Access granted: phishing with device code authorization for account takeover | Proofpoint US

By December 18, 2025 The Proofpoint Threat Research Team

Published: 2025-12-16 · Archived: 2026-04-05 13:18:17 UTC

Key findings

- Proofpoint is tracking multiple threat clusters - both state-aligned and financially-motivated - that are using various phishing tools to trick users into giving access to M365 accounts via OAuth device code authorization.
- Successful compromise leads to account takeover, data exfiltration, and more.
- Threat actors are using the OAuth 2.0 device authorization grant flow to compromise Microsoft 365 user accounts by approving access for various applications.

Overview

Social engineering is a tactic used by threat actors to trick a user into taking an action, for example adding an application on their system, or divulging confidential information. Techniques like ClickFix highlight how threat actors use security-themed issues to trick users into taking an action, leveraging legitimate tools and services to gain unauthorized access. Device code phishing is another way threat actors are abusing enterprise resources for account takeovers.

Proofpoint Threat Research has observed multiple threat clusters using device code phishing to trick users into granting a threat actor access to their Microsoft 365 account. In general, an attacker will socially engineer someone into logging into an application with legitimate credentials. The service generates a token that is then obtained by the threat actor. This gives them control over the M365 account.

Proofpoint has previously observed targeted malicious and limited red team activity leveraging device code phishing. But by September 2025, we observed widespread campaigns using these attack flows, which was highly unusual.

In recently observed activity, campaigns begin with an initial message with a URL embedded behind a button, as hyperlinked text, or within a QR code. When a user visits the URL, it initiates an attack sequence leveraging the legitimate Microsoft device authorization process. Once initiated, the user is presented with a device code. It is either presented directly on the landing page or received in a secondary email from the threat actor. The lures typically claim that the device code is an OTP and direct the user to input the code at Microsoft's verification URL. Once the user inputs the code, the original token is validated, giving the threat actor access to the targeted M365 account.

In observed campaigns, some messages directly claim to be token re-authorization notifications, while others use different lures to trick the user into clicking a URL, which leads to an attack chain that ends with application authorization.

While this is not necessarily a novel technique, it is notable to see it used increasingly by multiple threat clusters including a tracked cybercriminal threat actor, TA2723. Proofpoint threat researchers have identified a malicious application for sale on hacking forums, which could be used for this type of campaign. Additionally, red team tools are available – such as Squarephish and SquarephishV2– that can be used for this type of attack. These tools help threat actors mitigate the short-lived nature of device codes, enabling larger campaigns than were previously possible.

The tools

SquarePhish2 Tool

SquarePhish is a phishing tool that enables threat actors to target the OAuth Device Grant Authorization flow in combination with QR codes to compromise Microsoft accounts. It was originally published in 2022 by Dell SecureWorks. In 2024, an updated version – SquarePhish2 – was published on GitHub by an independent researcher. The attack chain is effective because it mimics the legitimate process that a user would follow to configure TOTP multifactor authentication. The attack begins with a phishing email containing a QR code that directs users to a website hosted on an attacker-controlled SquarePhish2 server. Upon scanning the QR code, the user is redirected to Microsoft's legitimate authentication page, while the server initiates the OAuth Device Authorization Grant flow using a preconfigured client ID.

A second email is then sent to the user from a Microsoft tenant, containing the device code, prompting them to complete the authentication process. SquarePhish2 can also automatically redirect users to the verification page, without needing to prompt for a second email. Once the user enters the code and authenticates, the tool polls the Microsoft endpoint for access. While SquarePhish2 offers advanced capabilities, its user-friendly configuration and automation features mean that it does not require deep technical expertise to operate, making it accessible to a broader range of threat actors. The ultimate objective is unauthorized access to sensitive Microsoft account data, enabling further exploitation such as account takeover, lateral movement, data exfiltration, or persistence within targeted environments.

Graphish tool

Threat actors have increasingly adopted tools like the Graphish phishing kit to target Microsoft accounts with efficiency. The tool was shared in criminal hacking forums, where members are vetted, and made available for free. This tool has a multitude of capabilities, including facilitating the creation of highly convincing phishing pages by leveraging Azure App Registrations and reverse proxy setups for adversary-in-the-middle (AiTM) attacks, hosted on attacker-controlled infrastructure. A typical AiTM attack begins with the user receiving a phishing message containing a link to a malicious webpage design to mimic a legitimate login page. The fake domain is connected to a reverse proxy server, which relays traffic between the user and the actual service. When the user enters their credentials, they are instantly intercepted by the attacker. If the user successfully completes an MFA challenge (like entering a one-time code), this enables a complete session hijacking.

