, user is prompted to Approve/Deny and then redirected to legit M365 login portal



A mobile application screen for multi-factor authentication. At the top, it asks "Are you trying to sign in?" and identifies the user as "Haven Information Security, LLC" with email "pc@securecake.com". It prompts the user to "Enter the number shown to sign in." Below this is a text input field containing "91". At the bottom is a numeric keypad with buttons for digits 1-9, 0, a backspace icon, and a checkmark icon. Three links are visible: "YES", "NO, IT'S NOT ME", and "I CAN'T SEE THE NUMBER".



A screenshot of a web browser showing the Microsoft login portal. The address bar shows "login.microsoftonline.com" with a red box highlighting it. The page title is "Sign in to Outlook". The main content area has a "Sign in" heading followed by "to continue to Outlook". There is a text input field for "Email, phone, or Skype". Below this are links for "No account? Create one!" and "Can't access your account?". A blue "Next" button is at the bottom right. At the very bottom, there is a "Sign-in options" link with a key icon. The footer contains "Terms of use", "Privacy & cookies", and a menu icon.

Anatomy of a Business Email Compromise

#7: “Evil proxy” brokers auth from User to M365, capturing MFA session cookie

```
[19:17:29] [+++] [0] Username: [pc@securecake.com]
[19:17:30] [imp] [0] dynamic redirect to URL: https://outlook.office.com
[19:17:30] [+++] [0] detected authorization URL - tokens intercepted: /common/SAS/ProcessAuth
:
```

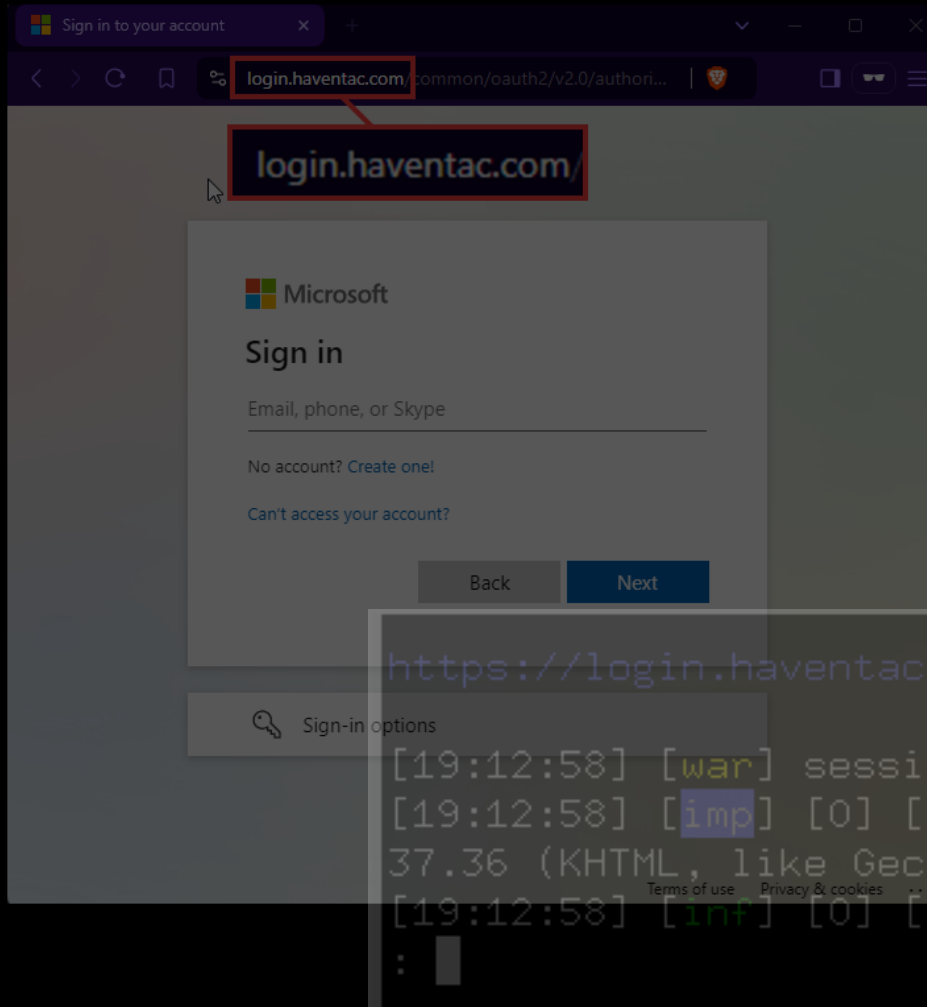
kali@kali: ~							
: sessions							
id	phishlet	username	password	tokens	remote ip	time	
20	new-o365	pc@securecake...	Ns3cur3!?!	captured	172.221.112.235	2024-08-21 19:17	

```
tokens      : captured
landing url  : https://login.haventac.com/ppcIwpKL
user-agent   : Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/127.0.0.0 Safari/537.36
remote ip    : 172.221.112.235
create time  : 2024-08-21 19:12
update time  : 2024-08-21 19:17

[ cookies ]
[{"path":"/", "domain":"login.microsoftonline.com", "expirationDate":1755805084, "value":"0.AVcAMe_N-B6jSkuT5F9XHpE1WltEZUfGMrBJg-Ydk3ZSdsobAAA.AgABFwQAAAAPtwJmzXqdR4BN2miheQMYAgDs_wUA9P9VnmIOYaT-BnmGhUsMA8dPnzLGN6YRGw1bH0sbsrPJE_ui9sRJRLQ1PqpJ91lMWzOpLIxFxmZQHZNcWaYHiEi3Fa9I9F9-r7016Gpb8zSZBBelthJmrERpLjfbKulmSM16p2_yDNCdbffeMbCC2tsr6Ai5FKkha0kiAHVvYi4Bct0hv01cUKktRP7-dVPLmkRfXDFd07Arv-FMPoTZf3in10-0Tx0hHa5WYN0xNRVchzdFFupK5T78TFoUw8026CiZh0lRC19
```

