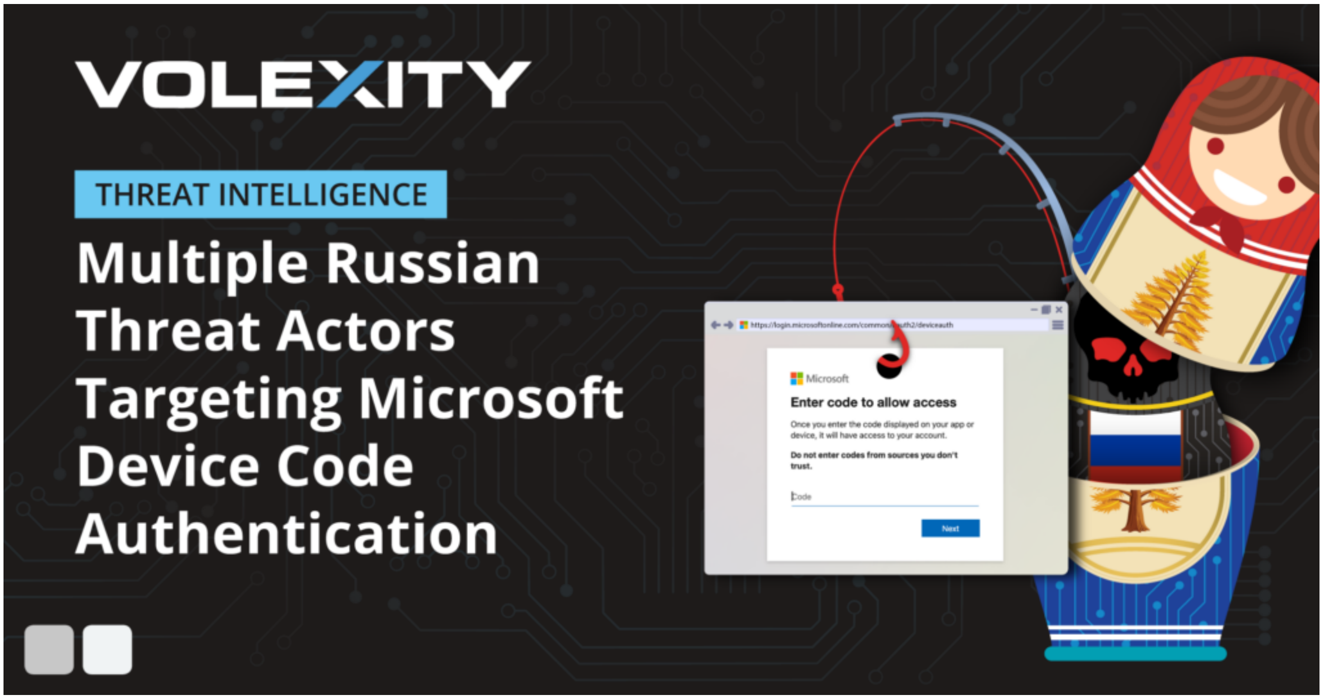
Multiple Russian Threat Actors Targeting Microsoft Device Code Authentication

volexity.com/blog/2025/02/13/multiple-russian-threat-actors-targeting-microsoft-device-code-authentication/

February 13, 2025

February 13, 2025

by Charlie Gardner, Steven Adair, Tom Lancaster


VOLEXITY
THREAT INTELLIGENCE
Multiple Russian Threat Actors Targeting Microsoft Device Code Authentication
https://login.microsoftonline.com/common/oauth2/deviceauth
Microsoft
Enter code to allow access
Once you enter the code displayed on your app or device, it will have access to your account.
Do not enter codes from sources you don't trust.
Code
Next

KEY TAKEAWAYS

- *Volexity has observed multiple Russian threat actors conducting social-engineering and spear-phishing campaigns targeting organizations with the ultimate goal of compromising Microsoft 365 accounts via Device Code Authentication phishing.*
- *Device Code Authentication phishing follows an atypical workflow to that expected by users, meaning users may not recognize it as phishing.*
- *Recent campaigns observed have been politically themed, particularly around the new administration in the United States and the changes this might mean for nations around the world.*

Starting in mid-January 2025, Volexity identified several social-engineering and spear-phishing campaigns by Russian threat actors aimed at compromising Microsoft 365 (M365) accounts. These attack campaigns were highly targeted and carried out in a variety of ways. The majority of these attacks originated via spear-phishing emails with different themes. In one case, the eventual breach began with highly tailored outreach via Signal.

Through its investigations, Volexity discovered that Russian threat actors were impersonating a variety of individuals in order to socially engineer targets, including impersonating individuals from the following:

- United States Department of State
- Ukrainian Ministry of Defence
- European Union Parliament
- Prominent research institutions

Communications carried a variety of different themes and messages, but they all ultimately resulted in the attacker inviting the targeted user to one of the following:

- Microsoft Teams Meeting / Video Conference
- Access to applications and data as an external M365 user
- Join a chatroom on a secure chat application

When these attacks were successful and the attackers gained access to accounts, the post-exploitation phase often had unique characteristics in each case:

- The way the attackers accessed material from compromised organizations (scripts versus native applications)
- The infrastructure used to access stolen accounts

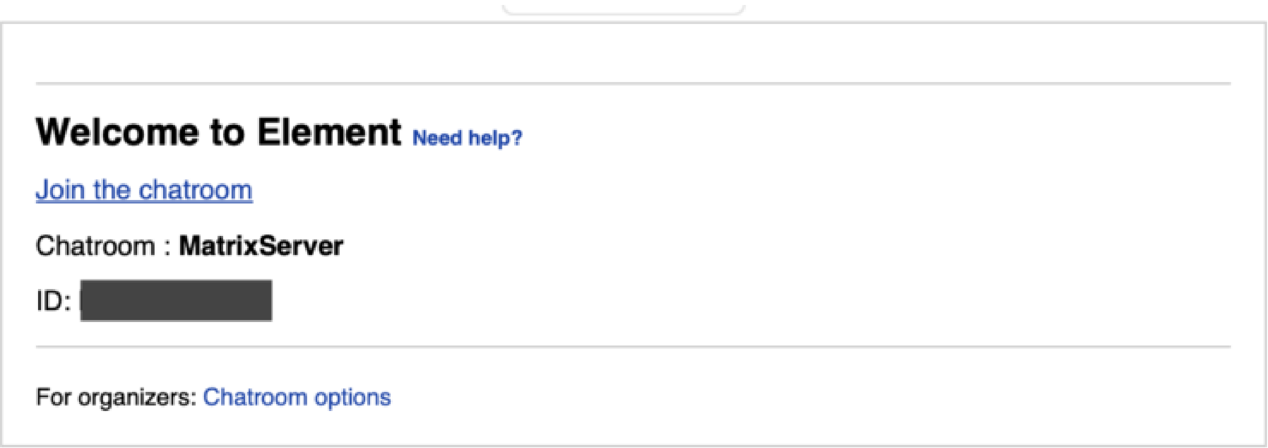
Despite the differences, Volexity found the attacks had one thing in common: they were all **Device Code Authentication** attacks. While this attack method is not new, it is one that is definitely lesser known and not commonly leveraged by nation-state actors. Details on the social-engineering and spear-phishing campaigns, along with how Device Code Authentication attacks work, will be covered further in this blog post. What Volexity has observed is that this method has been more effective at successfully compromising accounts than most other targeted spear-phishing campaigns.

