NCU-ISAO

Evil Generation:

A Look at Adversary-in-the-Middle Phishing Services

TLP:GREEN

Presenter:

Brian Hinze – VP, Member Services & Operations at NCU-ISAO

This session is designated:

TLP:GREEN

TLP:GREEN = Limited disclosure, recipients can spread this within their community. Sources may use TLP:GREEN when information is useful to increase awareness within their wider community.

Recipients may share TLP:GREEN information with peers and partner organizations within their community, but not via publicly accessible channels. TLP:GREEN information may not be shared outside of the community.

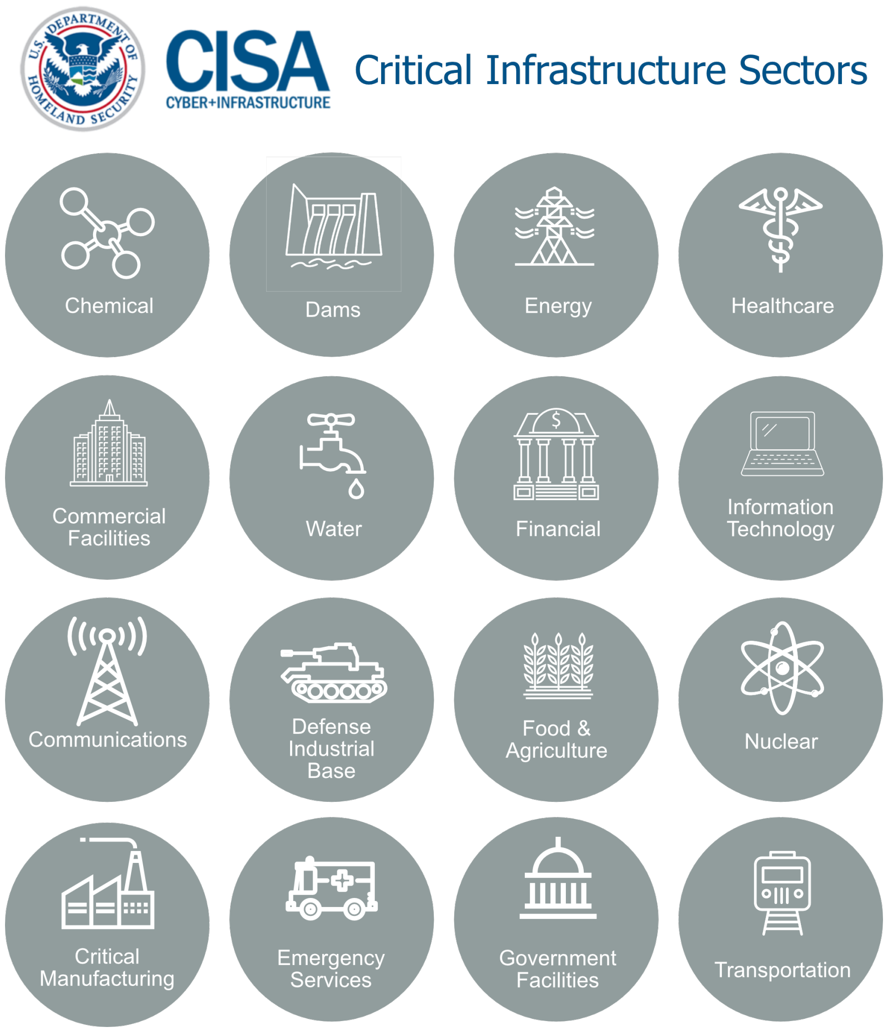
Note: when "community" is not defined, assume the cybersecurity/defense community.

A Quick History of the NCU-ISAO…

Enabled by the **CISA Act of 2015**, the NCU-ISAO began in concept with a credit union specific call to help lead credit unions to **cyber resilience…**

A collaboration of Credit Unions, CUSOs, and Leagues

- Help navigate the flooded waters of threat intelligence and alerts.
- Focus on credit union-specific issues around operations, risk, compliance through information sharing and collaboration.



About me…

Brian Hinze is the VP, Member Services & Operations, and serves as a Director and Treasurer for the NCU-ISAO.

I am responsible for overseeing the organizational operations and acting as the primary liaison for its members, leadership and working groups, as well as new member development.

I am committed to the success of the organization’s members and their journey to cyber resilience.

He joined the organization shortly after its inception and have 20 years of experience participating in and leading member associations, both in non-profit and advocating with regional trade associations in for-profit industry.

Session Overview

NCU-ISAO

Background

- Overview of a real attack on a credit union
- How it works - Adversary-in-the-Middle
- Frame-by-Frame Example Using EvilGinx

A Popular Trio: AiTM-as-a-Service

- EvilGinx
- EvilProxy
- Greatness

Countermeasures, Mitigations, Incident Response

Q&A

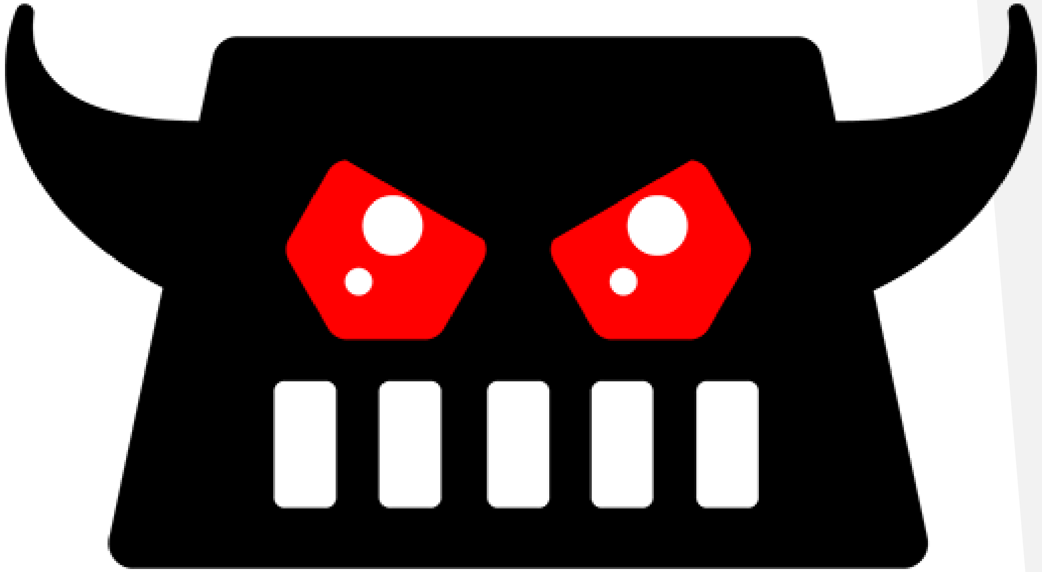


Image source: https://breakdev.org/evilginx-2-next-generation-of-phishing-2fa-tokens/

TLP:GREEN

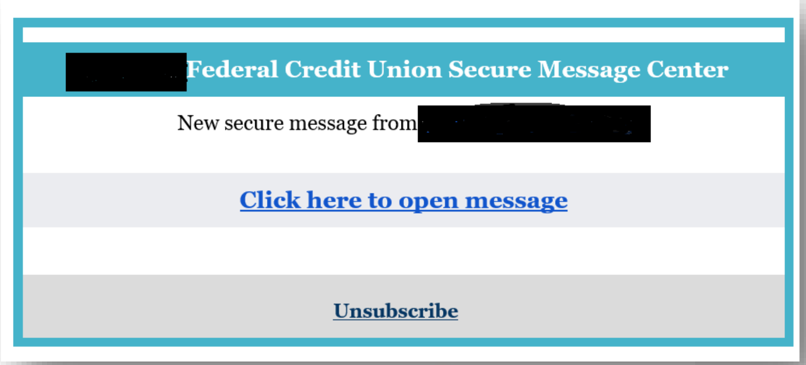
Background and Overview of an Attack Targeting Credit Unions, Banks, and their Vendors

Threat Background: NCU-ISAO has been tracking "Adversary-in-the-Middle (AiTM)" stealers since 2022:

- Less sophisticated versions of this campaign go back to mid-2021, using just image files and compromised user accounts to purport to be a 'Secure Message', linking to a Microsoft-branded phishing page.

- We assume that widespread adoption of MFA by enterprises became a barrier to the success this campaign.

- The modern campaign was first seen in June 2022 and *continues into 2024* using legitimate infrastructure and encryption services.
    - **In July 2022, a victim credit union reported their account was accessed after opening an email from a known contact at another credit union, even though they had MFA enabled. How could that be? (See next slide)**
    - NCU-ISAO & IACI researched these attacks, while also receiving intelligence via a trusted partner channel.
    - Within a couple of days, as the attack spread across the credit unions, we identified the attack as being associated with newly emerging "adversary-in-the-middle" proxy attacks.

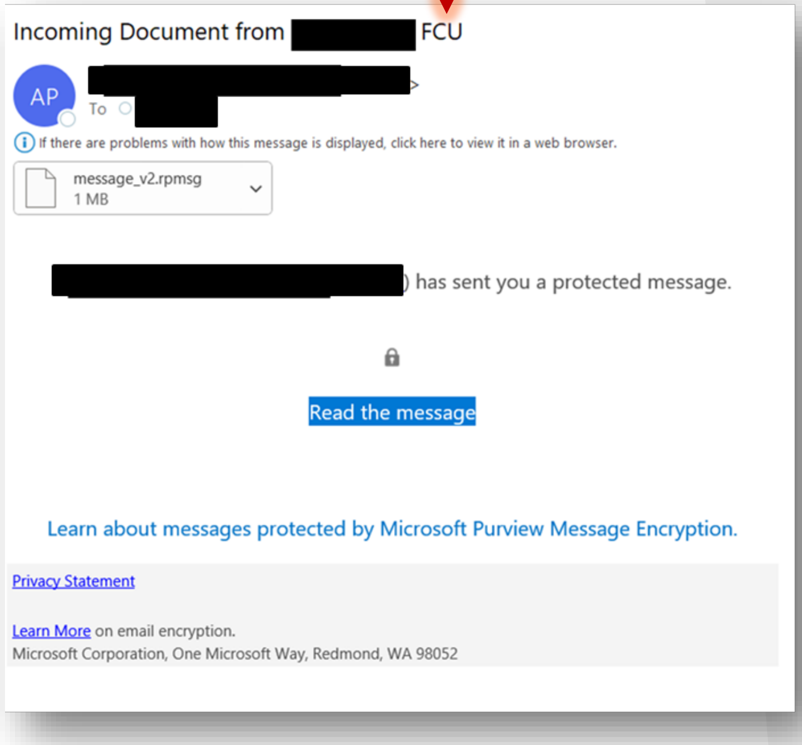


[redacted] Federal Credit Union Secure Message Center

New secure message from [redacted]

Click here to open message

Unsubscribe



Incoming Document from [redacted] FCU

[redacted] >

To ○ [redacted]

ⓘ If there are problems with how this message is displayed, click here to view it in a web browser.

message_v2.rpmsg
1 MB

[redacted]) has sent you a protected message.