Anatomy of a Business Email Compromise

#1-7: Becoming the “User”



M365 IAM:

- a. Username/PW ✓
- b. Device/Browser (User-Agent) ✓
- c. MFA/Device ✓
- d. Session Cookie ✓
- e. Source IP

TEMPORAL PROXIMITY

Anatomy of a Business Email Compromise

#8: “Threat Actor” imports cookie into browser session to bypass auth and MFA and access User Mailbox

The image shows a terminal window on the left and a browser window on the right. The terminal displays the output of a command, showing a list of cookies. One cookie is highlighted with a red box and a red arrow pointing to the browser's Cookie-Editor - Import window. The browser window shows the login.microsoftonline.com page. The Cookie-Editor - Import window is open, showing the supported format (JSON, Header string, Netscape) and the cookie data: `zge0k5AB1qNQ", "name": "ESTSAUTHPERSISTENT", "httpOnly": true}`. The Import button is highlighted with a red box.

```
landing url : https://login.microsoftonline.com/...
user-agent  : Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
remote ip   : 172.221.112.235
create time : 2024-08-21 19:12
update time : 2024-08-21 19:17

[ cookies ]
[{"path":"/", "domain":"login.microsoftonline.com", "name":"ESTSAUTHPERSISTENT", "value":"zge0k5AB1qNQ", "httpOnly":true}, {"path":"/", "domain":"login.microsoftonline.com", "name":"ESTSAUTHPERSISTENT", "value":"zge0k5AB1qNQ", "httpOnly":true}]
```

Sign in to Outlook

login.microsoftonline.com/common/oauth2/authorize?client_id=00000000...

Cookie-Editor - Import v1.13.0

Supported format: JSON, Header string, Netscape.