The attack requires the actor to own a domain name and register an SSL certificate, to enhance the credibility of the phishing site. By registering an application in Azure and extracting the client ID, the attacker can initiate OAuth-based phishing attempts that prompt users to grant access to their Microsoft accounts. For targeting enterprise environments, the tool includes guidance on bypassing organizational restrictions by verifying the malicious app with Azure, which increases its success rate against accounts. Similar to Squarephish, the tool is designed to be user-friendly and does not require advanced technical expertise, lowering the barrier for entry and enabling even low-skilled threat actors to conduct sophisticated phishing campaigns. The ultimate objective is unauthorized access to sensitive personal or organizational data, which can be exploited for credential theft, account takeover, and further compromise.

Campaigns

"Salary Bonus + Employer Benefits Reports 25"

Proofpoint tracks multiple campaigns leveraging OAuth device code phishing. For example, on 8 December, researchers identified a campaign that used a shared document reminder alert to trick users into clicking a Google Share URL hyperlinked as text, to access a fictitious document called "Salary Bonus + Employer Benefit Reports 25". Email messages were sent from attacker-controlled addresses and claimed to be the file.

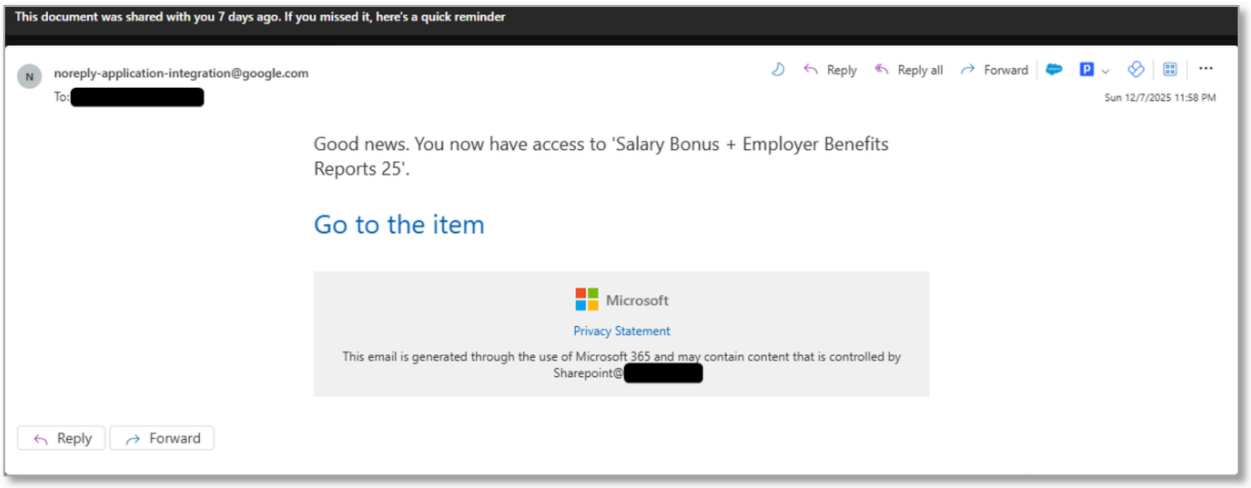

Figure 1: *Example of phishing message purporting to be "Salary Bonus + Employer Benefits Reports 25".*

Once clicked, the URL embedded in the email leads the user to an attacker-controlled website with a domain that is localized according to browsing IP and shows the targeted company branding. The website prompts the user to input their email address. Once done, the user is presented with a pop-up to "complete secure authentication" that includes a code and directions to input that code on the legitimate Microsoft device authorization page - hxxps://microsoft.com/devicelogin. This pop-up is purporting to be for MFA-token secure authentication. However, inputting the provided code into the Microsoft-provided OAuth page provides the threat actor access to the user's Microsoft 365 account.