Volexity assesses with high confidence that the series of attacks described in this blog post are from Russia-based threat actors. At this time, Volexity is tracking this activity under three different threat actors and assesses with medium confidence that at least one of them is **CozyLarch** (overlapping with DarkHalo, APT29, Midnight Blizzard, CozyDuke). Volexity is tracking the remaining activity under **UTA0304** and **UTA0307**. It is possible that all the activity described in this blog post is a single threat actor, but despite the similar targeting, timing, and attack method, other observed components of the operations are different enough to be tracked separately, for now.

From Secure Chat to Insecure Authentication

The discovery of this threat activity started toward the end of January 2025, when Volexity uncovered a highly targeted attack that had successfully compromised the M365 account of one of its customers. This breach was discovered after Volexity identified suspicious sign-in activity to the account, which was followed by a rapid download of files from the user's OneDrive. All authentication and download events came from virtual private server (VPS) and Tor IP addresses, which is not the most subtle way to access an account. Volexity noted this activity was likely scripted, as the User-Agent string for later access and file downloads was the Python User-Agent string `python-requests/2.25.1`.

Volexity then performed a detailed investigation into this incident, in an effort to identify how the account was compromised. A review of login activity showed the legitimate user had logged in and approved a multi-factor authentication (MFA) request. However, subsequent access was not from the legitimate user's IP address. This caused Volexity to initially suspect a phishing attack involving an adversary-in-the-middle (AiTM) framework. As a result, Volexity reviewed emails to the user leading up the time of the authentication event. This review identified a suspicious email just moments before the login activity from an email address purporting to be from someone with the name of a high-ranking official from the Ukrainian Ministry of Defence. The email was structured to look like a meeting invite for a chatroom on the messaging application, Element. Element is another encrypted messaging application that offers the ability for users to self-host a server with functionality that includes group video chats. The “invitation” email sent is shown below .



Welcome to Element Need help?

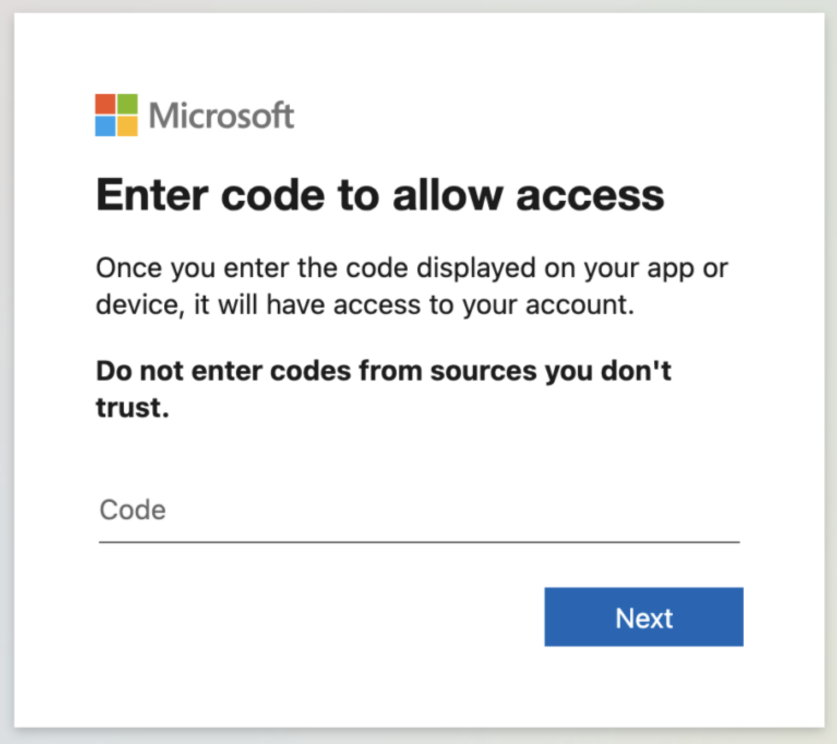
Join the chatroom

Chatroom : **MatrixServer**

ID: [redacted]

For organizers: Chatroom options

In fact, all hyperlinks in the email were linked to `https://login.microsoftonline.com/common/oauth2/deviceauth`, the page used for the Microsoft Device Code authentication workflow. Clicking the link leads to the dialogue shown below.



Microsoft

Enter code to allow access

Once you enter the code displayed on your app or device, it will have access to your account.

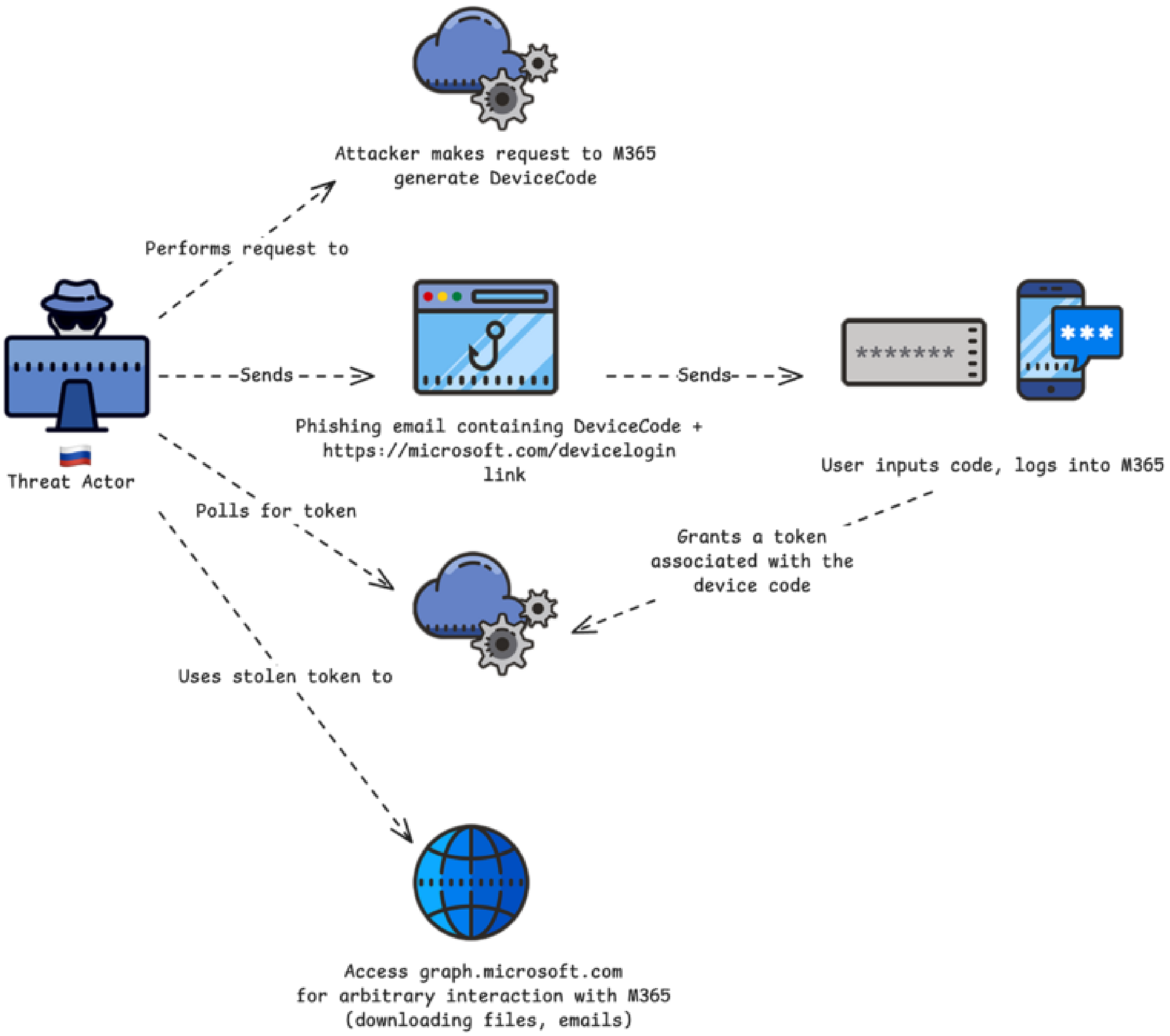
Do not enter codes from sources you don't trust.