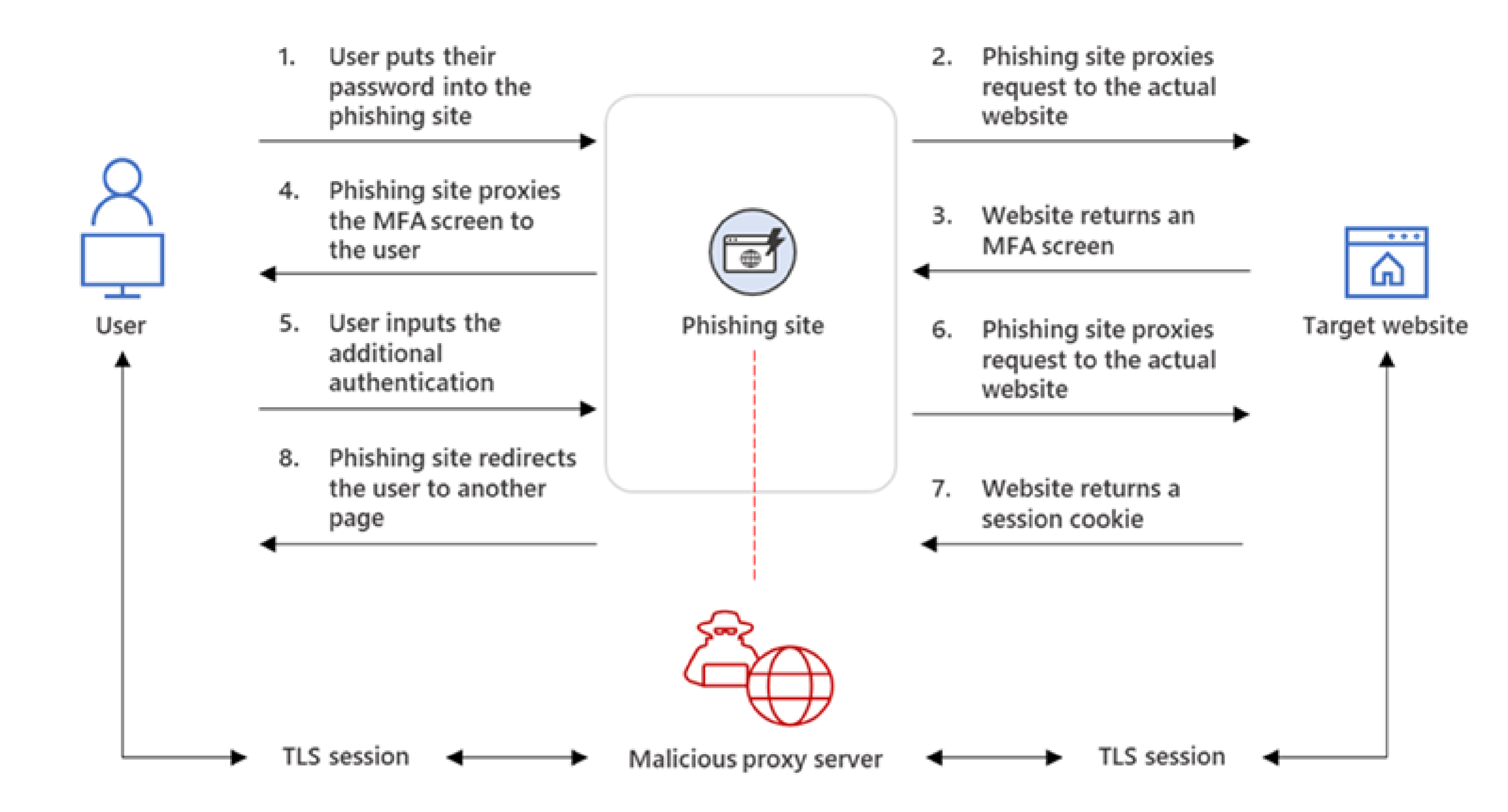
Learn about messages protected by Microsoft Purview Message Encryption.

Privacy Statement

Learn More on email encryption.
Microsoft Corporation, One Microsoft Way, Redmond, WA 98052

Enter: The “Adversary-in-the-Middle” Infrastructure:

- Traditional login page impersonation phishing pages only capture username and password.
- In AiTM phishing, attackers deploy a proxy server between a target user and the website the user wishes to visit (that is, the site the attacker wishes to impersonate).
- Such a setup allows the attacker to steal and intercept the target’s password and the session cookie that proves their ongoing and authenticated session with the website.
  - Stealing session cookies are the driving factor of AiTM attacks.
- Because our example is using proxied Microsoft logins, potential victims will even see their BRANDED login/password pages.



User

1. User puts their password into the phishing site
2. Phishing site proxies request to the actual website
3. Website returns an MFA screen
4. Phishing site proxies the MFA screen to the user
5. User inputs the additional authentication
6. Phishing site proxies request to the actual website
7. Website returns a session cookie
8. Phishing site redirects the user to another page

Phishing site

Target website

TLS session

Malicious proxy server

TLS session

Content & Image source: https://www.microsoft.com/en-us/security/blog/2022/07/12/from-cookie-theft-to-bec-attackers-use-aitm-phishing-sites-as-entry-point-to-further-financial-fraud/

TLP:GREEN

The Current Attack Pattern

Typical attack overview

1. CU Employee receives an email message from a Credit Union or vendor/industry partner with the subject line similar to but “Incoming Document From [Credit Union Name] or [Victim Name/Organization] e.g., XYZ Credit Union. Some novel variations observed.

    a. Messages observed may state that the message is encrypted, but it often is not.
    b. It is important to recognize through user training that they’ve been blind carbon copied (BCC’d), despite it being an “encrypted” message.

2. Clicking to view the ‘Encrypted Message,’ the victim is taken to a secondary malicious form at a visual form builder or other site builder where they are prompted to click to retrieve the message, which is where the actual link to the Microsoft phishing site is hosted.

    a. Hovering over the fake form/document link typically reveals a typo-squatted CU domain, customized by the adversary based on the compromised organization being spoofed.

3. If a victim opens the link, it will connect them to a malicious Microsoft login using either EvilProxy or EvilGinx to reverse proxy the connection to legitimate Microsoft login servers.

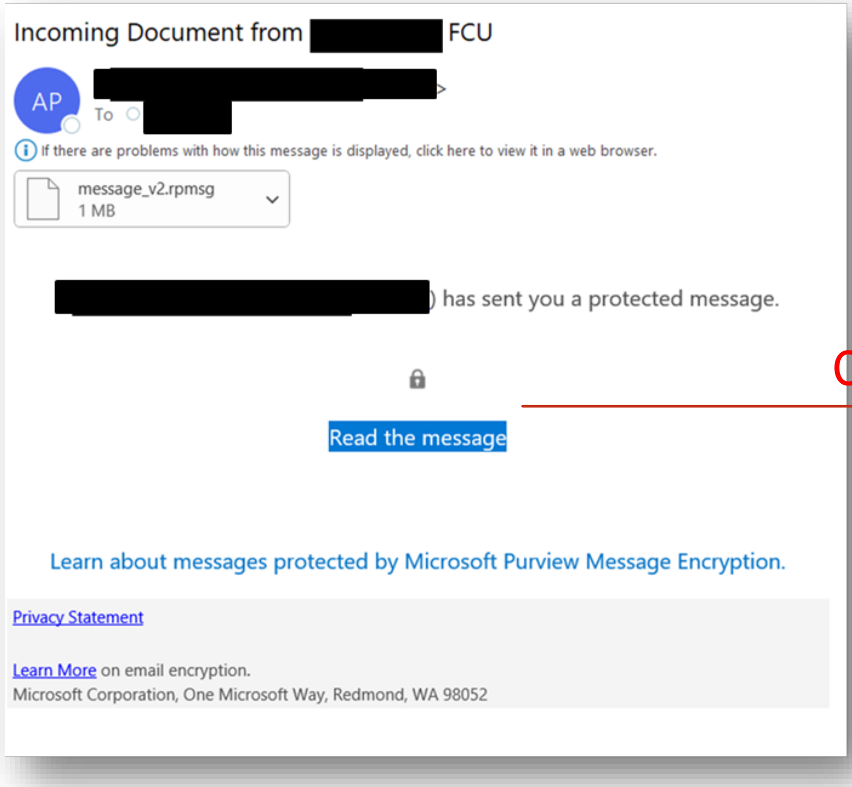
4. The now victim, enters their credentials that are stolen INCLUDING the authenticated session cookie, allowing the adversary to login remotely without needing MFA.

5. The adversary logs in to the victim’s online Outlook account, reads their emails, scrapes their contact list, and adds it to a cumulative list (see remediation below).

a. It is likely at this stage that reconnaissance is done to determine privileged users in an organization and other important details that may be used as pretexting for secondary campaigns.

6. A new site is established by threat actors is set up to impersonate the newly victimized CU and a new campaign is distributed to their contacts (or portions of a threat actor compiled master list), at which point the cycle above is repeated.

Going back to the attack…user receives a phishing email:



Incoming Document from [redacted] FCU

AP [redacted]>

To [redacted]

If there are problems with how this message is displayed, click here to view it in a web browser.

message_v2.rpmsg
1 MB

[redacted]) has sent you a protected message.

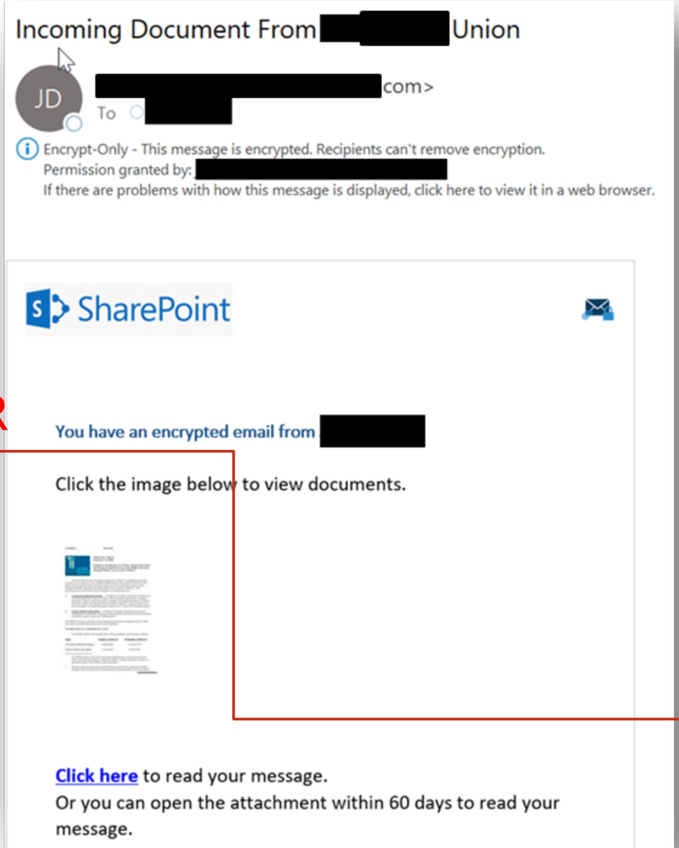
Read the message

Learn about messages protected by Microsoft Purview Message Encryption.

Privacy Statement

Learn More on email encryption.
Microsoft Corporation, One Microsoft Way, Redmond, WA 98052

OR



Incoming Document From [redacted] Union

JD [redacted]com>

To [redacted]

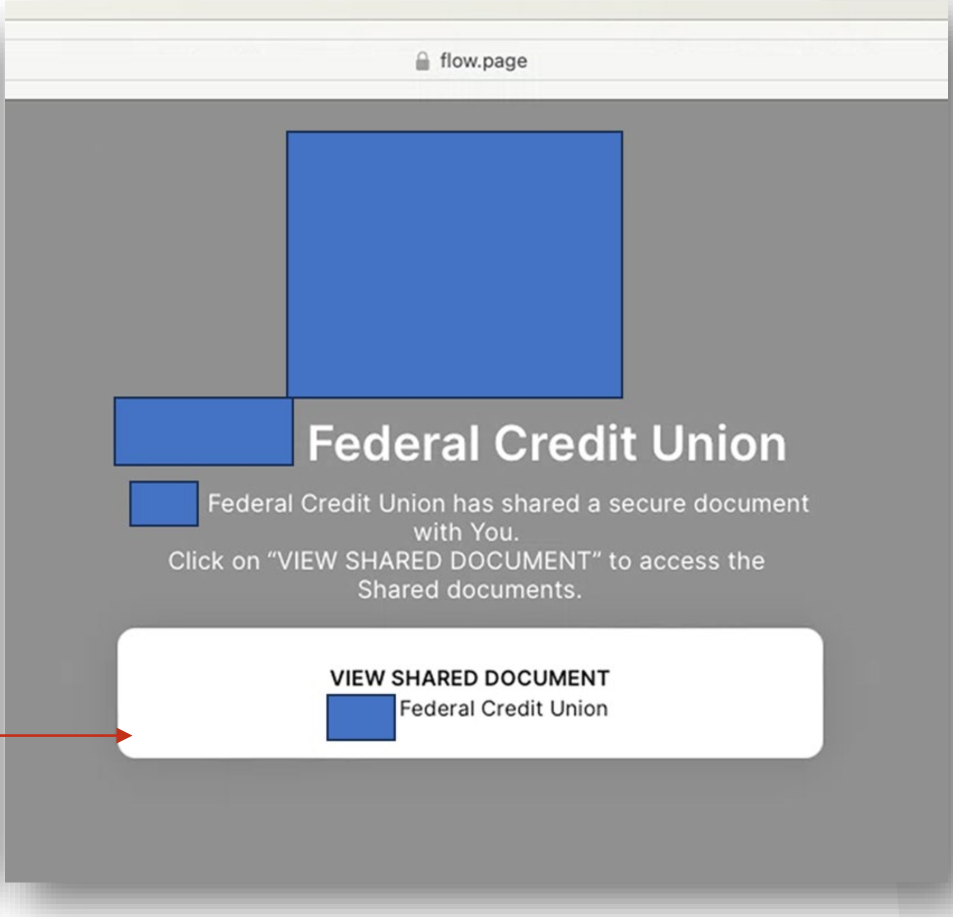
Encrypt-Only - This message is encrypted. Recipients can't remove encryption.
Permission granted by: [redacted]
If there are problems with how this message is displayed, click here to view it in a web browser.