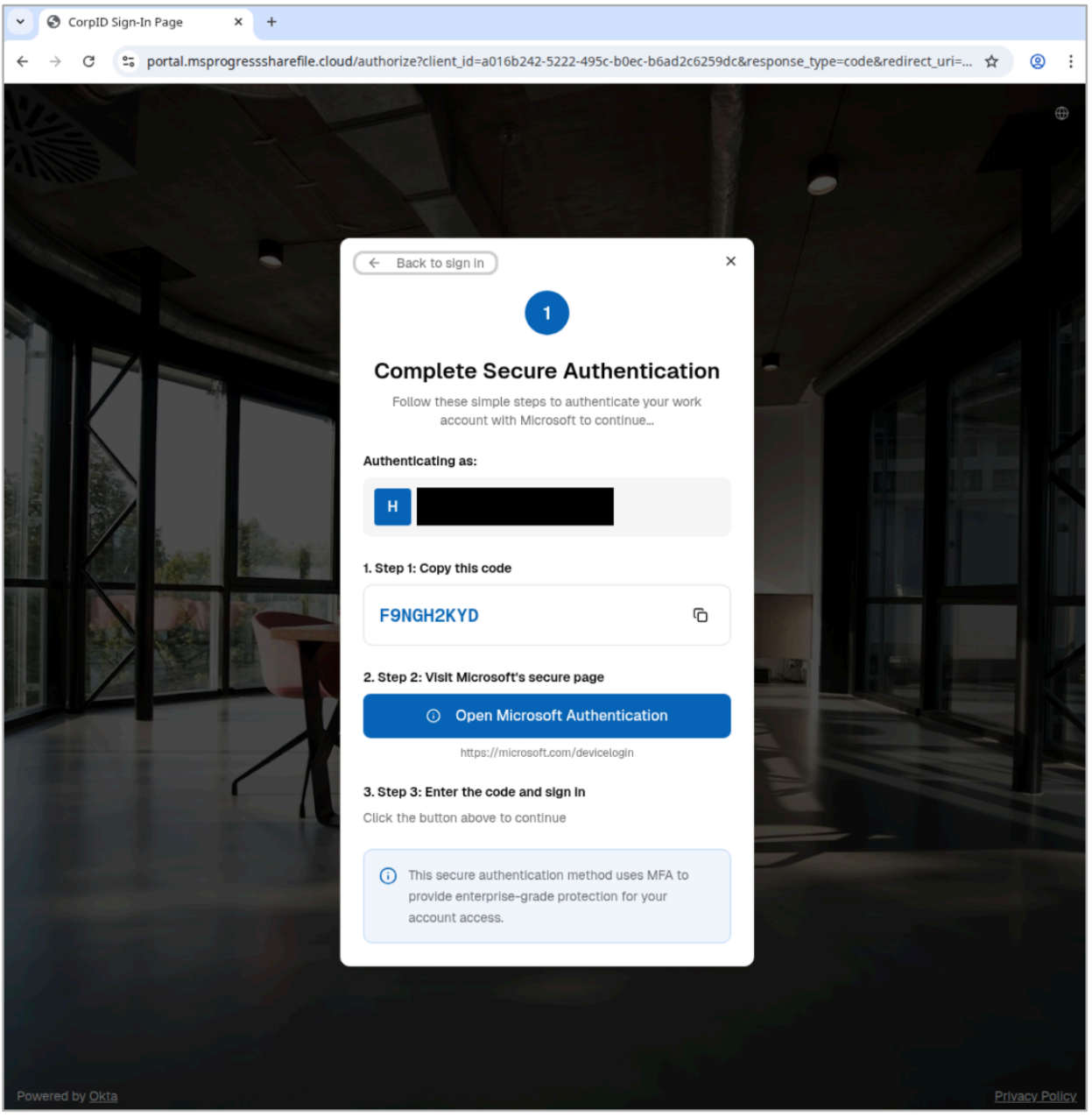

Figure 2: *Redirection to adding authorized device.*

TA2723

TA2723 is a financially-motivated, high-volume credential phishing threat actor that is notable for its campaigns spoofing Microsoft OneDrive, Linkedin and DocuSign. Beginning October 2025, Proofpoint Threat Research observed TA2723 conducting OAuth device code phishing.

In one campaign from 9 to 10 October, the email messages purported to be “[organization name] OCTOBER_SALARY_AMENDED RefID:6962_yslFRVQnQ”. The email message body appeared as if a document had been shared with the recipient and was customized to show the recipient’s name and the name of the shared file, consistent with the subject line. The message contained a virtoshare.com URL embedded as a “button” to Open the file.