Microsoft describes the purpose of this workflow as allowing *"'users to sign in to input-constrained devices such as a smart TV, IoT device, or a printer.*" However, in this case, it means if an attacker can convince a user to enter a specific code into this dialogue (and log in), they are granted long-term access to the user's account.

From Signal to Element

After working with its customer more closely, Volexity learned that the victim had been contacted on Signal by an individual purporting to be from the Ukrainian Ministry of Defence. This individual then requested the victim move off Signal to another secure chat application called Element. The attacker then had the victim join an Element server they controlled under the domain `sen-comms[.]com`. This allowed the attacker to further communicate with the victim in real time and inform them they needed to click a link from an email to join a secure chat room. This is where the email Volexity had discovered came into play. The message was a ploy to fool the user into thinking they were being invited into a secure chat, when in reality they were giving the attacker access to their account. The generated Device Codes are only valid for 15 minutes once they are created. As a result, the real-time communication with the victim, and having them expect the "invitation", served to ensure the phish would succeed through timely coordination.

The diagram below shows a high-level depiction of how the attack worked.


Attacker makes request to M365 generate DeviceCode
Performs request to
Threat Actor
Sends
Phishing email containing DeviceCode + https://microsoft.com/devicelogin link
Sends
****
***
User inputs code, logs into M365
Polls for token
Grants a token associated with the device code
Uses stolen token to
Access graph.microsoft.com for arbitrary interaction with M365 (downloading files, emails)

UTA0304 Infrastructure

Volexity tracks the threat actor behind this campaign as **UTA0304**. Through research conducted on the custom domain used by UTA0304 to operate its own Element server, Volexity was able to pivot and discover additional infrastructure it believes is likely operated by the group. The table below represents the list of infrastructure that Volexity has tied to this threat actor.

Domain	IP Address	Confidence
sen-comms[.]com	107.189.27.41	High
afpi-sec[.]com	144.172.113.77	Medium
chromeelevationservice[.]com	167.88.162.72	Medium

Domain	IP Address	Confidence
comms-net[.]com	107.189.26.199	High

Spoofing the United States Department of State

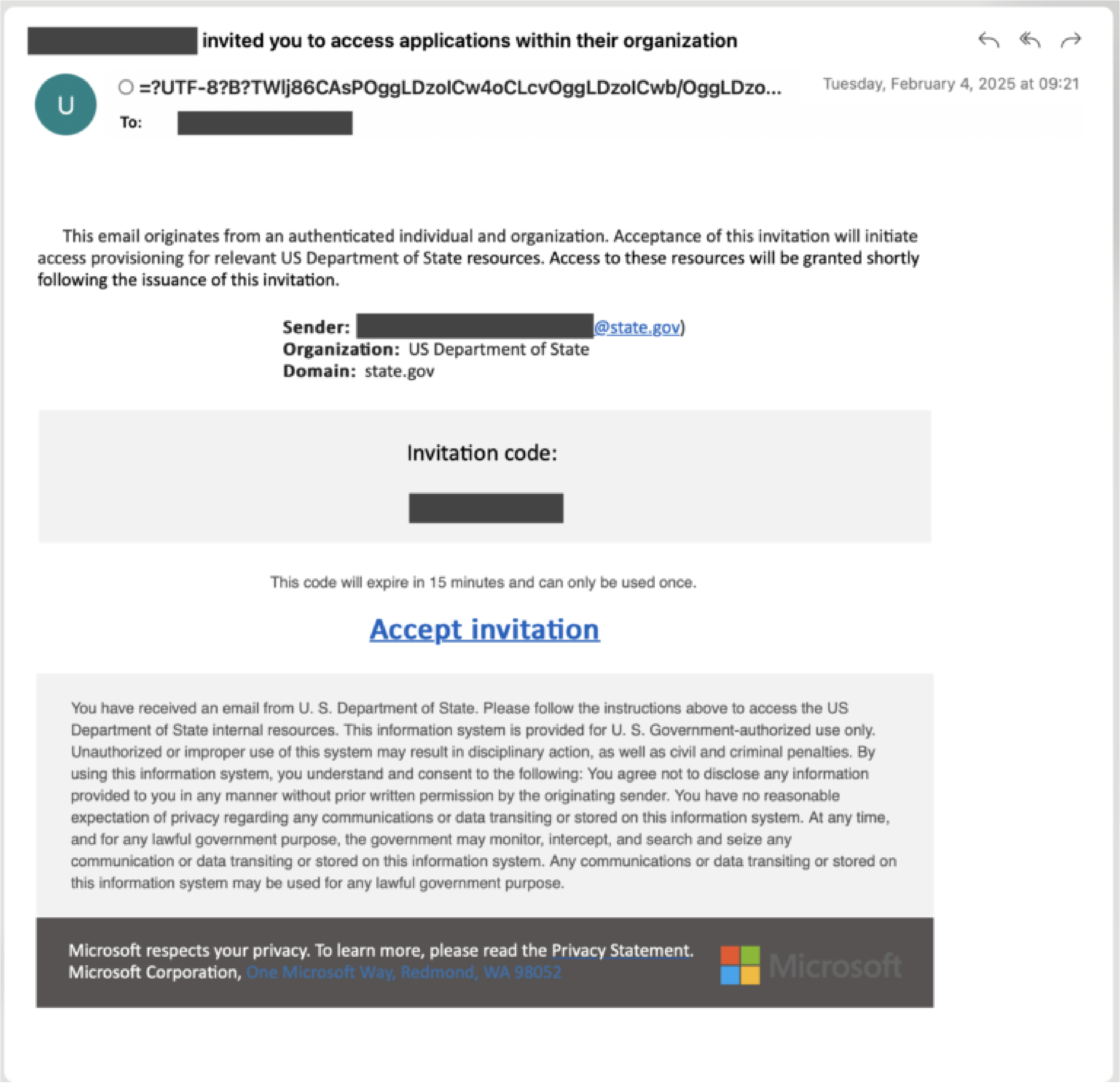
In early February 2025, Volexity observed multiple spear-phishing campaigns targeting users with fake Microsoft invitations purporting to be from the United States (US) Department of State. These emails were themed as invitations to join the US Department of State's Microsoft tenant as an external user, or as invitations to a Microsoft Teams chat named "***Measuring Influence Operations****".*

Similar to the campaign conducted by UTA0304, these fake US Department of State emails were targeting users with a Device Code OAuth phishing workflow. Each email was aimed at convincing the user to accept the invitation and enter a unique code provided in the phishing email. The link in the invitations would direct users to the Microsoft Device Code authentication page. If the user entered the code provided in the phishing email, the authentication page would subsequently authorize the threat actor to access to the user's account. However, it is worth noting that this campaign was sent out of the blue, with no precursor or build up to the emails, so users would not be expecting these messages. Even if they were to fall for the campaign, they would have to have done it within 15 minutes of receiving the email. This dramatically decreased the likelihood that this attack would be successful.