SharePoint

You have an encrypted email from [redacted]

Click the image below to view documents.

Click here to read your message.
Or you can open the attachment within 60 days to read your message.



flow.page

[redacted]

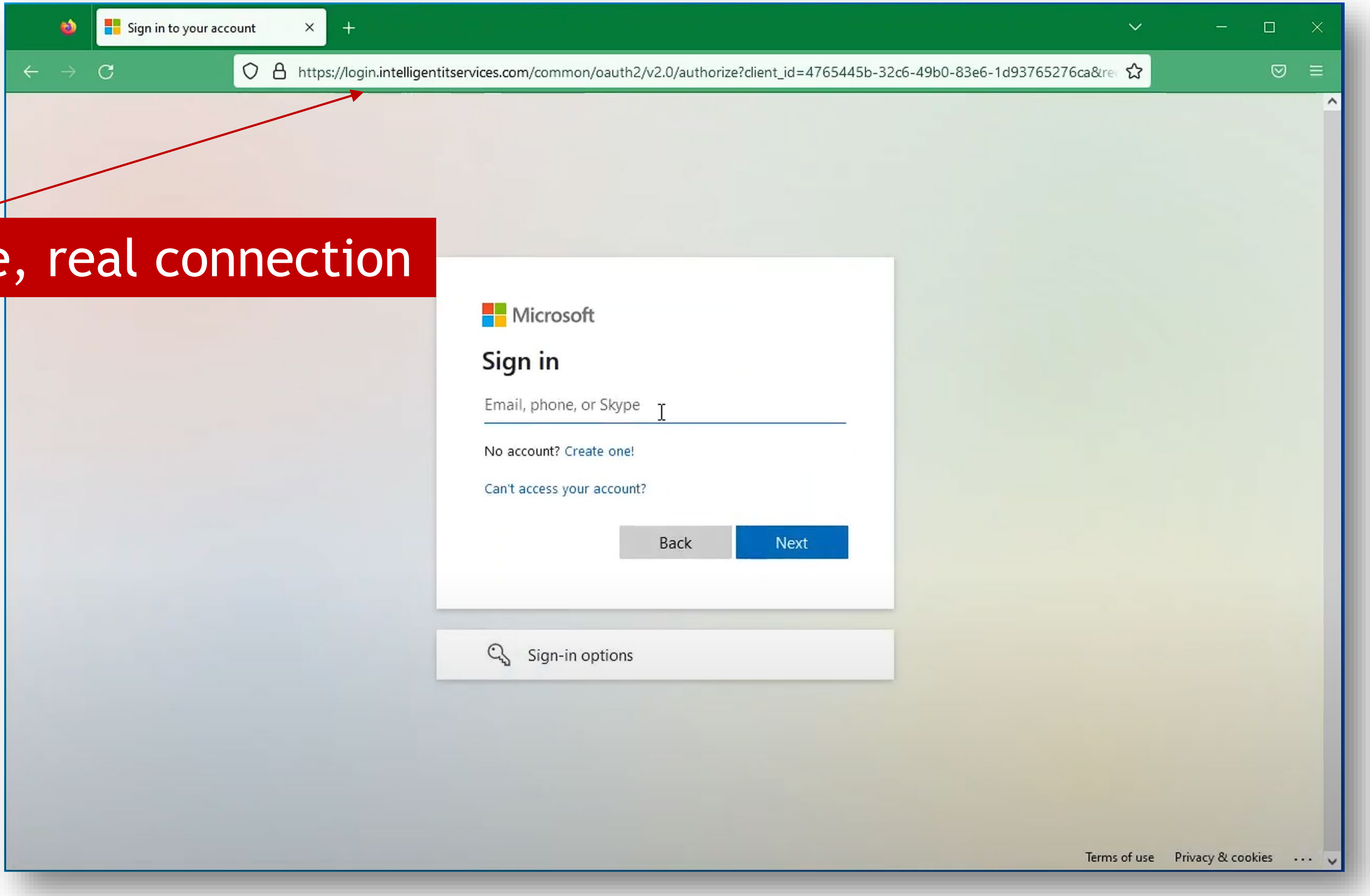
[redacted] Federal Credit Union

[redacted] Federal Credit Union has shared a secure document with You.
Click on "VIEW SHARED DOCUMENT" to access the Shared documents.

VIEW SHARED DOCUMENT
[redacted] Federal Credit Union

Screenshots of an attack (EvilGinx):

- Upon clicking the link inside, which is a URL loaded into the service that proxies a connection to Microsoft in this case:



Fake website, real connection

Sign in to your account

https://login.intelligentitservices.com/common/oauth2/v2.0/authorize?client_id=4765445b-32c6-49b0-83e6-1d93765276ca&re

Microsoft

Sign in

Email, phone, or Skype

No account? Create one!

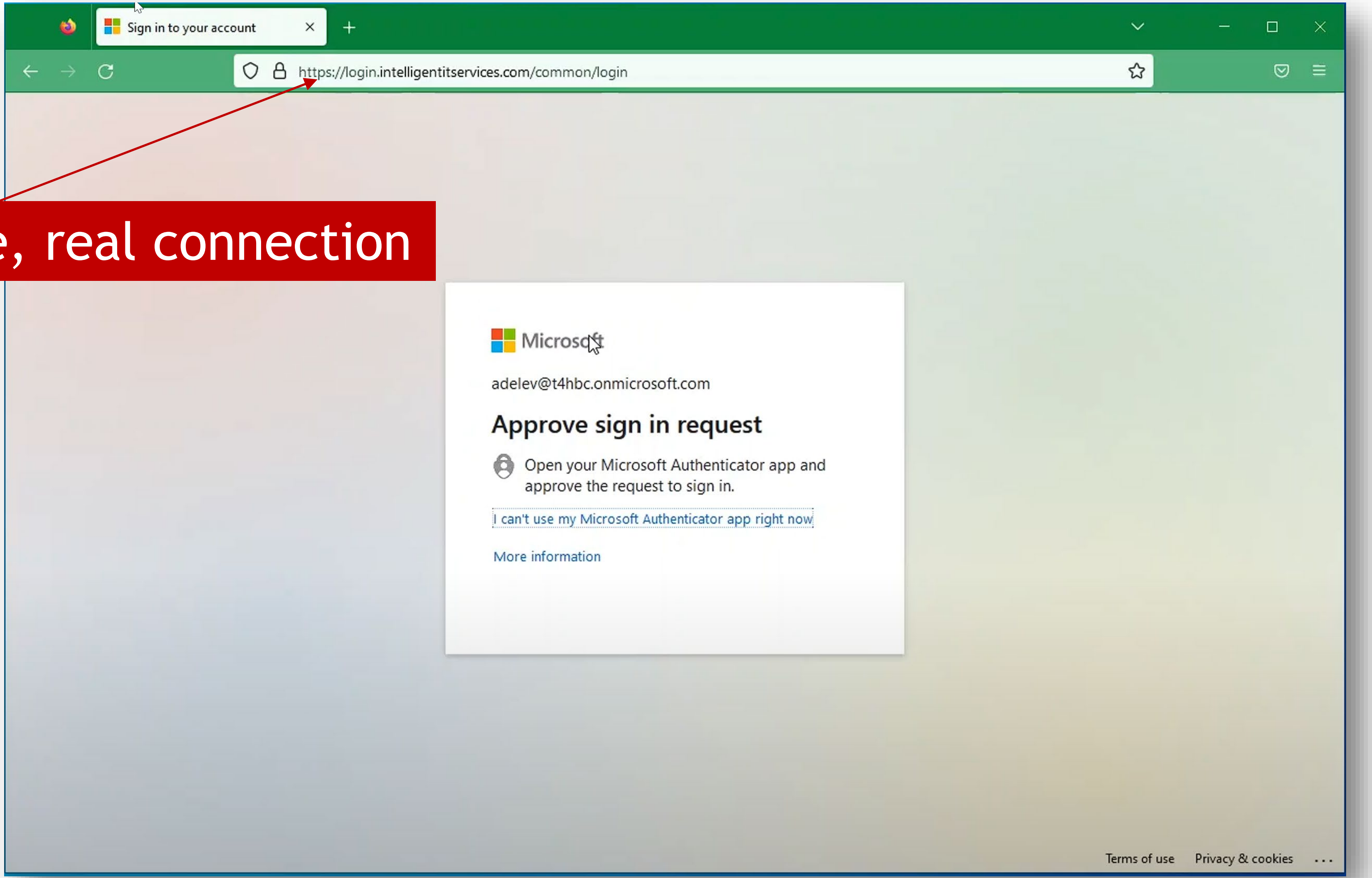
Can't access your account?

Image source: https://www.avertium.com/resources/threat-reports/mitm-attacks-evilproxy-and-evilginx/

TLP:GREEN

Screenshots of an attack (EvilGinx):

- Victim enters their Microsoft login information and is even prompted to authenticate using MS Authenticator, or whatever is linked to their AD account.
- NOTE: In some cases, especially in broader malspam campaigns, Base64 is used in the link to obfuscate the victim email and load the password or push to authenticator:


Sign in to your account
https://login.intelligentitservices.com/common/login
Microsoft
I can't use my Microsoft Authenticator app right now
More information
Terms of use
Privacy & cookies
...

adelev@t4hbc.onmicrosoft.com

Approve sign in request

Open your Microsoft Authenticator app and approve the request to sign in.

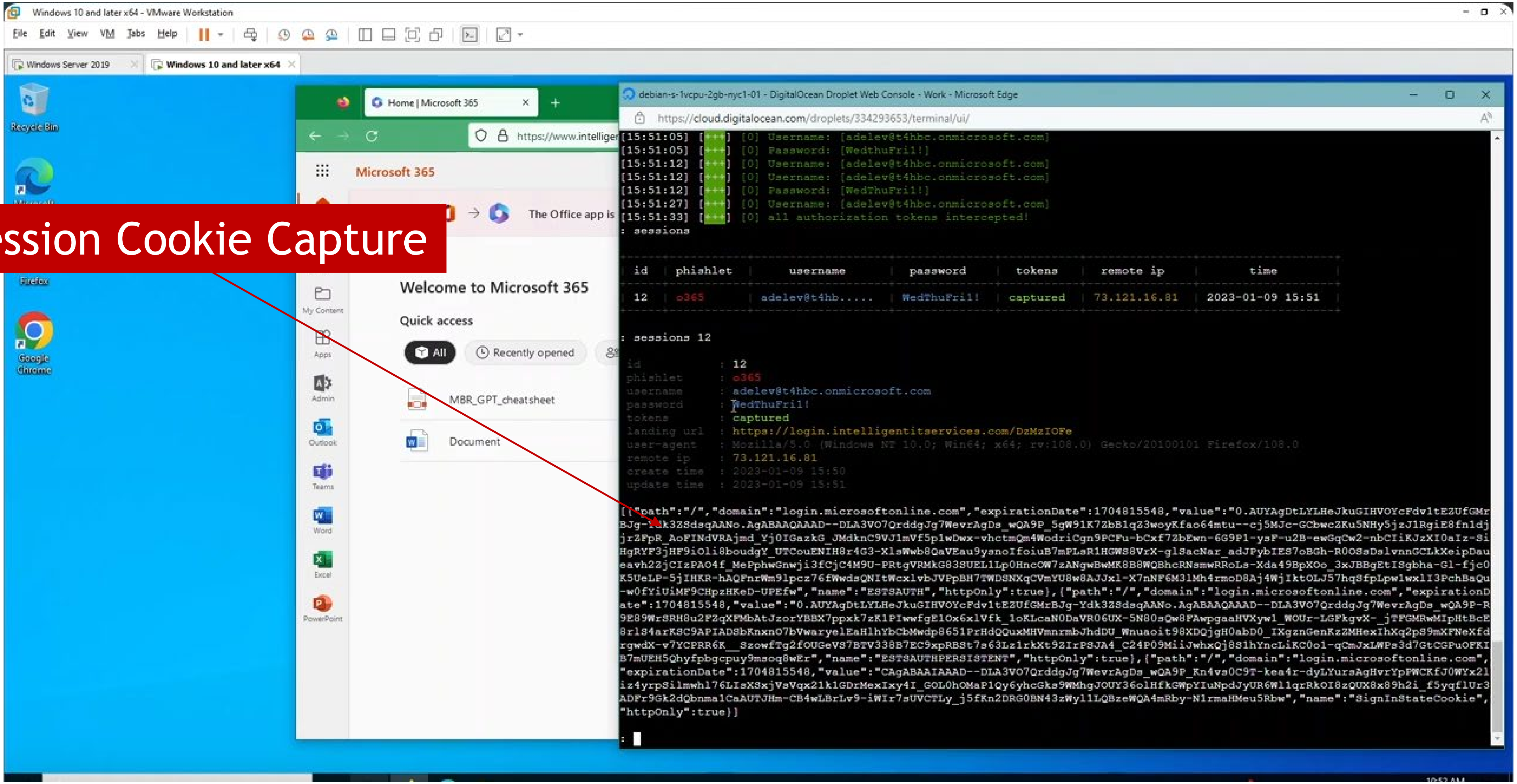
Fake website, real connection

Image source: https://www.avertium.com/resources/threat-reports/mitm-attacks-evilproxy-and-evilginx/

TLP:GREEN

Screenshots of an attack (EvilGinx):

- The EvilGinx panel on the attacker's end captures authentication information like username and password, or username if passwordless auth is uses, as well as the session cookie.