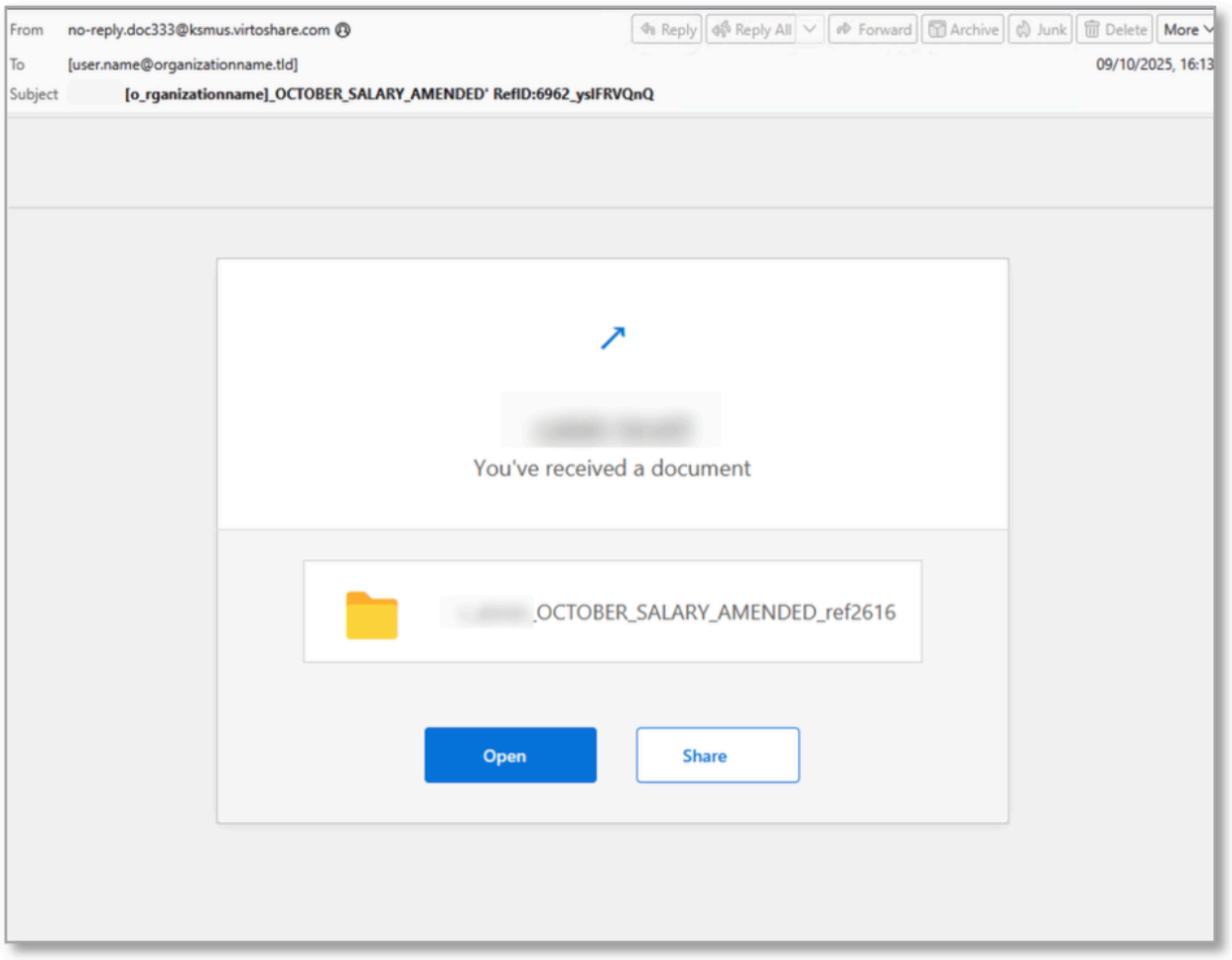

Figure 3: *Example TA2723 email message.*

When clicked, the recipient is redirected to a device code authorization page where they are prompted to input their email address and click a button to generate the one-time passcode (OTP).