After reviewing various parts of the attack, Volexity assesses with medium confidence that the Russian threat actor CozyLarch (aka APT29 or Midnight Blizzard) was behind these US Department of State themed spear-phishing campaigns. Additional details on each campaign are described in the sections that follow.

Campaign 1: M365 Tenant External User Invitation

CozyLarch sent invitations to several users, inviting them to access applications within the M365 tenant for the US Department of State. The invitation email was designed to look like a real invitation that would be sent from Microsoft, as shown below.



[redacted] invited you to access applications within their organization

○ =?UTF-8?B?TWlj86CAsPOggLDzolCw4oCLcvOggLDzolCwb/OggLDzo...

Tuesday, February 4, 2025 at 09:21

To: [redacted]

This email originates from an authenticated individual and organization. Acceptance of this invitation will initiate access provisioning for relevant US Department of State resources. Access to these resources will be granted shortly following the issuance of this invitation.

Sender: [redacted]@state.gov)
Organization: US Department of State
Domain: state.gov

Invitation code:

[redacted]

This code will expire in 15 minutes and can only be used once.

Accept invitation

You have received an email from U. S. Department of State. Please follow the instructions above to access the US Department of State internal resources. This information system is provided for U. S. Government-authorized use only. Unauthorized or improper use of this system may result in disciplinary action, as well as civil and criminal penalties. By using this information system, you understand and consent to the following: You agree not to disclose any information provided to you in any manner without prior written permission by the originating sender. You have no reasonable expectation of privacy regarding any communications or data transiting or stored on this information system. At any time, and for any lawful government purpose, the government may monitor, intercept, and search and seize any communication or data transiting or stored on this information system. Any communications or data transiting or stored on this information system may be used for any lawful government purpose.

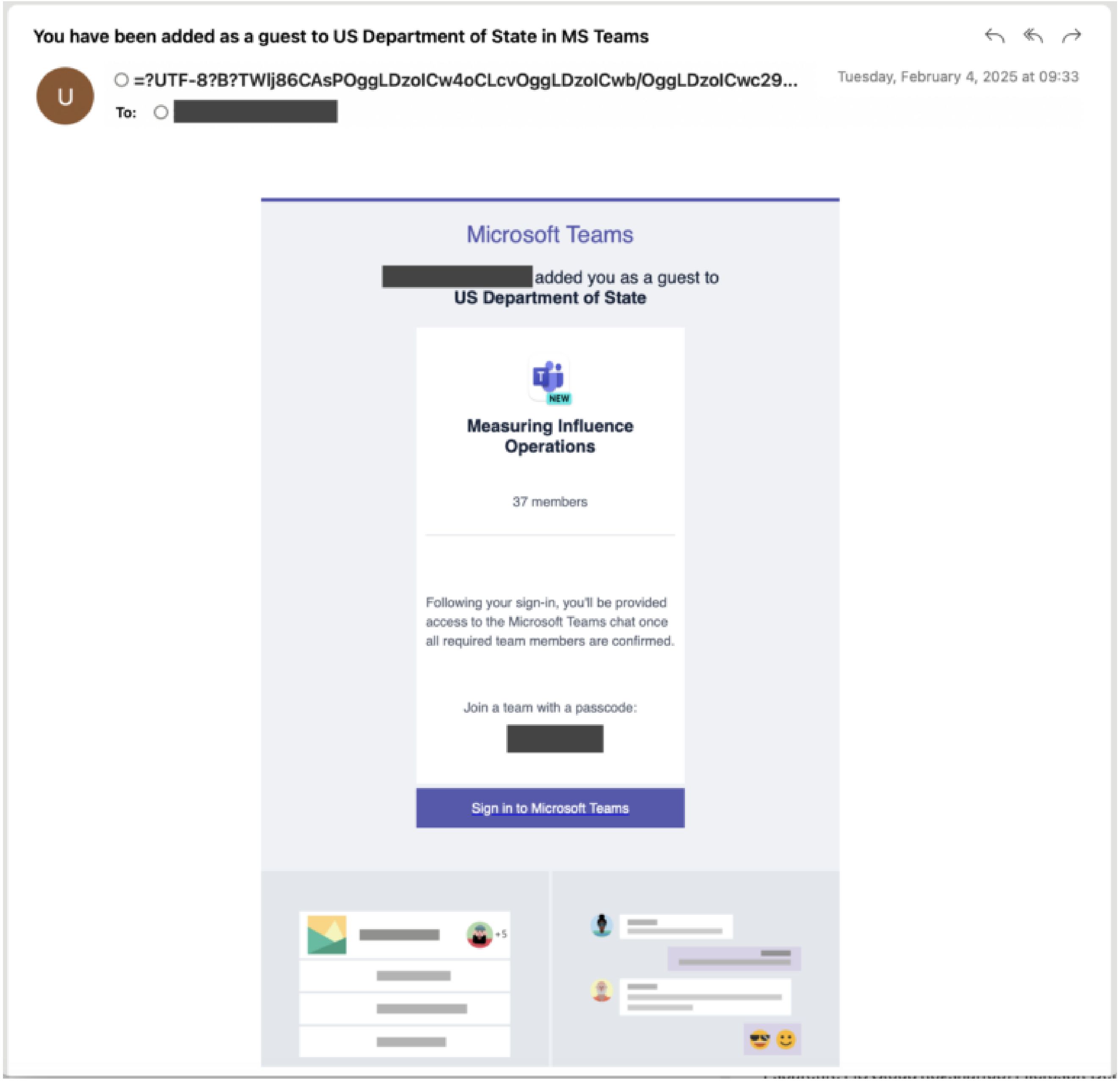
Microsoft respects your privacy. To learn more, please read the Privacy Statement.
Microsoft Corporation, One Microsoft Way, Redmond, WA 98052

In this instance, the “Accept invitation” hyperlink goes to https://www.microsoft.com/devicelogin, which is a simple redirect that sends the user to https://login.microsoftonline.com/common/oauth2/deviceauth.

The redirect link takes the user to the Microsoft Device Code OAuth workflow, and it is the same URL that UTA0304 directly embedded in their phishing campaign. However, unlike UTA0304, CozyLarch opted to use the redirect URL rather than the final login URL, perhaps because it may look even more recognizable to a discerning user, given that it is hosted on the main Microsoft domain. If the user entered the code provided from the email and continued through the authentication process, the attacker was granted access to the user’s M365 account.