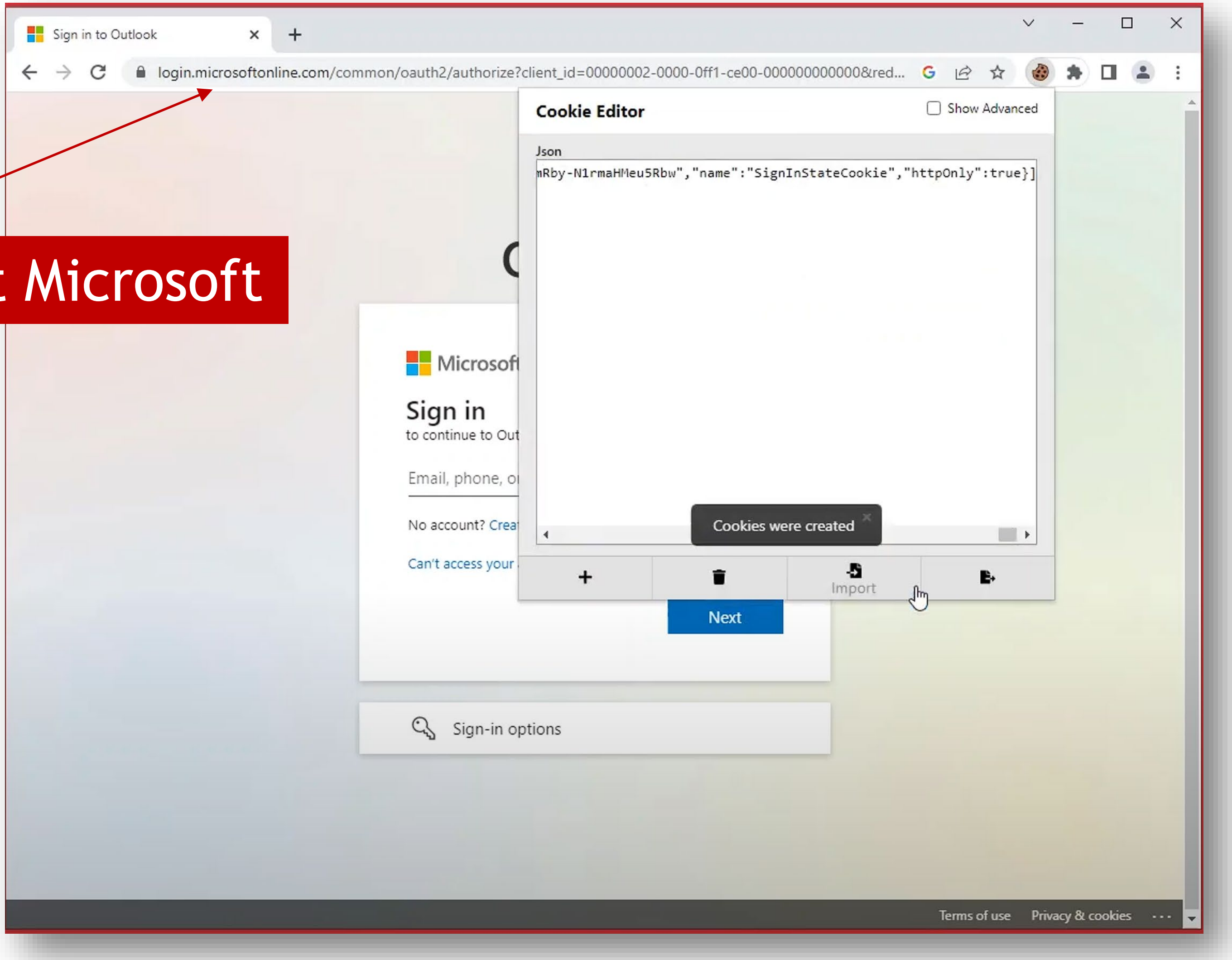
Session Cookie Capture

```
[15:51:05] [+++] [0] Username: [adelev@t4hbc.onmicrosoft.com]
[15:51:05] [+++] [0] Password: [WedthuFri1!]
[15:51:12] [+++] [0] Username: [adelev@t4hbc.onmicrosoft.com]
[15:51:12] [+++] [0] Username: [adelev@t4hbc.onmicrosoft.com]
[15:51:12] [+++] [0] Password: [WedThuFri1!]
[15:51:27] [+++] [0] Username: [adelev@t4hbc.onmicrosoft.com]
[15:51:33] [+++] [0] all authorization tokens intercepted!
: sessions

+----+----------+-----------------+-------------+----------+--------------+------------------+
| id | phishlet |    username     |  password   |  tokens  |  remote ip   |       time       |
+----+----------+-----------------+-------------+----------+--------------+------------------+
| 12 | o365     | adelev@t4hb.....| WedThuFri1! | captured | 73.121.16.81 | 2023-01-09 15:51 |
+----+----------+-----------------+-------------+----------+--------------+------------------+

: sessions 12

 id           : 12
 phishlet     : o365
 username     : adelev@t4hbc.onmicrosoft.com
 password     : WedThuFri1!
 tokens       : captured
 landing url  : https://login.intelligentitservices.com/DzMzIOFe
 user-agent   : Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:108.0) Gecko/20100101 Firefox/108.0
 remote ip    : 73.121.16.81
 create time  : 2023-01-09 15:50
 update time  : 2023-01-09 15:51

[{"path":"/","domain":"login.microsoftonline.com","expirationDate":1704815548,"value":"0.AUYAgDtLYLHeJkuGIHVOYcFdv1tEZUfGMr
BJg-Ydk3ZSdsqAANo.AgABAAQAAAD--DLA3VO7QrddgJg7WevrAgDs_wQA9P_5gW91K7ZbB1qZ3woyKfao64mtu--cj5MJc-GCbwcZKu5NHy5jzJ1RgiE8fn1dj
jrZFpR_AoFINdVRAjmd_Yj0IGazkG_JMdknC9VJ1mVf5p1wDwx-vhctmQm4WodriCgn9PCFu-bCxf7ZbEwn-6G9P1-ysF-u2B-ewGqCw2-nbCIiKJzXI0aIz-Si
HgRYF3jHF9iOli8boudgY_UTCouENIH8r4G3-XlsWwb8QaVEau9ysnoIfoiuB7mFLaR1HGW88VrX-gl8acNar_adJFybIES7oBGh-R0O8sDslvnnGCLkXeipDau
eavh2ZjCIzPAO4f_MePphwGnwji3fCjC4M9U-PRtgVRMkG83SUEL1Lp0HncOW7zANgwBwMK8B8WQBhcRNsmwRRoLs-Xda49BpXOo_3xJBBgEtI8gbha-Gl-fjc0
K5UeLP-5jIHKR-hAQFnrWm9lpcz76fWwdsQNItWcxlvbJVPpBH7TWDSNXqCVmYU8w8AJJxl-X7nNF6M31Mh4rmoD8Aj4WjIktOLJ57hqSfpLpwlwxlI3PchBaQu
-w0fYiUiMF9CHpzHKeD-UPEfw","name":"ESTSAUTH","httpOnly":true},{"path":"/","domain":"login.microsoftonline.com","expirationD
ate":1704815548,"value":"0.AUYAgDtLYLHeJkuGIHVOYcFdv1tEZUfGMrBJg-Ydk3ZSdsqAANo.AgABAAQAAAD--DLA3VO7QrddgJg7WevrAgDs_wQA9P-R
9E89WrSRH8u2FZqXFMbAtJzorYBBX7ppxk7zK1PIwwfgE1Ox6xlVfk_1oKLcaN0DaVR06UX-5N80sQw8FAwpgaaHVXywl_WOUr-LGFkgvX-_jTFGMRwMIpHtBcE
8rlS4arKSC9APIADSbKnxnO7bVwaryelEaHlhYbCbMwdp8651PrHdQQuxMHVmnrmbJhdDU_Wnuaoit98XDQjgH0abD0_IXgznGenKzZMHexIhXq2pS9mXFNeXfd
rgwdX-v7YCPRR6K__SzowfTg2fOUGeVS7BTV338B7EC9xpRBSt7s63Lz1rkXt9ZIrPSJA4_C24P09MiiJwhxQj8S1hYncLiKC0o1-qCmJxLWPs3d7GtCGPuOFKI
B7mUEH5Qhyfpbgcpuy9msoq8wEr","name":"ESTSAUTHPERSISTENT","httpOnly":true},{"path":"/","domain":"login.microsoftonline.com",
"expirationDate":1704815548,"value":"CAgABAAIAAAD--DLA3VO7QrddgJg7WevrAgDs_wQA9P_Kn4vs0C9T-kea4r-dyLYursAgHvrYpPWCKfJ0WYx2l
iz4yrpSilmwhl76LIsX8xjVsVqx21k1GDrMexIxy4I_GOL0hOMaP1Qy6yhcGks9WMhgJOUY36olHfkGWpYIuNpdJyUR6Wl1qrRkOI8zQUX8x89h2i_f5yqflUr3
ADFr9Gk2dQbnma1CaAUTJHm-CB4wLBrLv9-iWIr7sUVCTLy_j5fKn2DRG0BN43zWyl1LQBzeWQA4mRby-N1rmaHMeu5Rbw","name":"SignInStateCookie",
"httpOnly":true}]

: 
```

Image source: https://www.avertium.com/resources/threat-reports/mitm-attacks-evilproxy-and-evilginx/

Screenshots of an attack (EvilGinx):

- All login and session cookie information was captured during authentication, and now the attacker heads to outlook[.]office[.]com and is asked to log in, where they modify their session cookie to the previously authenticated one:



Attacker logs in at Microsoft

login.microsoftonline.com/common/oauth2/authorize?client_id=00000002-0000-0ff1-ce00-000000000000&red...

Cookie Editor

Json

```
mRby-N1rmaHMeu5Rbw","name":"SignInStateCookie","httpOnly":true}]
```

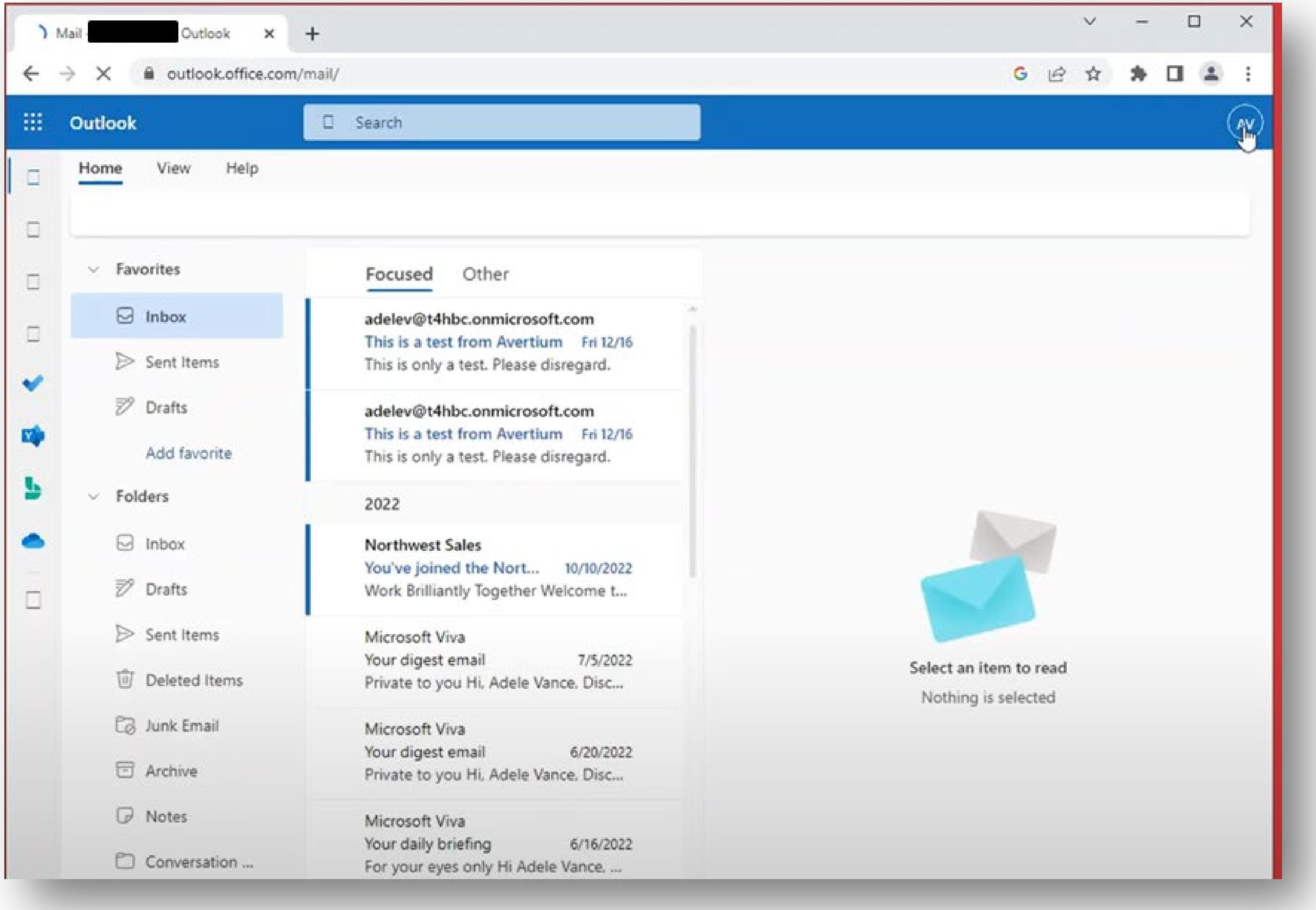
Cookies were created

Image source: https://www.avertium.com/resources/threat-reports/mitm-attacks-evilproxy-and-evilginx/