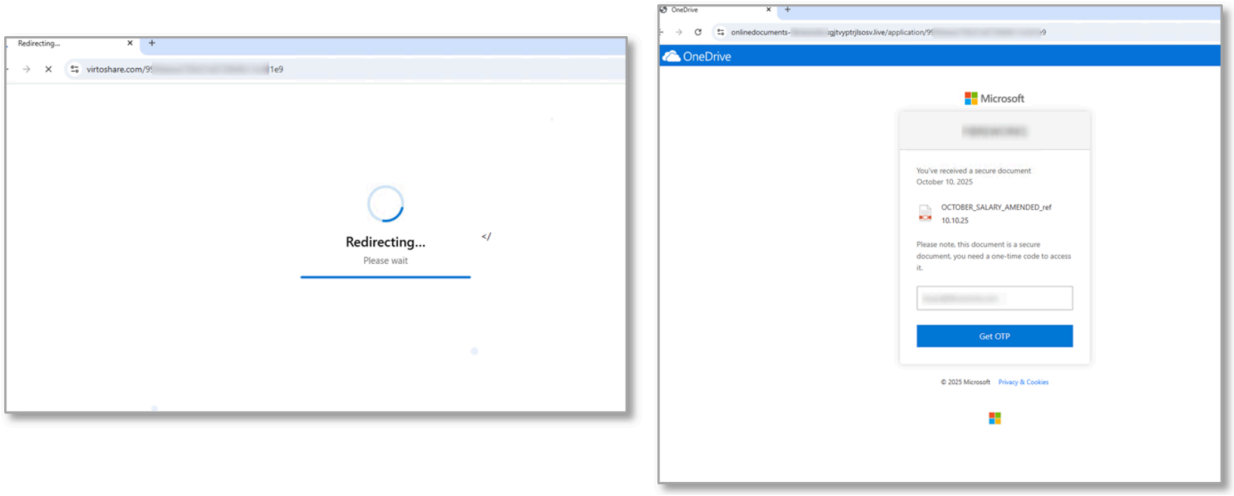

Figure 4: *URL redirect from email message to OTP generation site*

When clicked, the URL behind this button - which then shows as “Access Document” - is updated to redirect the user to the legitimate device authorization page from Microsoft, where they will have authorized access to the attacker-controlled application.

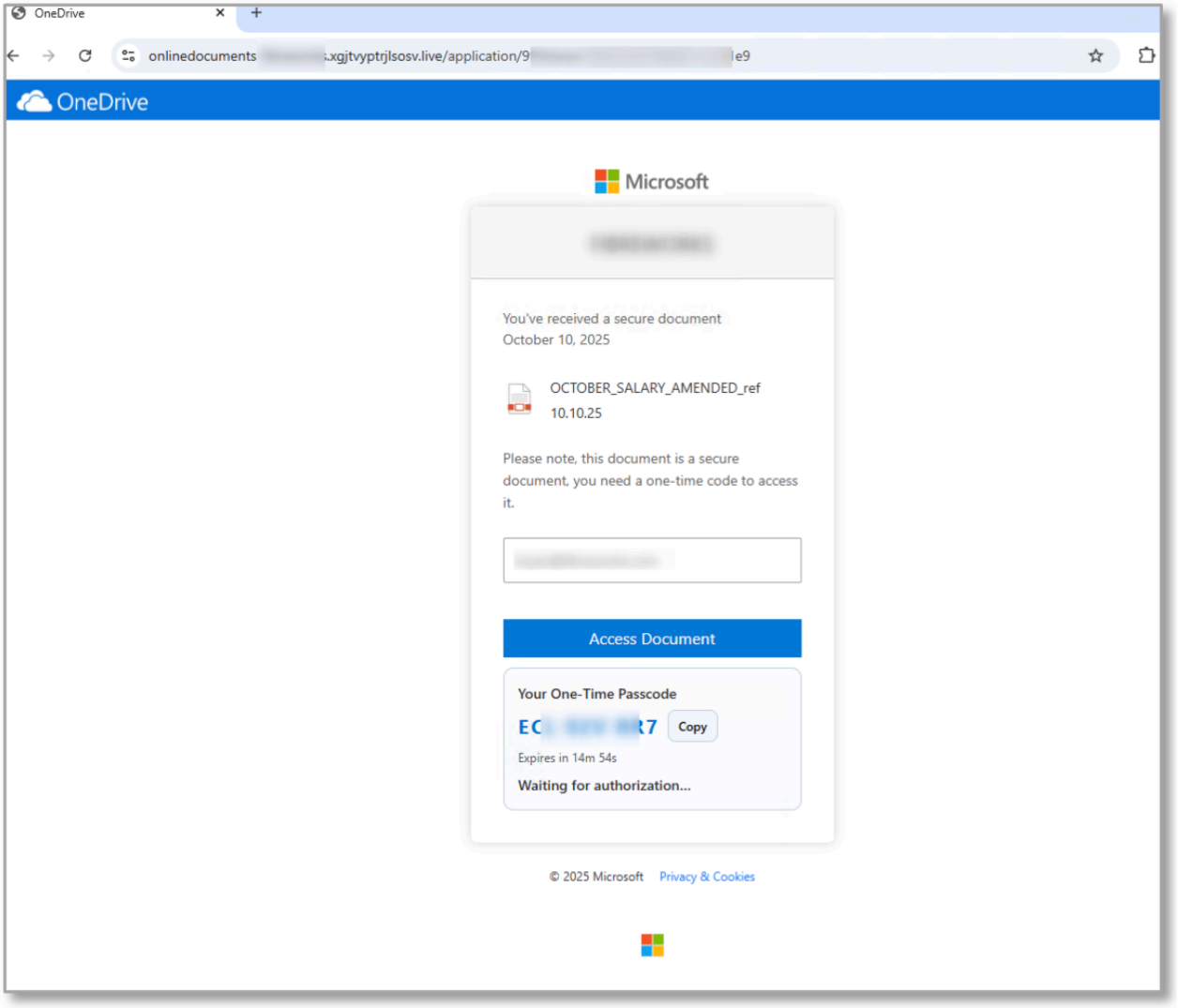

Figure 5: *OTP and updated 'Access Document' button URL redirect.*

Proofpoint Threat Research suspects that SquarePhish2 could have been used in this TA2723 campaign from 6 to 8 October, and the Graphish kit could have been used in a second wave of this campaign from 9 to 10 October. The assessment is due to the timing and evolution of the campaigns, TTP changes, and that the Graphish kit had been recently published on the vetted forum in the prior weeks. A successful attack would enable the threat actor to have access to the user's M365 account, which could lead to account takeover, data exfiltration, lateral movement, and other follow-on activity.