Campaign 2: M365 Teams Chat Invitation

CozyLarch launched a second campaign, in which they targeted users with a fake invitation to join a Microsoft Teams chat named “***Measuring Influence Operations***”. The email made it appear as though there were already 37 other members in the chat. A screenshot of one of the observed spear-phishing messages is shown below.



You have been added as a guest to US Department of State in MS Teams

U ○ =?UTF-8?B?TWlj86CAsPOggLDzolCw4oCLcvOggLDzolCwb/OggLDzolCwc29... Tuesday, February 4, 2025 at 09:33

To: ○ [redacted]

Microsoft Teams

[redacted] added you as a guest to
US Department of State

Measuring Influence Operations

37 members

Following your sign-in, you'll be provided access to the Microsoft Teams chat once all required team members are confirmed.

Join a team with a passcode:

[redacted]

The “Sign in to Microsoft Teams” button in the email body is a hyperlink that leads to the same https://www.microsoft.com/devicelogin URL observed in the other campaign. The attack flow and end goal are the same, with only a small difference in the theme of the emails.

Email Source Analysis

The emails are designed to appear as though they come from Microsoft. The messages used mixed encoding in the “friendly” name that make the address difficult to discern. An example of the full “from” header used in one phishing email is given below:

```
\"Mic\udb40\udc30\udb40\udc30\udb40\udc30\u200br\udb40\udc30\udb40\udc30o
\udb40\udc30\udb40\udc30soft Invitations on behal f of US
Dep\udb40\udc30\udb40\udc30\udb40\udc30artme\udb40\udc30\udb40\udc30\udb4
0\udc30nt of St\udb40\udc30\udb40\udc30\udb40\udc30 ate
\uff1cinvites\uff20mic\udb40\udc30\udb40\udc30\udb40\udc30\u200br\udb40\u
dc30\udb40\udc30o\udb40\udc30\udb40\udc30soft.co
m\uff1e\u180e\u3000\u180e\u3000\u180e
\u180e\u3000\u180e\u3000\u180e\u3000\u180e\u3000\u180e\u3000\u180e\u3000
\u180e\u3000\u180e\u3000\u180e\u3000\u180e\u3000\u180e\u3000\u180e\u3000\
u180e\u3000\u180e\u3000\u180e\u3000\u180e\u3000 \u180e \u180e\u3000\u180e
\u180e\u3000\u180e\u3000\u180e\u3000\u180e\u3000\u180e\u3000\u180e\u3000\
u180e
\u3000\u180e\u3000\u180e\u3000\u180e\u3000\u180e\u3000\u180e\u3000\u180e\
u3000\u180e\u3000\u180e\u3000\u180e\u3000\u180e
\u180e\u3000\u180e\u3000\u180e\u3000\u180e\u3000\u180e\u3000\u180e\u3000\
u180e\u3000\u180e\u3000\u180e\u3000
\u180e\u3000\u180e\u3000\u180e\u3000\u180e\u3000\u180e\u3000\u180e\u3000\
u180e\u3000\u180e\u3000\u180e\u3000\u180e\u3000
\u180e\u3000\u180e\u3000\u180e\u3000\u180e\u3000\u180e\u3000\u180e\u3000\
u180e\u3000\u180e\u3000\u180e\u3000\u180e\u3000
\u180e\u3000\u180e\u3000\u180e\u3000\u180e\u3000\u180e\u3000\u180e\u3000\
u180e\u3000\u180e\u3000\u180e\u3000\u180e\u3000
\u180e\u3000\u180e\u3000\u180e\u3000\u180e\u3000\u180e\u3000\u180e\u3000\
u180e\u3000\u180e\u3000\u180e\u3000\u180e\u3000
\u180e\u3000\u180e\u3000\u180e\u3000\u180e\u3000\u180e\u3000\u180e\u3000\
u180e\u3000\u180e\u3000\u180e\u3000\u180e\u3000
\u180e\u3000\u180e\u3000\u180e\u3000\u180e\u3000\u180e\u3000\u180e\u3000\
u180e\u3000\u180e\u3000\u180e\u3000\u180e\u3000
\u180e\u3000\u180e\u3000\u180e \u061c Cc:\" <[email protected]>
```

The attacker attempted to make it appear as if the emails were from `invites@microsoft[.]com`, and also set the `Reply-To` header as `invites@microsoft[.]com`. However, the true address could be seen at the end of the `From:` field; all messages were sent via Google Gmail accounts. Volexity observed the following Gmail accounts as the actual senders of the messages observed:

- `brensonkarl@gmail[.]com`
- `kaylassammers@gmail[.]com`
- `kendisggibson@gmail[.]com`
- `leslytthomson@gmail[.]com`
- `mikedanvil@gmail[.]com`
- `sheilmagnett@gmail[.]com`

- susannmarton@gmail[.]com

These addresses are believed to be controlled by CozyLarch and can be used to reliably detect phishing emails that may have been sent.

Using Wireless Proxy Networks for Email Distribution

Volexity also noted that the sending IP address associated with each spear-phishing email was recorded in the headers. Looking at the `Received` header in the messages, it became apparent that the attacker was using Proxy IP addresses based in the US to send messages. Volexity observed nearly a dozen IP addresses belonging to mobile networks in the US (AT&T and Verizon Wireless).