TLP:GREEN

Screenshots of an attack (EvilGinx):

- The attack is now in and able to read messages, send messages and scrape the victim's contacts to redistribute the campaign to new victims; in our case, other credit unions and their business partners, customers, etc.



adelev@t4hbc.onmicrosoft.com
This is a test from Avertium Fri 12/16
This is only a test. Please disregard.

adelev@t4hbc.onmicrosoft.com
This is a test from Avertium Fri 12/16
This is only a test. Please disregard.

2022

Northwest Sales
You've joined the Nort... 10/10/2022
Work Brilliantly Together Welcome t...

Microsoft Viva
Your digest email 7/5/2022
Private to you Hi, Adele Vance, Disc...

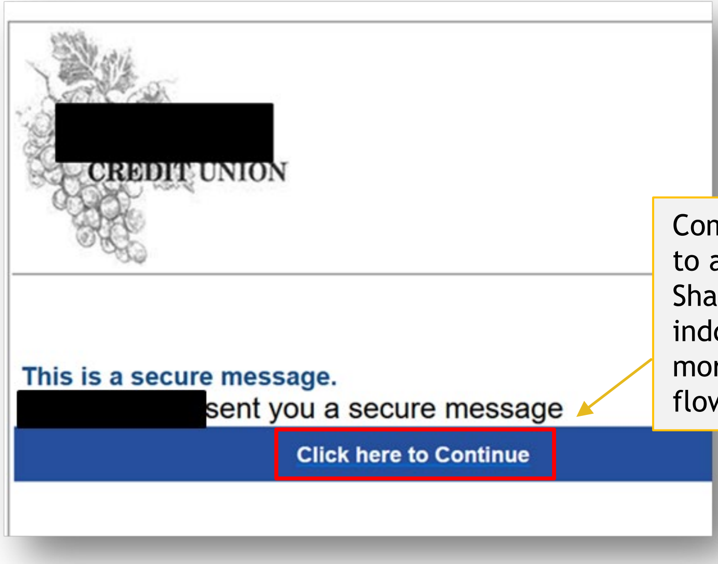
Microsoft Viva
Your digest email 6/20/2022
Private to you Hi, Adele Vance, Disc...

Microsoft Viva
Your daily briefing 6/16/2022
For your eyes only Hi Adele Vance, ...

Image source: https://www.avertium.com/resources/threat-reports/mitm-attacks-evilproxy-and-evilginx/

TLP:GREEN

Here's what happened (Microsoft example):



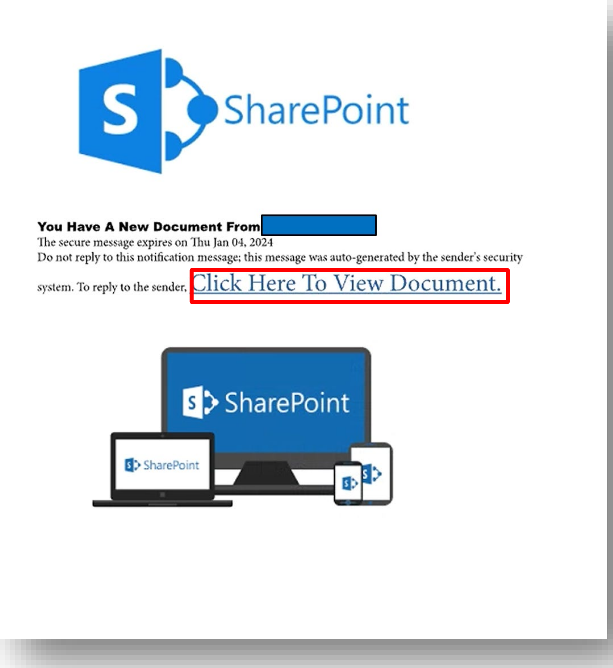
CREDIT UNION [redacted]

This is a secure message.

[redacted] sent you a secure message

Click here to Continue

Commonly linking to a fake SharePoint site on indd.adobe.com or more recently, flow.page.

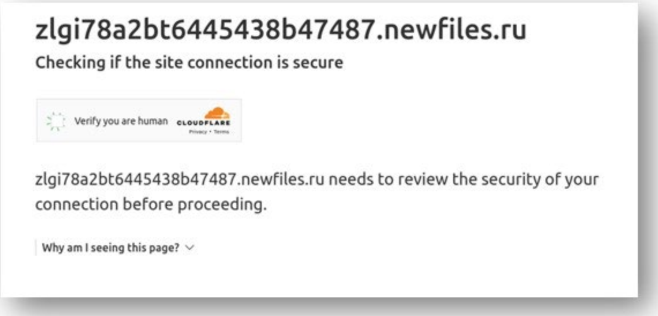


You Have A New Document From [redacted]

The secure message expires on Thu Jan 04, 2024

Do not reply to this notification message; this message was auto-generated by the sender's security system. To reply to the sender, Click Here To View Document.

Only if behind Cloudflare



zlgi78a2bt6445438b47487.newfiles.ru

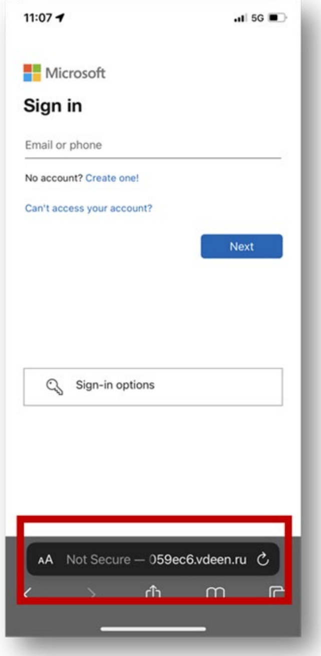
Checking if the site connection is secure

Verify you are human

zlgi78a2bt6445438b47487.newfiles.ru needs to review the security of your connection before proceeding.

Why am I seeing this page?

1. Phishing email
2. Hosted fake Adobe.com or SharePoint link to document
   - Abusing Legit Services
3. Cloudflare anti-bot (sometimes not present)
4. Proxied Microsoft login
5. Credential and session cookie capture by the AiTM service.



11:07 5G

Microsoft

Sign in

Email or phone

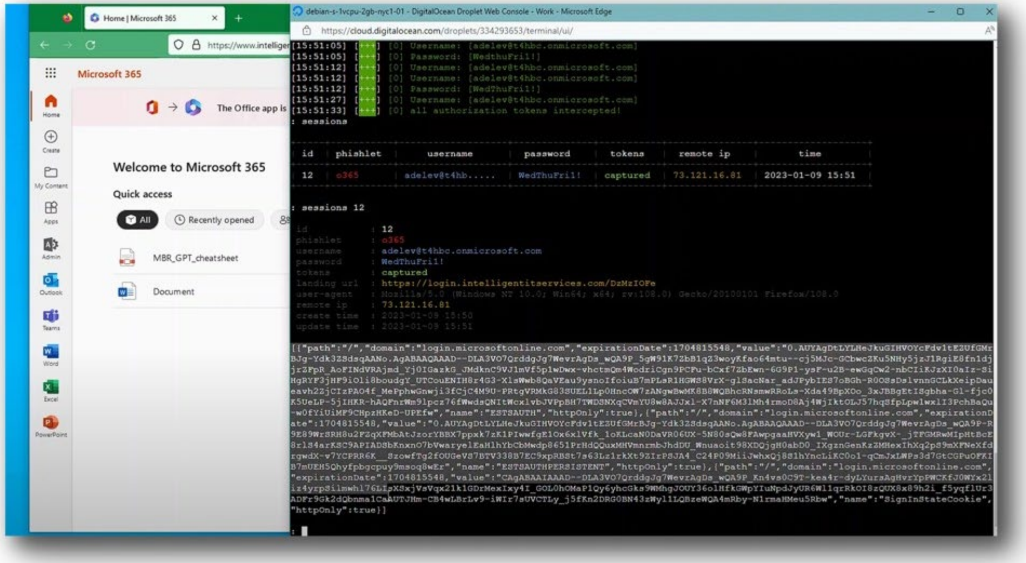
No account? Create one!

Can't access your account?

Next

Sign-in options

AA Not Secure — 059ec6.vdeen.ru



Home | Microsoft 365

https://www.intelliger

Microsoft 365

The Office app is

Welcome to Microsoft 365

Quick access

All | Recently opened

MBR_GPT_cheatsheet

Document

debian-s-1vcpu-2gb-nyc1-01 - DigitalOcean Droplet Web Console - Work - Microsoft Edge