State-aligned threat actors using device code phishing

Since January 2025, Proofpoint Threat Research has tracked multiple state-aligned threat actors abusing OAuth device code authorization for account takeover, which aligns with a wider trend of state-aligned threat actors increasingly adopting password-less phishing techniques. This technique has been most widely used by Russia-aligned threat actors, as noted in prior public reporting by Volexity covering the initial adoption of this technique. We have also observed suspected China-aligned activity and other unattributed espionage campaigns using this attack vector.

State-aligned threat actors often conduct patient rapport building via benign outreach prior to a device code phishing attempt, with some campaigns showing evidence of multi-channel targeting via both email and other communication

channels. One particularly notable threat actor we have observed conducting device code phishing since at least September 2025 is a suspected Russia-aligned group we are tracking as UNK_AcademicFlare.

UNK_AcademicFlare activity

Since September 2025, Proofpoint has observed UNK_AcademicFlare using compromised email addresses belonging to multiple government and military organizations to target entities within government, think tank, higher education, and transportation sectors in the U.S. and Europe. Typically, these compromised email addresses are used to conduct benign outreach and rapport building related to the targets' area of expertise to ultimately arrange a fictitious meeting or interview. The threat actor then claims to share a document with questions or topics for the target to review. To do so, they provide a link to a Cloudflare Worker URL that spoofs a OneDrive account associated with the compromised sender's organization, which leads to a device code phishing workflow.

Figure 6: *UNK_AcademicFlare benign conversation starter.*

Figure 7: *UNK_AcademicFlare email linking to Cloudflare worker URL.*

In the above example, UNK_AcademicFlare sent a benign conversation starter email to an individual working for a U.S. university using a compromised Zambian government email address. The threat actor later provided a link to a Cloudflare Worker domain spoofing a Zambian government OneDrive account: onedrive[.]gov-zm[.]workers[.]dev.