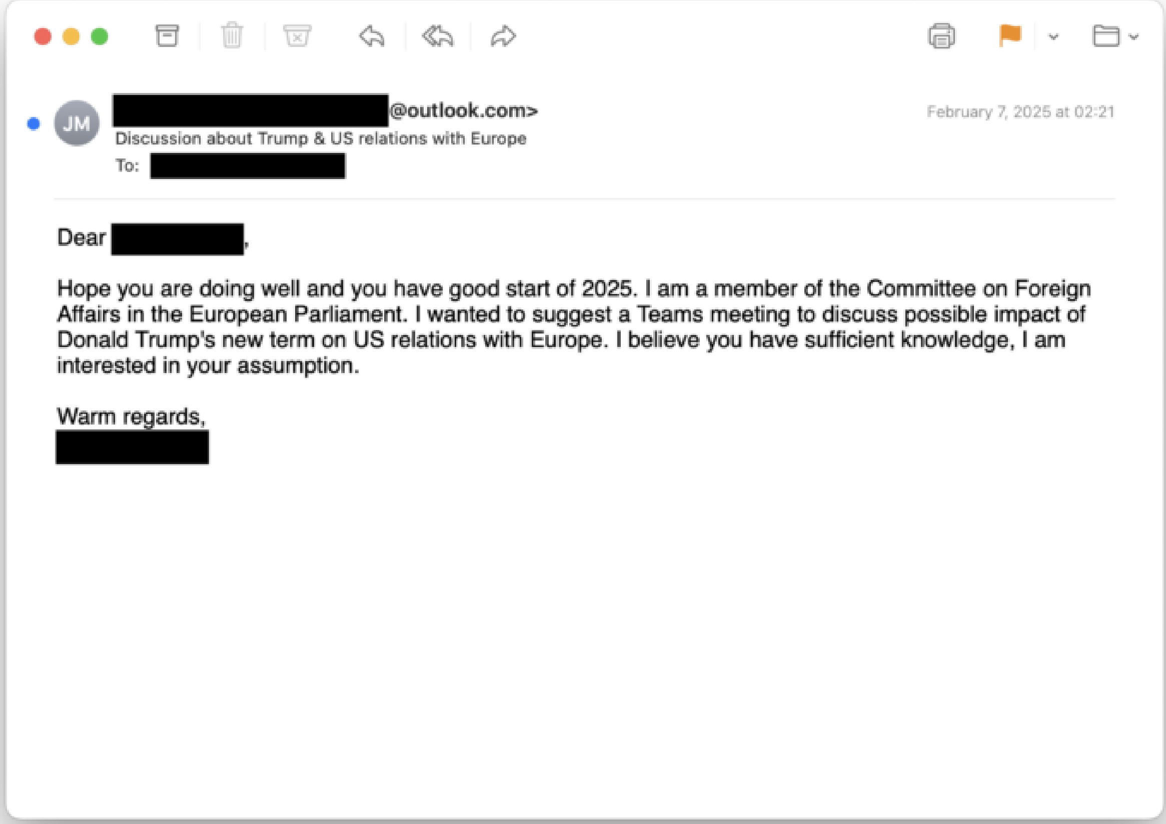
European Parliament and Donald Trump

Starting in late January through to the publication of this blog (February 13, 2025), Volexity has observed another campaign by a Russian threat actor it tracks as **UTA0307** targeting numerous organizations. UTA0307 created a fake email under the identity of a member of the European Parliament who is on the Committee on Foreign Affairs. The threat actor reached out to numerous individuals with personalized emails requesting a Microsoft Teams meeting to discuss Donald Trump and his impact on relations between the US and the European Union. Volexity also observed a smaller set of campaigns centered on discussing China's foreign policy and China-European Union relations.

The email subject lines used in these various campaigns are listed below:

- *Trump and EU*
- *Discussion on Eastern Europe and the Caucasus*
- *Discussion about Donald Trump's new term*
- *Discussion about Trump & US relations with Europe*
- *Collaboration on China and East Asia Research*

The image below shows an example spear phish that was sent by UTA0307.



[redacted]@outlook.com>
Discussion about Trump & US relations with Europe
To: [redacted]

February 7, 2025 at 02:21

Dear [redacted],

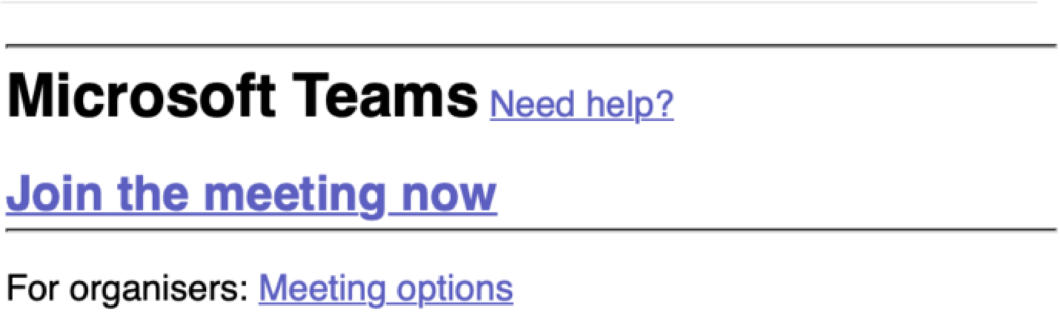
Hope you are doing well and you have good start of 2025. I am a member of the Committee on Foreign Affairs in the European Parliament. I wanted to suggest a Teams meeting to discuss possible impact of Donald Trump's new term on US relations with Europe. I believe you have sufficient knowledge, I am interested in your assumption.

Warm regards,
[redacted]

None of the initial emails contained any malicious content or links at the onset. The threat actor was leveraging a tactic that has become commonplace for numerous nation-state actors, where they wait until a conversation has started prior to sending anything malicious. This serves the purpose of knowing they have an engaged target, and that the target's guard is potentially down. In the specific cases of Device Code Authentication phishing, it is especially important to have a responsive target, as the threat actor has only 15 minutes to convince the target to enter the code that has been generated.

A Different Device Code OAuth Phishing Technique

Volexity actually discovered the operations of UTA0307 following a successful compromise. Similar to the initial discovery of UTA0304, Volexity worked backwards from detecting a breach to identifying the above spear-phishing emails. In this case, the victim had engaged from the initial email and had several messages back and forth with UTA0307 regarding a meeting being set up. They agreed to join a Microsoft Teams meeting, and a fake invitation email was sent. However, this time the link in the email did not go to Microsoft. The target received an email with the subject "*Join Teams meeting*", and the body of the email, shown below, was designed to look like a real invitation.