https://cloud.digitalocean.com/droplets/334293653/terminal/ui/

```
[15:51:05] [+++] [0] Username: [adelev@t4hbc.onmicrosoft.com]
[15:51:05] [+++] [0] Password: [WedthuFri1!]
[15:51:12] [+++] [0] Username: [adelev@t4hbc.onmicrosoft.com]
[15:51:12] [+++] [0] Username: [adelev@t4hbc.onmicrosoft.com]
[15:51:12] [+++] [0] Password: [WedThuFri1!]
[15:51:27] [+++] [0] Username: [adelev@t4hbc.onmicrosoft.com]
[15:51:33] [+++] [0] all authorization tokens intercepted!
: sessions

+----+----------+----------------+-------------+----------+-------------+------------------+
| id | phishlet |    username    |  password   |  tokens  |  remote ip  |       time       |
+----+----------+----------------+-------------+----------+-------------+------------------+
| 12 | o365     | adelev@t4hb..... | WedThuFri1! | captured | 73.121.16.81 | 2023-01-09 15:51 |
+----+----------+----------------+-------------+----------+-------------+------------------+

: sessions 12

 id           : 12
 phishlet     : o365
 username     : adelev@t4hbc.onmicrosoft.com
 password     : WedThuFri1!
 tokens       : captured
 landing url  : https://login.intelligentitservices.com/DzMzIOFe
 user-agent   : Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:108.0) Gecko/20100101 Firefox/108.0
 remote ip    : 73.121.16.81
 create time  : 2023-01-09 15:50
 update time  : 2023-01-09 15:51
```

```
[{"path":"/","domain":"login.microsoftonline.com","expirationDate":1704815548,"value":"0.AUYAgDtLYLHeJkuGIHVOYcFdv1tEZUfGMr
BJg-Ydk3ZSdsqAANo.AgABAAQAAAD--DLA3VO7QrddgJg7WevrAgDs_wQA9P_5gW91K7ZbB1qZ3woyKfao64mtu--cj5MJc-GCbwcZKu5NHy5jzJ1RgiE8fn1dj
jrZFpR_AoFINdVRAjmd_Yj0IGazkG_JMdknC9VJ1mVf5p1wDwx-vhctmQm4WodriCgn9PCFu-bCxf7ZbEwn-6G9P1-ysF-u2B-ewGqCw2-nbCIiKJzXI0aIz-Si
HgRYF3jHF9iOli8boudgY_UTCouENIH8r4G3-XlsWwb8QaVEau9ysnoIfoiuB7mPLsR1HGWS8VrX-glSacNar_adJPybIES7oBGh-R0OSsDslvnnGCLkXeipDau
eavh2ZjCIzPAO4f_MePphwGnwji3fCjC4M9U-PRtgVRMkG83SUEL1Lp0HncOW7zANgwBwMK8B8WQBhcRNsmwRRoLs-Xda49BpXOo_3xJBBgEtISgbha-Gl-fjc0
K5UeLP-5jIHKR-hAQFnrWm9lpcz76fWwdsQNItWcxlvbJVPpBH7TWDSNXqCVmYU8w8AJJxl-X7nNF6M3lMh4rmoD8Aj4WjIktOLJ57hqSfpLpwlwxlI3PchBaQu
-w0fYiUiMF9CHpzHKeD-UPEfw","name":"ESTSAUTH","httpOnly":true},{"path":"/","domain":"login.microsoftonline.com","expirationD
ate":1704815548,"value":"0.AUYAgDtLYLHeJkuGIHVOYcFdv1tEZUfGMrBJg-Ydk3ZSdsqAANo.AgABAAQAAAD--DLA3VO7QrddgJg7WevrAgDs_wQA9P-R
9E89WrSRH8u2FZqXFMbAtJzorYBBX7ppxk7zK1PIwwfgE1Ox6xlVfk_1oKLcaN0DaVR06UX-5N80sQw8FAwpgaaHVXyw1_WOUr-LGFkgvX-_jTFGMRwMIpHtBcE
8rlS4arKSC9APIADSbKnxnO7bVwaryelEaHlhYbCbMwdp8651PrHdQQuxMHVmnrmbJhdDU_Wnuaoit98XDQjgH0abD0_IXgznGenKzZMHexIhXq2pS9mXFNeXfd
rgwdX-v7YCPRR6K__SzowfTg2fOUGeVS7BTV338B7EC9xpRBSt7s63Lz1rkXt9ZIrPSJA4_C24P09MiiJwhxQj8S1hYncLiKC0o1-qCmJxLWPs3d7GtCGPuOFKI
B7mUEH5Qhyfpbgcpuy9msoq8wEr","name":"ESTSAUTHPERSISTENT","httpOnly":true},{"path":"/","domain":"login.microsoftonline.com",
"expirationDate":1704815548,"value":"CAgABAAIAAAD--DLA3VO7QrddgJg7WevrAgDs_wQA9P_Kn4vs0C9T-kea4r-dyLYursAgHvrYpPWCKfJ0WYx21
iz4yrpSilmwhl76LIsXSxjVsVqx21k1GDrMexIxy4I_GOL0hOMaP1Qy6yhcGks9WMhgJOUY36olHfkGWpYIuNpdJyUR6Wl1qrRkOI8zQUX8x89h2i_f5yqflUr3
ADFr9Gk2dQbnma1CaAUTJHm-CB4wLBrLv9-iWIr7sUVCTLy_j5fKn2DRG0BN43zWyl1LQBzeWQA4mRby-N1rmaHMeu5Rbw","name":"SignInStateCookie",
"httpOnly":true}]
```

Post-compromise activity:

Once compromised, attackers log in to the victim’s email to:

- Read messages and identify targets or other sensitive information, which can be used in secondary pretexting attacks.
- Add alternate MFA to establish persistence and create inbox rules.
- Identify privileged users
  - Persistence is established by using “My Sign-ins” to add a new MFA method creating new employees/users, etc.
  - Attackers may also create new users (fake employees)
- Scrape contacts from the victim contact list – additionally, sector-specific contact lists appear to be compiled by attackers
- Redistribute the phishing attack to a new set of victims

If a privileged user is compromised,
you have an even bigger problem (a few examples):

- ***Creating new users & delegating mailbox access***
- ***Creating Mail-flow rules including hiding automatic replies***
- ***Creating Oauth tokens***
- ***Exposing sensitive information***

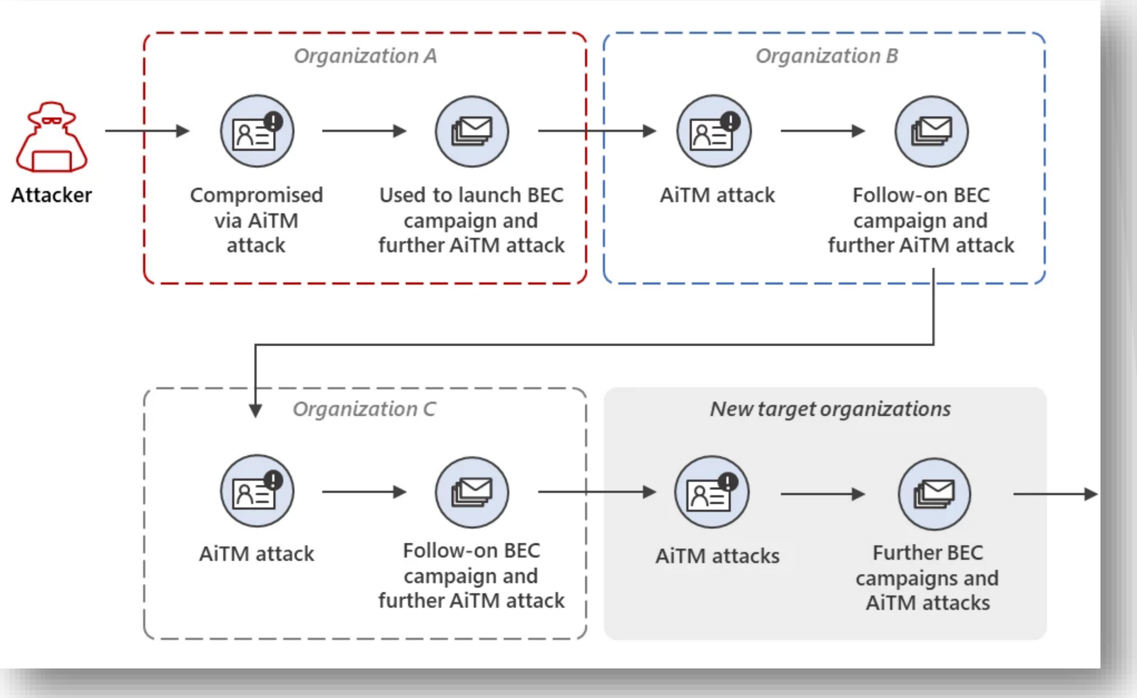

Attacker
Organization A
Compromised via AiTM attack
Used to launch BEC campaign and further AiTM attack
Organization B
AiTM attack
Follow-on BEC campaign and further AiTM attack
Organization C
AiTM attack
Follow-on BEC campaign and further AiTM attack
New target organizations
AiTM attacks
Further BEC campaigns and AiTM attacks

Image source: https://www.microsoft.com/en-us/security/blog/2023/06/08/detecting-and-mitigating-a-multi-stage-aitm-phishing-and-bec-campaign/

Hang on! Is this a vulnerability?

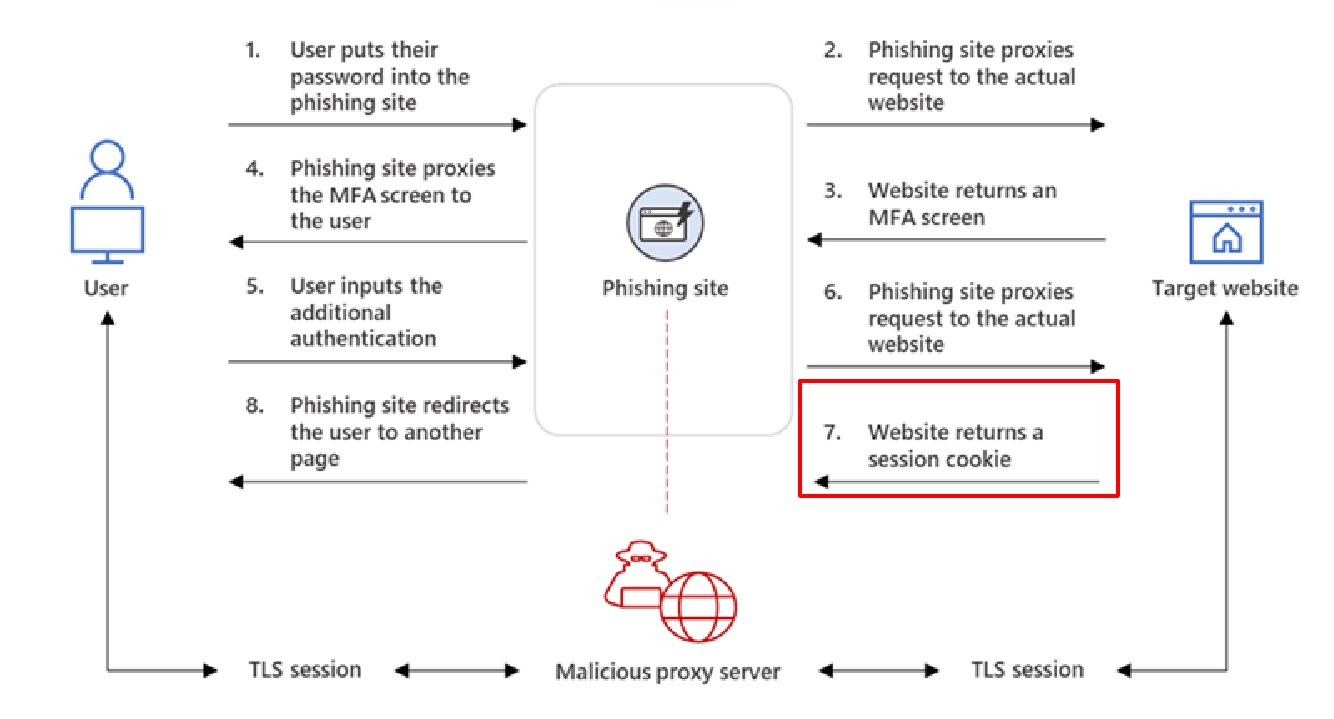
Microsoft says NO:

"In AiTM phishing, attackers deploy a proxy server between a target user and the website the user wishes to visit (that is, the site the attacker wishes to impersonate).

[The] setup allows the attacker to steal and intercept the target's password and the session cookie that proves their ongoing and authenticated session with the website.

…This is not a vulnerability in MFA; since AiTM phishing steals the session cookie, the attacker gets authenticated to a session on the user's behalf, regardless of the sign-in method the latter uses."

Additionally: The author of the EvilGinx framework claims, "Every sign-in page, requiring the user to provide their password, with any form of 2FA implemented, can be phished using this technique!"



1. User puts their password into the phishing site
2. Phishing site proxies request to the actual website
3. Website returns an MFA screen
4. Phishing site proxies the MFA screen to the user
5. User inputs the additional authentication
6. Phishing site proxies request to the actual website
7. Website returns a session cookie
8. Phishing site redirects the user to another page

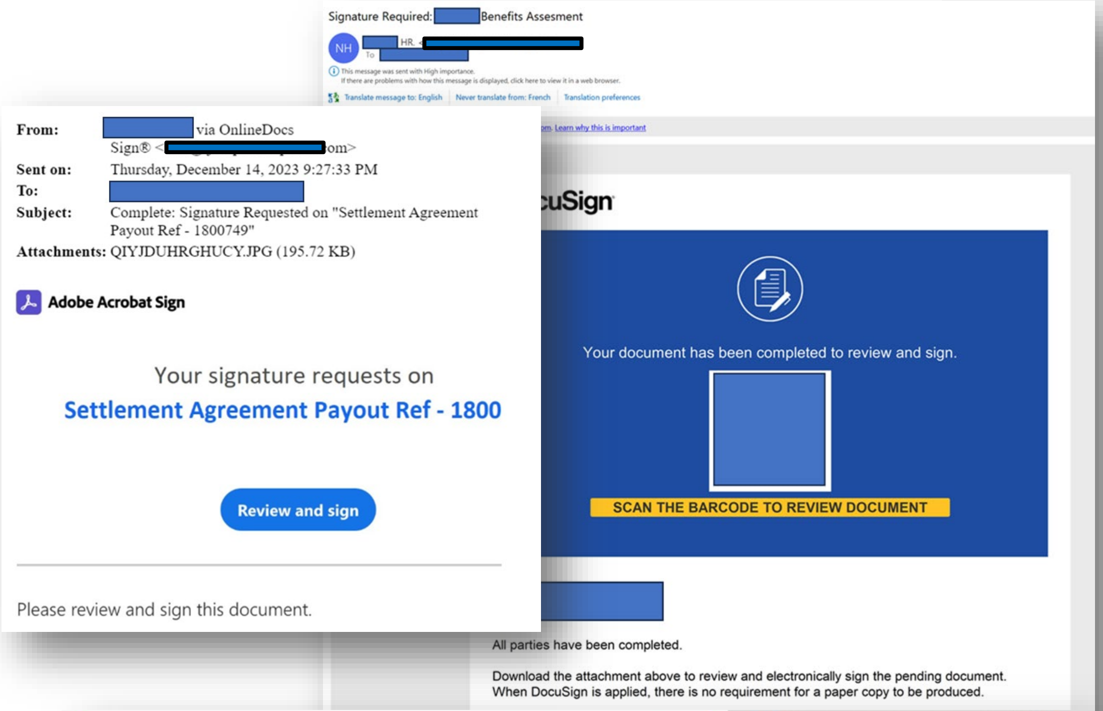
Image source: https://www.microsoft.com/en-us/security/blog/2022/07/12/from-cookie-theft-to-bec-attackers-use-aitm-phishing-sites-as-entry-point-to-further-financial-fraud/

A Popular Trio: AiTM-as-a-Service

EvilProxy:

The most widely used of the AiTM services, your organization is most likely to have seen an associated EvilProxy campaign in recent years.