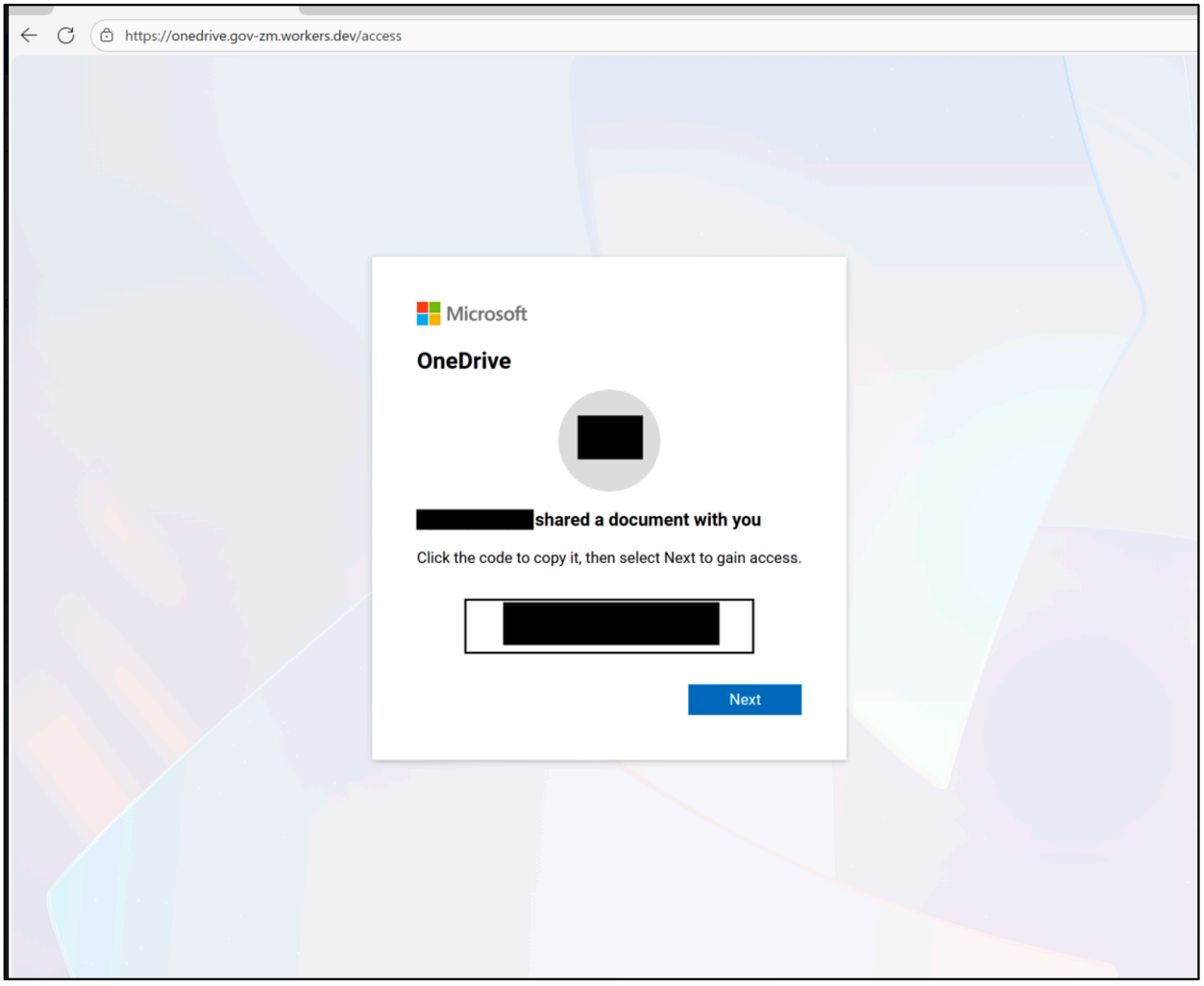

Figure 8: *UNK_AcademicFlare Cloudflare worker device code landing page.*

This link redirects to a landing page stating that the sender has shared a document and instructs the user to copy the provided code and click 'Next' to gain access. The presented code is a unique device code that is dynamically generated for the target and clicking 'Next' redirects the user to the Microsoft device code login URL hxxps://login.microsoftonline[.]com/common/oauth2/deviceauth.

Proofpoint assesses that UNK_AcademicFlare is likely a Russia-aligned threat actor based on the targeting of Russia-focused specialists at multiple think tanks, as well as government and energy sector organizations in Ukraine. This assessment is further supported by the actor's repeated use of Russia and Ukraine-themed lure content and reliance on device code phishing techniques.

Recommendations

Block device code flow where possible

The strongest mitigation is to create a Conditional Access policy using the Authentication Flows condition to block device code flow for all users. Conditional Access policies can first be deployed in a report only mode, or the 'Policy impact'

viewed over historic sign in log records, to determine the impact for an environment.

If blocking device code flow completely is not feasible, Conditional Access can be used to create an allow-list approach based on accepted use cases. For example, only enabling device code authentication for approved users, operating systems, or IP ranges such as using ‘Named locations’.

Require compliant or joined devices

If organizations use device registration or Intune, Conditional access policies requiring that sign ins originate from a compliant or registered device will protect users from device code phishing. This should be deployed as a defense in depth strategy, as there will likely be exclusions from this requirement, when compared with a dedicated device code flow policy.

Enhance user awareness regarding device code phishing attacks

Traditional phishing awareness often emphasizes checking URLs for legitimacy. This approach does not effectively address device code phishing, where users are prompted to enter a device code on the trusted Microsoft portal hxxps://microsoft.com/devicelogin. User training should include guidance on not entering device codes received from untrusted sources.

Conclusion

From the use of malicious OAuth applications for persistent access to the abuse of legitimate Microsoft authentication flows with device codes, threat actors’ tactics to achieve account takeover are evolving with quick adoption across the threat landscape. These campaigns rely heavily on social engineering, most often using lures with embedded URLs or QR codes to trick users into thinking they are securing their accounts. Proofpoint tracks multiple threat clusters that are using this device code authentication technique and recommends that organizations strengthen OAuth controls and enhance user awareness and education about these evolving threats. Proofpoint assesses that the abuse of OAuth authentication flows will continue to grow with the adoption of FIDO compliant MFA controls.