`zge0k5AB1qNQ", "name": "ESTSAUTHPERSISTENT", "httpOnly": true}`

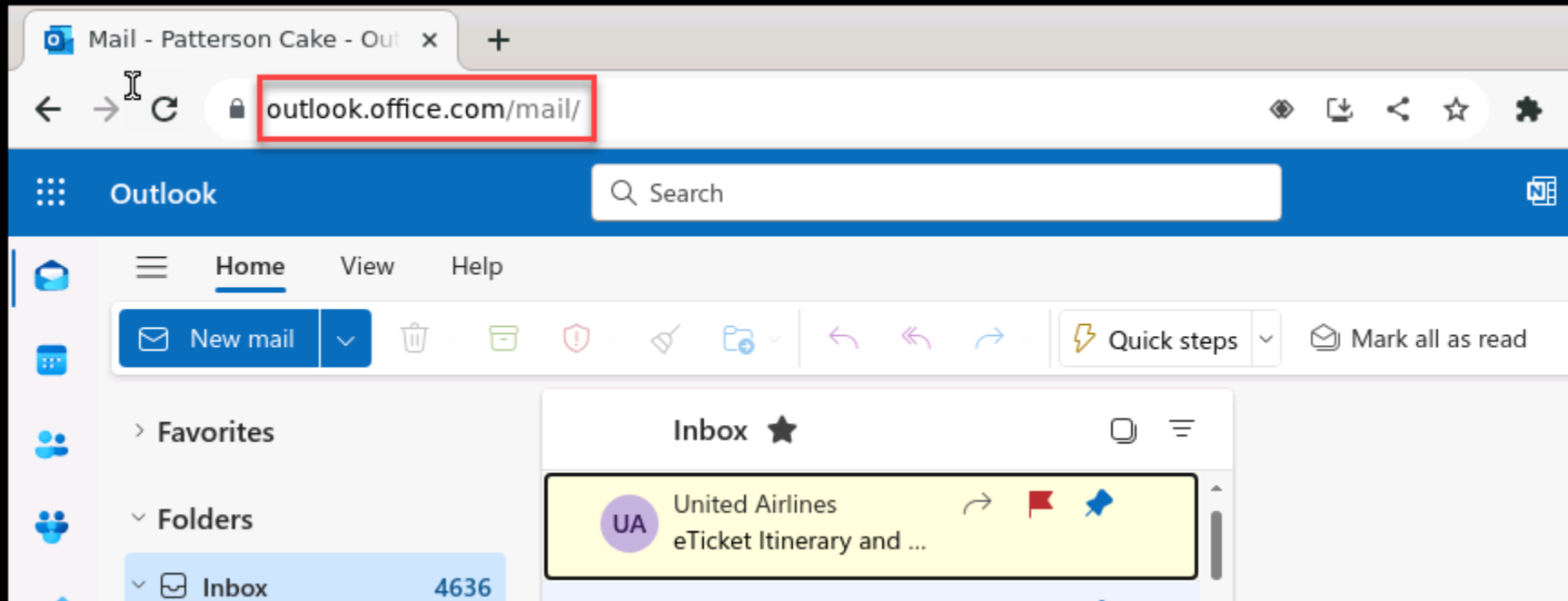
Import

Sign-in options

Terms of use Privacy & cookies

Anatomy of a Business Email Compromise

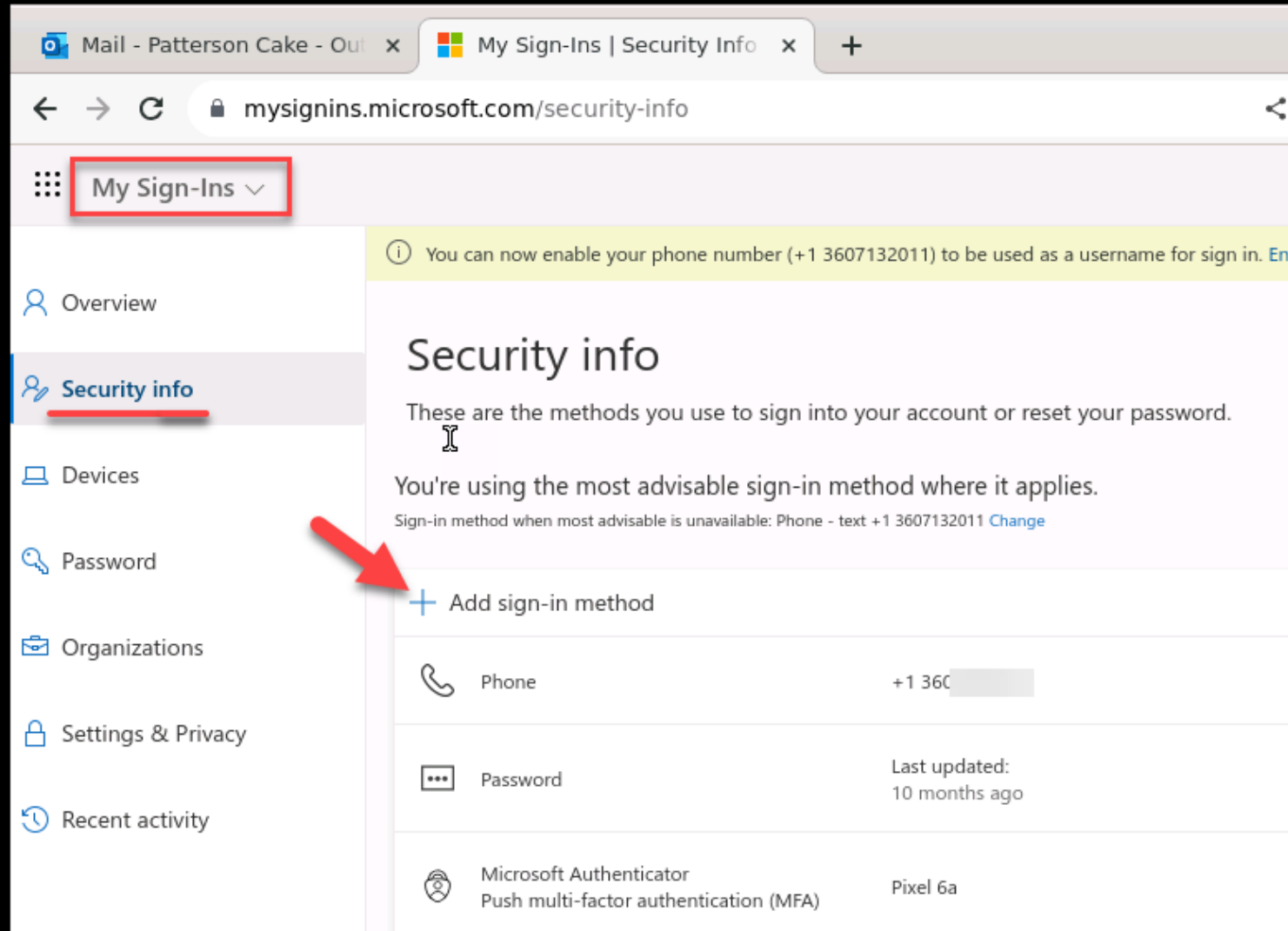
#9: “Threat Actor” has full access to M365 account/mailbox, without using username/pw or MFA!



[... SharePoint, OneDrive, Teams, VPN? ...]

Anatomy of a Business Email Compromise

#10: “Threat Actor” often adds a new MFA sign-in method to maintain **persistence** w/o session cookie