- Widely distributed as malspam, with some campaigns noted by Proofpoint, for example, as targeting executives.
- Often sold as a service, with tutorials, via illicit communities on Telegram or the Dark Web.
  - The latest version refreshes cookies in the background.
- NCU-ISAO believes EvilProxy is responsible for a massive wave of QR-code based phishing (Quishing) attacks from Sept.-Nov. 2023.
- Common lures are DocuSign, SAP Concur, AdobeSign, and Microsoft (MFA themed).
- Evasion in campaigns, along with user enumeration/tracking is done through redirectors and Base64 encoded email addresses on payload links.
- Intermediary sites and Cloudflare are often used.



Signature Required: [redacted] Benefits Assesment

NH [redacted] HR. < [redacted]
To [redacted]

This message was sent with High importance.
If there are problems with how this message is displayed, click here to view it in a web browser.

Translate message to: English
Never translate from: French
Translation preferences
Learn why this is important

From: [redacted] via OnlineDocs
Sign® < [redacted] om>
Sent on: Thursday, December 14, 2023 9:27:33 PM
To: [redacted]
Subject: Complete: Signature Requested on "Settlement Agreement Payout Ref - 1800749"
Attachments: QIYJDUHRGHUCY.JPG (195.72 KB)

Your signature requests on
Settlement Agreement Payout Ref - 1800

Please review and sign this document.

Your document has been completed to review and sign.

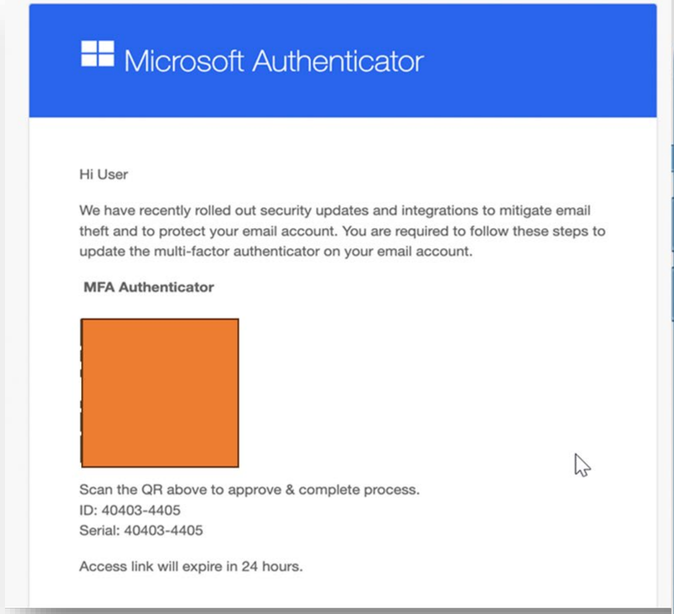
[redacted]

SCAN THE BARCODE TO REVIEW DOCUMENT

[redacted]

All parties have been completed.

Download the attachment above to review and electronically sign the pending document. When DocuSign is applied, there is no requirement for a paper copy to be produced.



Microsoft Authenticator

Hi User

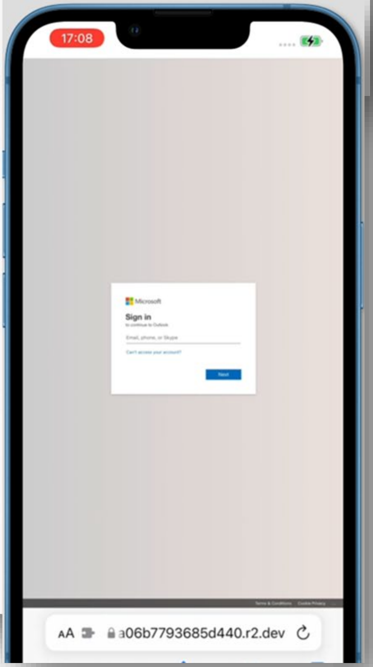
We have recently rolled out security updates and integrations to mitigate email theft and to protect your email account. You are required to follow these steps to update the multi-factor authenticator on your email account.

MFA Authenticator

[redacted]

Scan the QR above to approve & complete process.
ID: 40403-4405
Serial: 40403-4405

Access link will expire in 24 hours.



Content & Image source: NCU-ISAO intel & https://www.proofpoint.com/us/blog/email-and-cloud-threats/cloud-account-takeover-campaign-leveraging-evilproxy-targets-top-level

TLP:GREEN

EvilGinx:

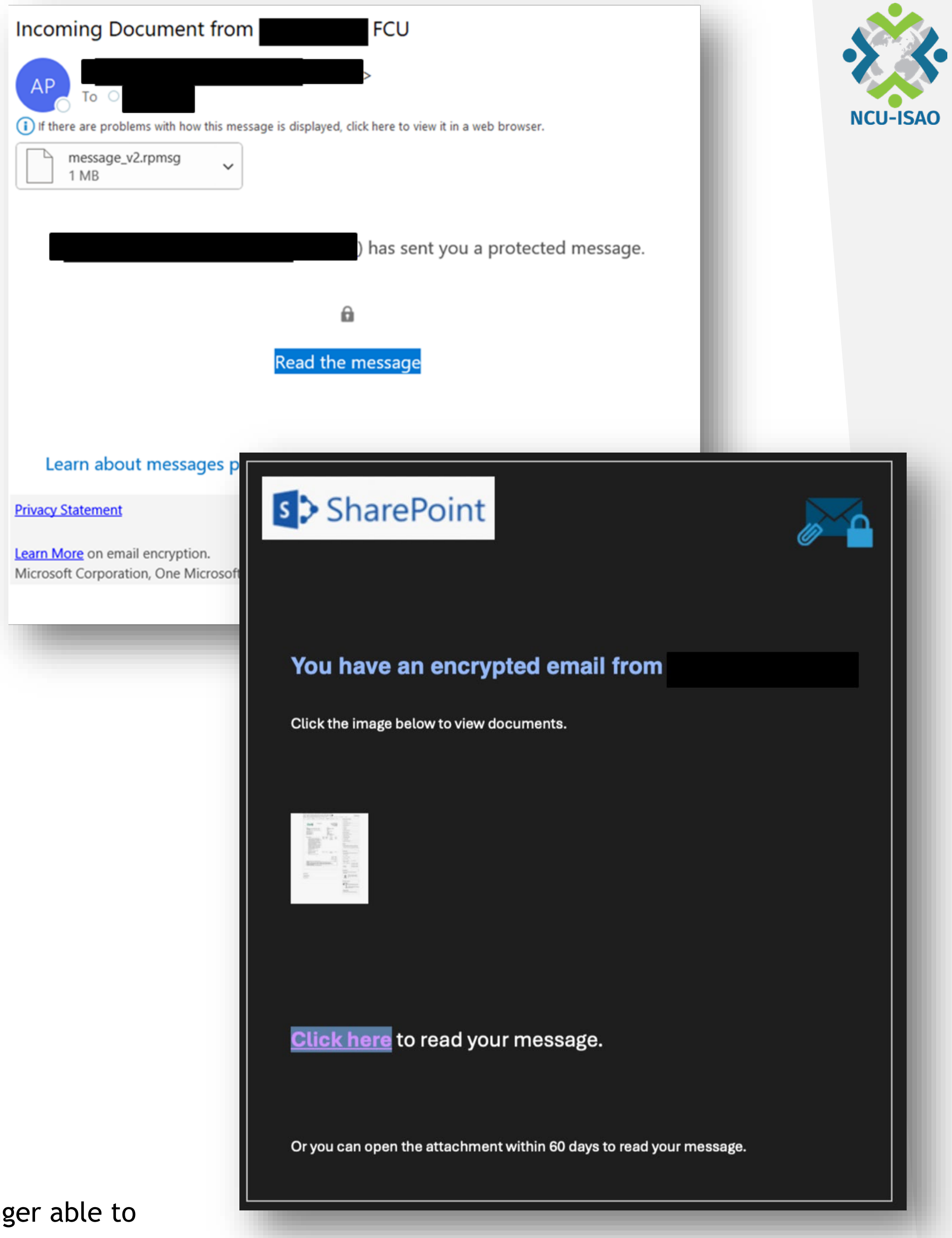
- **Established in 2018 for ‘pentesting’ MFA, now on version 3, EvilGinx becomes a web proxy (via lure URLs). Every packet, coming from victim's browser, is intercepted, modified and forwarded to the real website.**

- Distinctively, EvilGinx uses ‘phishlets,’ or YAML configuration files for proxying the legitimate connection from phishing pages.

- The community has taken the service a step further, creating EvilGoPhish as a simplified deployment tool for campaigns, including SMS.

- GitHub-based with preconfigured ‘phishlets’ for Microsoft, Google, Cloudflare, Stackoverflow, Yahoo, and more.

- **EvilQR was also released in August 2023, supporting credential theft of proxied logins with QR codes (Discord, WhatsApp, TikTok, Binance, Steam).**
  - **NOTE:** This QR-focused service currently does not support Microsoft, Google, or Apple at this time.
  - It also has cumbersome limitations like once-per-use QRs.



Incoming Document from [redacted] FCU

AP [redacted]

To [redacted]

If there are problems with how this message is displayed, click here to view it in a web browser.

message_v2.rpmsg
1 MB

[redacted]) has sent you a protected message.

Read the message

Learn about messages p

Privacy Statement

Learn More on email encryption.
Microsoft Corporation, One Microsof

You have an encrypted email from [redacted]

Click the image below to view documents.

Click here to read your message.

Or you can open the attachment within 60 days to read your message.

Because the control agent used in these attacks on CUs in 2022 has changed, we are no longer able to determine if EvilGinx is the AiTM being used in attacks on CUs.

Content & Image source: NCU-ISAO Intel & https://breakdev.org/evilginx-2-next-generation-of-phishing-2fa-tokens/