Indicators of compromise

Campaign Indicators			
Indicator	**Type**	**Description**	**First Seen**
hxxps://sharefile.progressivesharepoint.top/	URL	Phishing landing page	20-Oct-2025
hxxps://progressiveweba.z13.web.core.windows.net	URL	Redirector	20-Oct-2025

hxxps://agimplfundmgt.z13.web.core.windows.net	URL	Redirector	20-Oct-2025
hxxps://blackrockfundmgt.z13.web.core.windows.net	URL	Redirector	20-Oct-2025
robert.pena@FirstTrustAdvisorsLP.onmicrosoft.com	Email address	Sender email address	20-Oct-2025
hxxps://onlinedocuments-[OrganizationName].vxhwuulcnfzlfmh.live/application/a[PII_Linkable_hex]9	URL	Device code generation landing page	14-Oct-2025
hxxps://onlinedocuments-[OrganisationName].vxhwuulcnfzlfmh.live/token/request?id=a[PII_Linkable_hex]9	URL	OTP generation	14-Oct-2025
xgjtvyptrjlsosv.live	Domain	OTP generation	9-Oct-2025
196.251.80.184	IP	OTP generation	9-Oct-2025
vaultally.com	Domain	Sender email domain	14-Oct-2025
docifytoday.com	Domain	Sender email domain	14-Oct-2025

filetix.com	Domain	Sender email domain	14-Oct-2025
nebulafiles.com	Domain	Sender email domain	14-Oct-2025
novodocument.com	Domain	Sender email domain	14-Oct-2025
spacesdocs.com	Domain	Sender email domain	14-Oct-2025
hxxps://www.vaultaliy.com/a[PII_Linkable_hex]9	URL	Link in email message	14-Oct-2025
hxxps://www.virtoshare.com/99[PII_Linkable]e9	URL	Link in email message	9-Oct-2025
hxxps://onlinedocuments-[OrganisationName].xgjtvyptrjlsosv.live/application/99[PII_Linkable]e9	URL	Device code generation landing page	9-Oct-2025
hxxps://onlinedocuments-[OrganisationName].xgjtvyptrjlsosv.live/token/request?id=99[PII_Linkable]e9	URL	OTP generation	9-Oct-2025
no-reply.doc333@ksmus.virtoshare.com	Email address	Sender email address	9-Oct-2025

acxioswan.com	Domain	Sender email domain	9-Oct-2025
acxishare.com	Domain	Sender email domain	9-Oct-2025
collabodex.com	Domain	Sender email domain	9-Oct-2025
infoldium.com	Domain	Sender email domain	9-Oct-2025
hxxps://www.renewauth.com/3a[PII_Linkable]59	URL	Link in email message	6-Oct-2025
hxxps://www.myfilepass.com/69[PII_Linkable]ed	URL	Link in email message	6-Oct-2025
hxxps://login.microsoftonline.com/common/oauth2/deviceauth[Abused]	URL	Device code prompt	6-Oct-2025
renewauth.com	Domain	Sender email domain	6-Oct-2025
myfilepass.com	Domain	Sender email domain	6-Oct-2025

confidentfiles.com	Domain	Sender email domain	6-Oct-2025
magnavite.com	Domain	Sender email domain	6-Oct-2025
97d7e46b-1bff-4f24-b262-8b0b3914d88a.us5.azurecomm.net	URL	Device code message sender	6-Oct-2025
bluecubecapital.com	Domain	Sender email address domain	29-Sept-2025
allspringglobalinvestmentsllc.onmicrosoft.com	Domain	Sender email address domain	29-Sept-2025
aresmanagementllc.onmicrosoft.com	Domain	Sender email address domain	29-Sept-2025
citadeladvisorsllc.onmicrosoft.com	Domain	Sender email address domain	29-Sept-2025
cpuhp.onmicrosoft.com	Domain	Sender email address domain	29-Sept-2025
millenniummanagementllc.onmicrosoft.com	Domain	Sender email address domain	29-Sept-2025

hxxps://clientlogin.blitzcapital.net/	URL	Device code prompt	29-Sept-2025
hxxps://onedrive[.]gov-zm[.]workers[.]dev	URL	Redirector	5-Nov-2025
hxxps://portal.msprogresssharefile.cloud/	URL	Landing Page	2-Dec-2025
hxxps://sharingfilesystems.z13.web.core.windows.net	URL	Redirector	2-Dec-2025
hxxps://myapplicationinterfaces.s3.eu-north-1.amazonaws.com/index.html	URL	Redirector	2-Dec-2025
hxxps://corphostedfileservices.s3.eu-north-1.amazonaws.com/auth.html	URL	Redirector	2-Dec-2025

References

https://aadinternals.com/post/phishing/#new-phishing-technique-device-code-authentication

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

https://www.secureworks.com/blog/oauths-device-code-flow-abused-in-phishing-attacks

https://github.com/nromsdahl/squarephish2

https://www.praetorian.com/blog/introducing-github-device-code-phishing/

https://www.calypt.com/blog/index.php/a-phishing-technique-for-compromising-office-365-azure-ad-accounts/

https://0xboku.com/2021/07/12/ArtOfDeviceCodePhish.html

https://learn.microsoft.com/en-us/entra/identity-platform/v2-oauth2-device-code