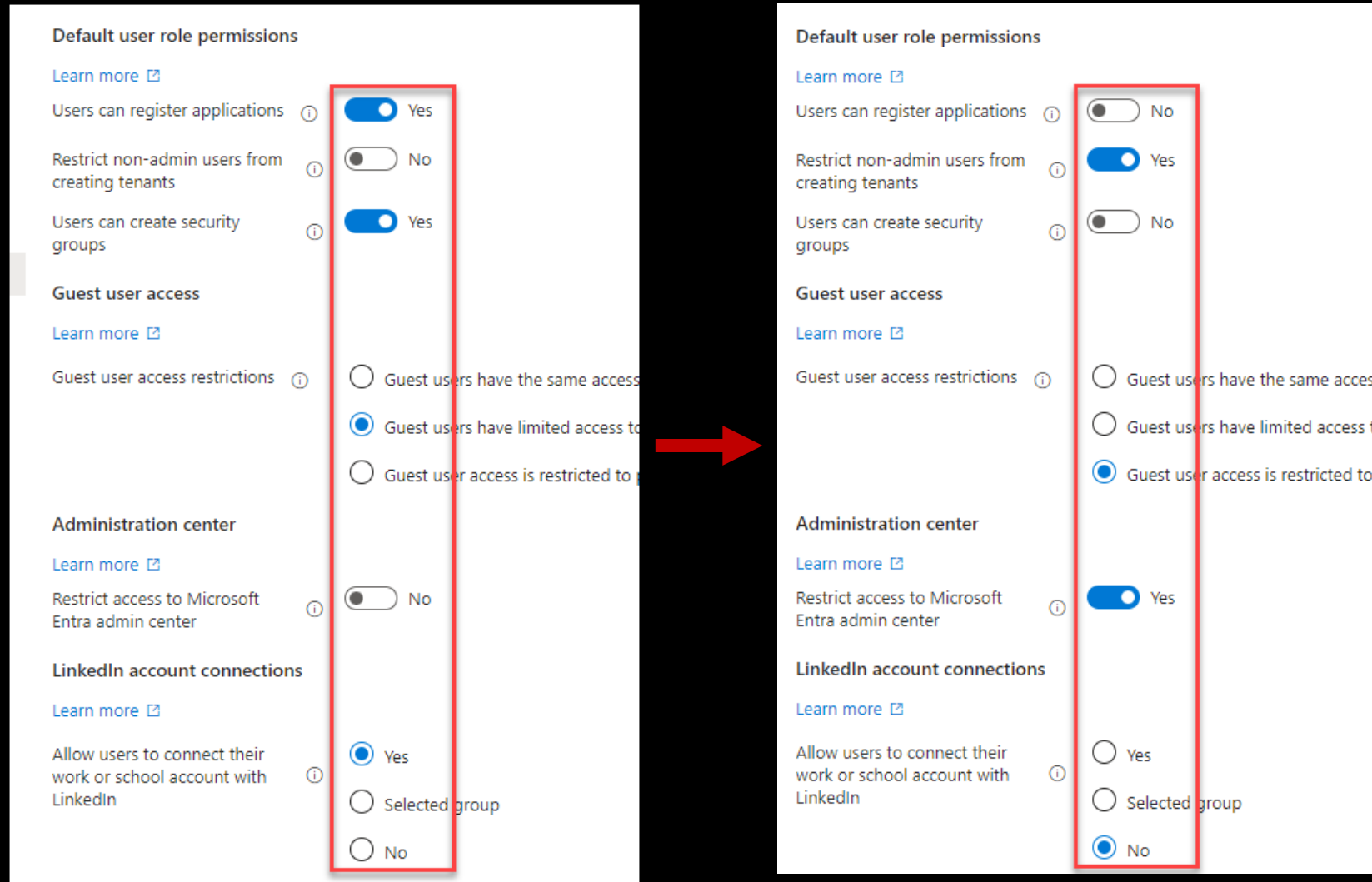


Anatomy of a Business Email Compromise

#11: “Threat Actor” searches/monitors mailbox looking for financial “opportunities:”

- Often observes for a few days to a couple of weeks
- Impersonates User to interact with business associates to redirect \$\$\$ via ACH, wire transfer, or account access [other staff, HR, accounts payable, vendors, etc.]
- Creates inbox-rules to redirect and hide unauthorized mail communications
- Pilfers M365 (email, SharePoint, OneDrive) looking for additional credentials
- Registers “Enterprise Applications” to maintain persistence of gain additional functionality, eg mailbox synchronization, M365 search, etc.
- Impersonates User to “Phish” established business relationships
- Rinse...wash...repeat...

M365 BEC HARDENING



Entra\Users\User Settings

Q&A

Patterson Cake

@SecureCake

github.com/secure-cake

patterson@blackhillsinfosec.com



[... blackhillsinfosec.com/blog ...]

Thank you!