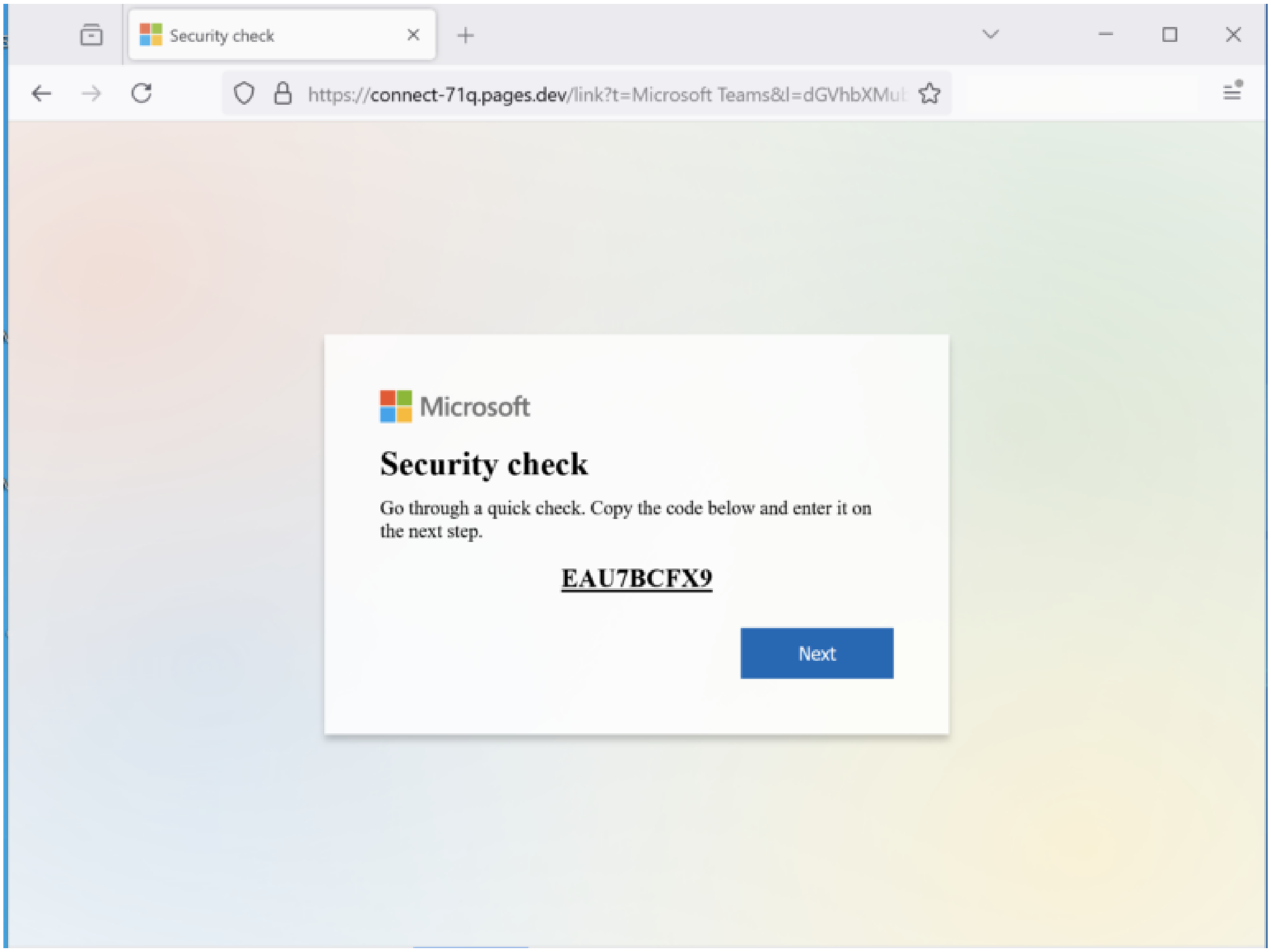


Microsoft Teams Need help?

Join the meeting now

For organisers: Meeting options

The “Join the meeting now” hyperlink, however, linked to a website controlled by UTA0307 (`connect-71q.pages[.]dev`). This page in turn was set up to automatically generate a new Microsoft Device Code each time it was visited. The website was designed to appear as an official Microsoft interstitial page before the user can join a Microsoft Teams meeting. The message that appears on the landing page (shown below) claims that the victim needs to pass a security check by copying a code and entering it on a subsequent page



Security check
https://connect-71q.pages.dev/link?t=Microsoft Teams&l=dGVhbXMu
Microsoft

Security check

Go through a quick check. Copy the code below and enter it on the next step.

EAU7BCFX9

When the user clicks the “Next” button, a new tab is opened with the real Microsoft Device Code Authentication interface that requests an authentication code. If the victim enters the code supplied by the phishing page, they grant UTA0307 access to their M365 account. Interestingly, in the background of the initial phishing page, Volexity noted that the website would continuously poll the domain `rosejob[.]com`. It appears this domain was set up to monitor successful Device Code Authentication and, if detected, would redirect the user to a real Microsoft Teams meeting URL in an effort to make the activity appear legitimate.

The threat actor never joined this Microsoft Teams meeting. However, UTA0307 did add authorization for an authentication application under their control to enable multi-factor authentication when logging into the compromised account. Volexity assesses with medium confidence that this was a requirement of logging into the account, even with the stolen authentication token.

One benefit of this attack workflow versus other previously observed DeviceID phishing workflows is that, when a DeviceID code is generated, it is only valid for 15 minutes. Having an interstitial page that automatically generates new codes means UTA0307 does not have to worry about their phishing content expiring.

UTA0307 Post-compromise Activities, Targeting and Attribution

Volexity observed UTA0307 exfiltrating documents from a compromised M365 account that would be of interest to a Russian threat actor. This was determined based on identification of FileDownloaded operations observed in M365 audit log data. Given this information about the threat actor’s objectives, their targeting, and their use of a highly similar technique to that used in recent days and weeks by CozyLarch and UTA0304, Volexity assesses with medium confidence that UTA0307 is also a Russian threat actor.

However, the exact implementation of the DeviceID OAuth phishing technique used in this activity differs slightly from those previously documented by Volexity, which provides some evidence that this activity may have been conducted by a separate threat actor. For example, while the previously observed phishing campaigns saw the attacker use the client ID for Microsoft Office when handling Device Code Authentication, this activity instead used the client ID for Microsoft Teams, as shown below (note that Microsoft uses `appId` and `client_id` interchangeably in their logs when referring to the ID for an application):

```
"appDisplayName": "Microsoft Teams",

"appId": "1fec8e78-bce4-4aaf-ab1b-5451cc387264",
```

Another difference between this and the UTA0304 campaign is that in this case, all subsequent access to the compromised account occurred via Mullad VPN exit nodes (versus the other observed VPS and Tor IP addresses). Based on these two factors, Volexity has chosen to track this activity under the UTA0307 alias, rather than CozyLarch or UTA0304.

Detecting Device Code Authentication

Volexity identified a way to reliably detect this attack through monitoring and analysis of Microsoft Entra ID sign-in logs. When a user enters a device code and subsequently authenticates, it results in a login to the application associated with the generated code. This can be a common application like Microsoft Office that is frequently accessed by users and would not be a reliable indicator. However, the good news is that Device Code Authentications result in the `authenticationProtocol` field being set with the value **`deviceCode`**.

The line below is what will appear in the JSON data in the Entra ID sign-in logs when a Device Code Authentication occurs:

> `“authenticationProtocol": "deviceCode",`

Volexity further noted that as authenticated sessions refresh and are kept alive, subsequent sign-ins that initially occurred via a `deviceCode` often do not have anything set for `authenticationProtocol,` but they contain the following entry:

> `“originalTransferMethod": "deviceCodeFlow",`

These values can be searched and filtered on in the Entra Admin center by adding filters for "Authentications Protocol" and "Original Transfer Method". The latter can be filtered in both *interactive* and *non-interactive* sign-ins. The frequency and legitimacy of these values occurring in the sign-in logs for a particular organization may vary, as this is a legitimate Microsoft feature. An organization can evaluate their risk and usage of these workflows, and potentially use this information as a proactive detection mechanism.