TLP:GREEN

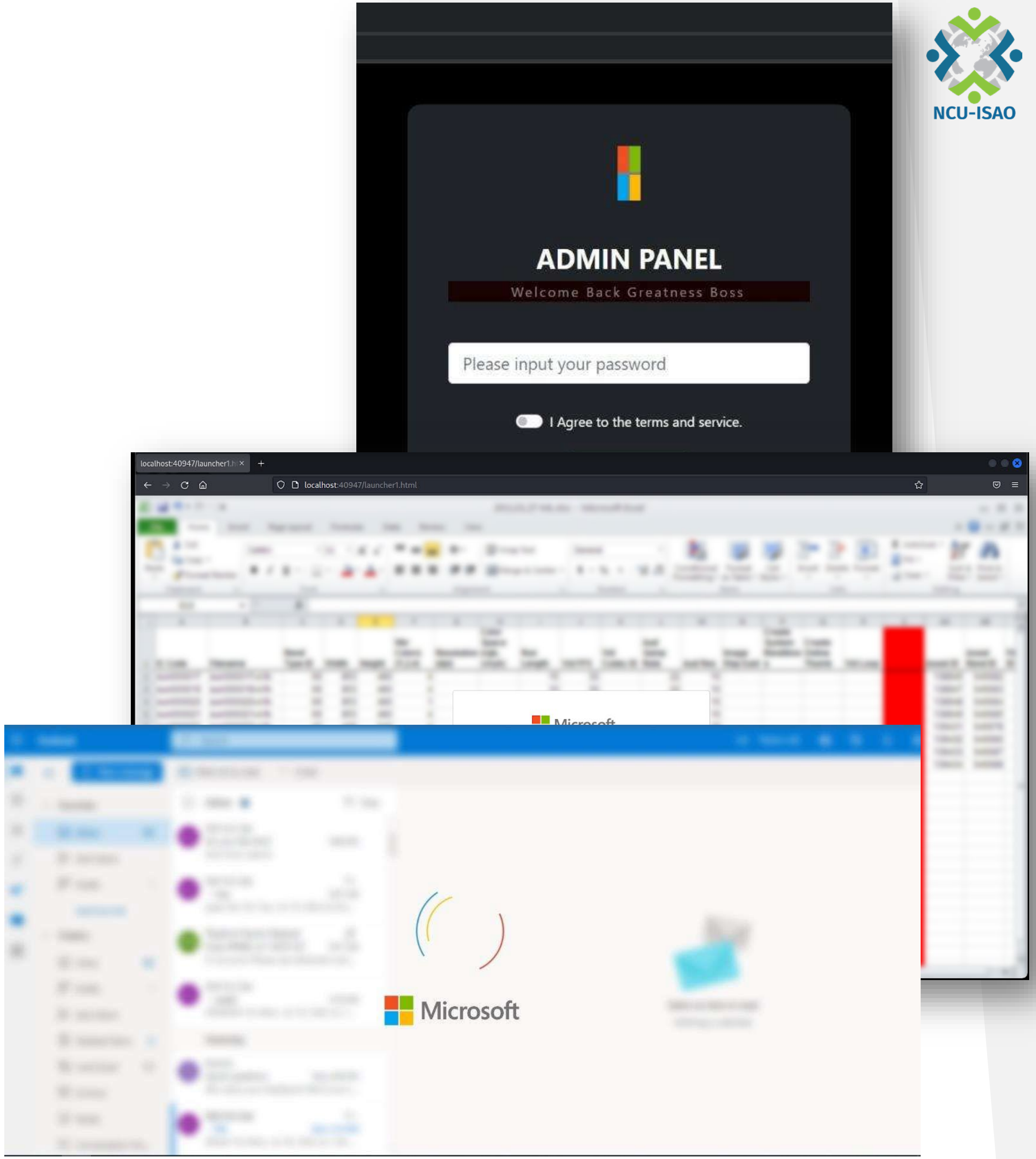
Greatness:

Offered as a Phishing Service, Cisco uncovered a Greatness campaign in May 2023, which is only focused on Microsoft 365 at this time.

- The service offers unskilled threat actors an administrative panel with API key to proxy the company’s branded MS login page and send compromised account details to the threat actor via a Telegram bot integration.

- The Phishing-as-a-Service is only known to target companies in the U.S., Canada, Australia, U.K., and South Africa.

- Observed Greatness campaigns are typically recognized by an HTML attachment that, when executed, will appear to open a Word/Excel/PowerPoint/Outlook file that is blurred out, prompting the user to log in.



ADMIN PANEL

Welcome Back Greatness Boss

Please input your password

I Agree to the terms and service.

localhost:40947/launcher1.html

Content & Image source: NCU-ISAO Intel & https://blog.talosintelligence.com/new-phishing-as-a-service-tool-greatness-already-seen-in-the-wild/

Mitigation, Countermeasures, & Incident Response

Help! How can we stop this from happening to us?

- **Tactics evolve! User awareness is the most important pro-active defense!**
  - Join an information sharing organization in your vertical; learn about new attacks like QR codes phishing as it happens!
  - Users should also be very suspicious when they receive a large number of out-of-office replies for no reason, and being BCC'd on "encrypted" messages.

- **Advanced email defense and mail-flow rules**
  - While not always the case, these messages share some standard characteristics, compromised host domains, subject lines, etc.
    - Given widespread attacks for some time now, Microsoft Defender/Exchange Online are doing a better job detecting these attacks and users interacting with them, but that is post impact.

- **Deploy conditional access policies:**
  - Easier said than done in larger organizations, but good conditional access will supersede the stolen session cookie.
  - Explicit IP-based conditions are ideal, but minimally, country-based geolocations.
  - Forcing device compliance conditions, such as MDM enrollment.

Image source: unsplash.com

TLP:GREEN

Help (cont…)! How can we stop this from happening to us?

NCU-ISAO

- **Analyze data such as SSL certificates generated by control agents**
  - Several of these services will autogenerate an SSL script with certain signature characteristics. Censys, Shodan, etc. can allow you to lookup, correlate, and create blocklists, but criminal tactics do evolve.
- **Set session cookies to expire sooner than the default for each application and understand refresh token conditions.**
  - https://learn.microsoft.com/en-us/microsoft-365/enterprise/session-timeouts?view=o365-worldwide
  - This will introduce business friction and diminish the user experience, but potentially avoid compromise if threat actors don't act fast.
- **CRITICAL: Move to phishing resistant authentication methods TODAY!**
  - For Microsoft, passwordless auth is a good step, but does not prevent victim cookie capture or MFA fatigue tactics.
  - https://cloudbrothers.info/fido2-security-keys-are-important/

…See next slide

Image source: unsplash.com

TLP:GREEN

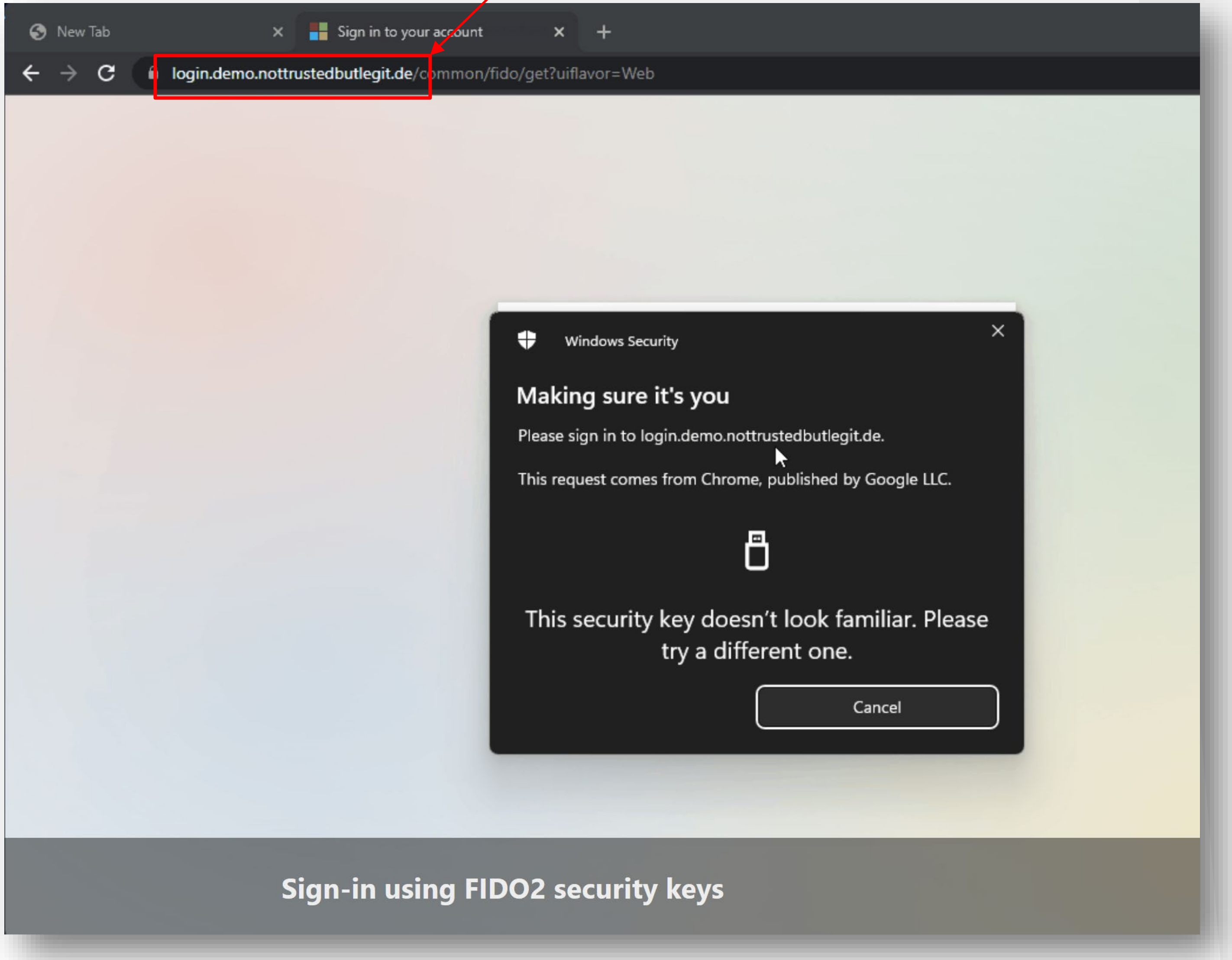
Implementing FIDO2 Authentication (or Biometrics)!

In this attack a very simple, but super effective technique is used to prevent the user to sign-in:

- The WebAuthn Client (the browser) compares the domain name with the Relying Party Identifier (RP ID) of the public keys in the FIDO2 security key. If a domain string matches it can be used as a method to sign-in. Otherwise, the user is unable to use the credential stored in the key.

Microsoft allows for the selection of multiple MFA methods, when present, so going in on FIDO2 we recommend reducing/removing fall-back MFA methods.

The USB Security Key does not recognize the website as authorized to sign in…


New Tab
Sign in to your account
login.demo.nottrustedbutlegit.de/common/fido/get?uiflavor=Web
Windows Security
Cancel

Making sure it's you

Please sign in to login.demo.nottrustedbutlegit.de.

This request comes from Chrome, published by Google LLC.

This security key doesn't look familiar. Please try a different one.

Sign-in using FIDO2 security keys

Image source: https://cloudbrothers.info/fido2-security-keys-are-important/

TLP:GREEN

What to do if a user falls victim to this attack (Part 1)?

Remediation Steps in M365 (Compromised Users:

If alerted to a compromised sender by NCU-ISAO or another CU, run a message trace for the sender and see if any users at your organization have received this message and interacted with it.

If so, we recommend the following steps be taken (Microsoft 365):

In 365 Admin:

- Block the user's access until remediation is complete.
- Reset the user's password and require it be different than before (this will also force a new login)
- Revoke all sessions (this will also expire the captured session cookie the bad guys are using).
- Under the user's licenses, see if there are any delegates on their mailbox that don't belong and remove them.
- Consider: block user's access to Outlook on the Web (webmail), which is done with their license as well.
  - This will break Microsoft 365 encrypted messages in certain conditions, and not necessarily prevent access to other Microsoft services.
- If they had administrative access, look for newly created employee accounts that the criminals may have set up.
- Critical: log the user in to myaccount[.]microsoft[.]com to see if the bad guys added another form of 2FA authentication to his account and delete it, if so.

What to do if a user falls victim to this attack (cont…)?

Additionally:

- Verify no suspicious emails sent from user.
- Verify no suspicious address forwards in M365.
- Verify no suspicious inbox rules have been added.
- Verify no suspicious audit or sign-in logs.

○ If it is a privileged user, make sure no Exchange Mail-flow Rules have been added.

In Microsoft Entra:

- If your tenant allows non-admins to register applications, look for new app registrations (this would create an Oauth token they could use). Revoking all sessions should also revoke the active Oauth key if this happened, but you'll still want to delete it.

Other:

- In their browser, tell them to clear all cache and browsing history. We are ultimately trying to get all session cookies revoked and removed prior to reestablishing access.

Image source: unsplash.com

NCU-ISAO

Thank you!

Q&A

Get in touch with me:

- Email: brian.hinze@ncuisao.org
- Website: https://ncuisao.org/

Referenced Web-sources:

NCU-ISAO

Note: Some uncited content is derived from NCU-ISAO intelligence and member-shared information.

Sources & References:

- https://www.cyberpunk.rs/evilginx-phishing-examples-v2-x-linkedin-facebook-custom
- https://github.com/bbtfr/evil-proxy
- https://breakdev.org/evilqr-phishing/
- https://github.com/hash3liZer/phishlets
- https://github.com/fin3ss3g0d/evilgophish
- https://breakdev.org/evilginx-2-next-generation-of-phishing-2fa-tokens/
- https://www.microsoft.com/en-us/security/blog/2022/07/12/from-cookie-theft-to-bec-attackers-use-aitm-phishing-sites-as-entry-point-to-further-financial-fraud/
- https://www.proofpoint.com/us/blog/email-and-cloud-threats/cloud-account-takeover-campaign-leveraging-evilproxy-targets-top-level
- https://www.microsoft.com/en-us/security/blog/2023/06/08/detecting-and-mitigating-a-multi-stage-aitm-phishing-and-bec-campaign/
- https://www.proofpoint.com/us/blog/email-and-cloud-threats/defending-against-evilproxy-phishing-toolkit
- https://cloudbrothers.info/fido2-security-keys-are-important/
- https://blog.talosintelligence.com/new-phishing-as-a-service-tool-greatness-already-seen-in-the-wild/