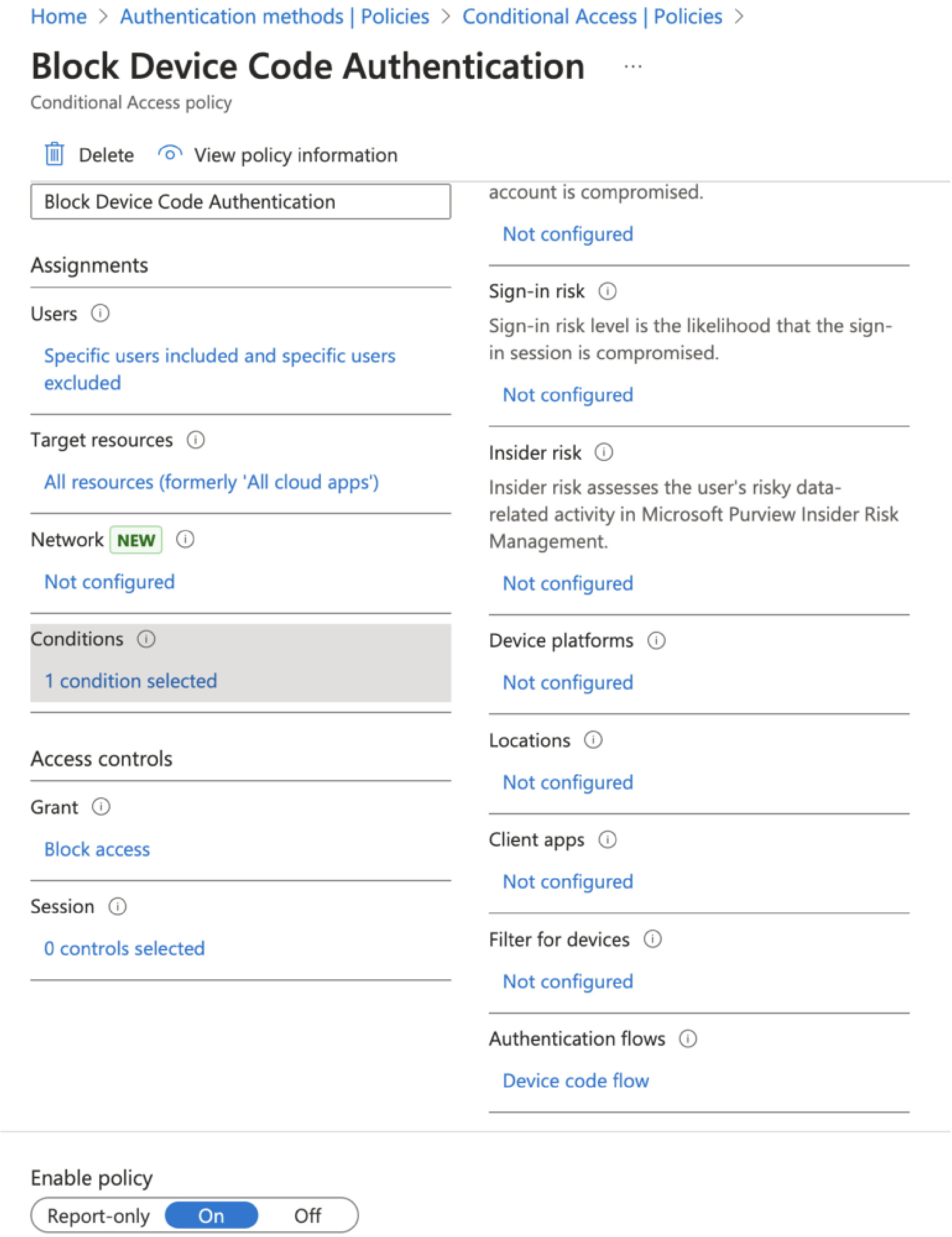
If an organization has the ability to monitor URLs that are being accessed by users or sent in email, there are additional detection opportunities to discover Device Code Authentication attacks. The following official URLs can be monitored for as related to Microsoft Device Code Authentication:

- `https://login.microsoftonline.com/common/oauth2/deviceauth`
- `https://www.microsoft.com/devicelogin`
- `https://aka.ms/devicelogin`

Organizations can monitor for access to these URLs or for their presence in various communication methods, such as email. Attackers can find other means to redirect users to these URLs, but one of the main advantages of using the list above in phishing attacks is that the URL displayed is hosted on a legitimate Microsoft domain.

Preventing Device Code Authentication

Volexity believes the most effective way to prevent this potential attack vector is through conditional access policies on an organization's M365 tenant. It is possible for organizations to create a conditional access policy that disallows device code authentication altogether. It is fairly trivial to set up, and Microsoft provides online guidance on exactly how to do this. Based on Volexity's own testing, blocking the "Device code flow" from "Authentications flows" prevents this attack from working. The image below shows what a conditional access policy would look like once it's set up and in place to block this authentication flow.



Home > Authentication methods | Policies > Conditional Access | Policies >

Block Device Code Authentication ...

Conditional Access policy

Delete   View policy information

Block Device Code Authentication

Assignments

Users

Specific users included and specific users excluded

Target resources

All resources (formerly 'All cloud apps')

Network NEW

Not configured

Conditions

1 condition selected

Access controls

Grant

Block access

Session

0 controls selected

account is compromised.

Not configured

Sign-in risk

Sign-in risk level is the likelihood that the sign-in session is compromised.

Not configured

Insider risk

Insider risk assesses the user's risky data-related activity in Microsoft Purview Insider Risk Management.

Not configured

Device platforms

Not configured

Locations

Not configured

Client apps

Not configured

Filter for devices

Not configured

Authentication flows

Device code flow

Enable policy

Report-only [✓ On] Off

Prior to implementing such a policy, organizations should evaluate the use of Device Code Authentication in their environment. This feature is used legitimately, and blocking it could have a negative impact. Volexity's review of its own customers identified several instances of legitimate access to resources via these means. However, at the majority of Volexity's customers, there was either no recent Device Code Authentication activity or there was only activity tied to the attacks described in this blog post.

Conclusion

Volexity continues to track multiple spear-phishing campaigns targeting Device Code Authentication. This blog post serves to cover a few of the larger and unique campaigns observed. Volexity has observed other similar spear-phishing campaigns in recent weeks targeting Device Code Authentication that it believes are the work of Russian threat actors. Further, it should be noted that it is possible this is the work of a single threat actor running multiple, different campaigns. However, at this time, Volexity believes this activity is sufficiently different enough to warrant tracking this activity under two different unknown threat actors and one it believes is likely CozyLarch.

While Device Code Authentication attacks are not new, they appear to have been rarely leveraged by nation-state threat actors . Volexity's visibility into targeted attacks indicates this particular method has been far more effective than the combined effort of years of other social-engineering and spear-phishing attacks conducted by the same (or similar) threat actors. It appears that these Russian threat actors have made a concerted effort to launch several campaigns against organizations with a goal of simultaneously abusing this method before the targets catch on and implement countermeasures.

The detection mechanisms and countermeasures to these attacks have been available for years. However, Volexity believes they are seldom implemented and that most organizations are not even aware of this authentication flow, let alone the means to detect its misuse. These attacks serve as a reminder that threat actors will constantly look for ways to abuse legitimate features, and organizations must continually evaluate and implement methods to detect and prevent such attacks.

These attacks also serve as a good opportunity to engage with users and remind them to be on the lookout for anything out of the ordinary when it comes to accessing resources when they are asked for login credentials or authorization grants. This phishing workflow has proven useful for an attacker, as many traditional sources of evidence and detection, both for a user and network defenders, are not present. For example:

1. There is no “malicious” link or attachment. The only link is to the provider’s infrastructure (in this case, Microsoft). This means users cannot easily identify the link as being suspicious, and automated solutions detecting malicious emails will likely fail to do so for the same reason.

2. Users are generally less aware of attacks that leverage legitimate services, and may be even less aware when it comes to those that involve entering a device code rather than their username or password.
3. After successful authentication, the logs will show the authenticating application as a legitimate or benign application, reducing signal that can be keyed off of in sign-in logs by detection teams.

These are items that organizations should look to further train users on and implement technical countermeasures against where possible.

Indicators associated with these campaigns are available on the Volexity GitHub.

If you believe you have been targeted by a similar attack and want to share details with Volexity for informational purposes, additional investigation, or incident response, please contact us.

> *Volexity's Threat Intelligence research, such as the content from this blog, is published to customers via its Threat Intelligence Service. The activity described in this blog post was shared with Volexity Threat Intelligence customers in TIB-20250206, TIB-20250211, and TIB-20250213.*
>
> *If you are interested in learning more about Volexity's services, including Network Security Monitoring and Incident Response, or our leading memory forensics solutions, Volexity Surge Collect Pro for memory acquisition and Volexity Volcano for memory analysis, please do not hesitate to contact us.*