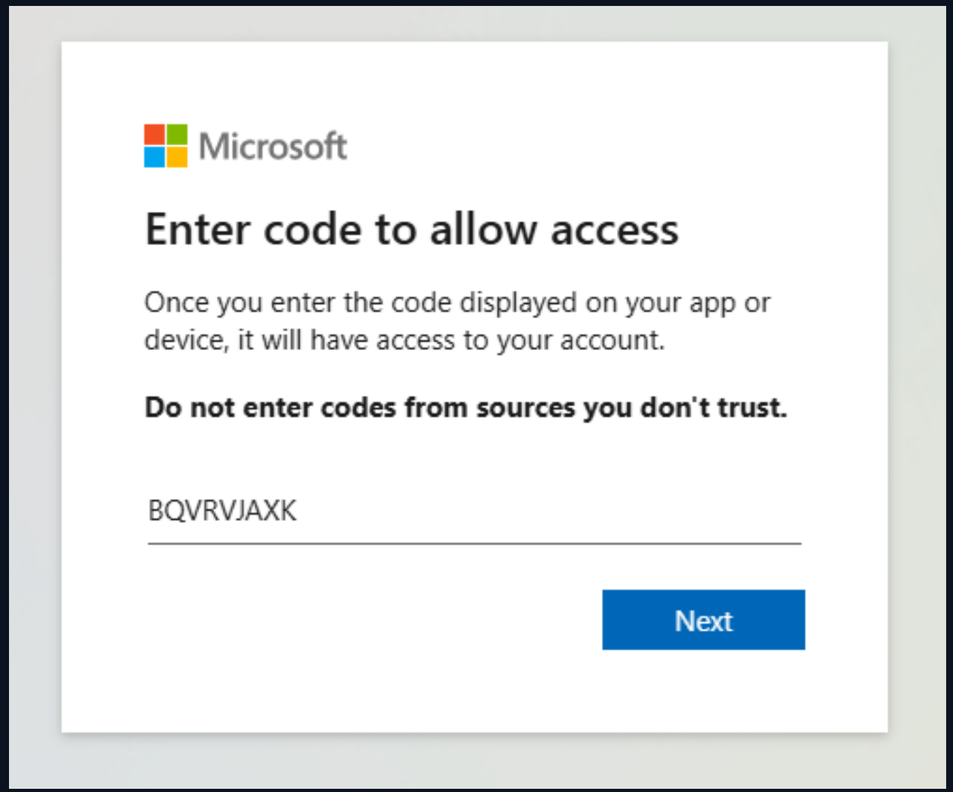
Device Code Phishing

Attack, Detect, Prevent

Ryan O’Donnell
in/odonnell-ryan/

Agenda

1. Background
2. Attack Demo
3. Detection
4. Prevention
5. Resources



Current Events

Research Threat intelligence Microsoft Defender Social engineering / phishing ·

10 min read

Storm-2372 conducts device code phishing campaign

By Microsoft Threat Intelligence

Microsoft Threat Intelligence blog

Phishing Lures

Storm-2372's device code phishing campaign has been active since August 2024. Observed early activity indicates that Storm-2372 likely targeted potential victims using third-party messaging services including WhatsApp, Signal, and Microsoft Teams, falsely posing as a prominent person relevant to the target to develop rapport before sending subsequent invitations to online events or meetings via phishing emails.

Microsoft Threat Intelligence blog

Post-Compromise

Additionally, Microsoft observed Storm-2372 using Microsoft Graph to search through messages of the account they've compromised. The threat actor was using keyword searching to view messages containing words such as username, password, admin, teamviewer, anydesk, credentials, secret, ministry, and gov. Microsoft then observed email exfiltration via Microsoft Graph of the emails found from these searches.

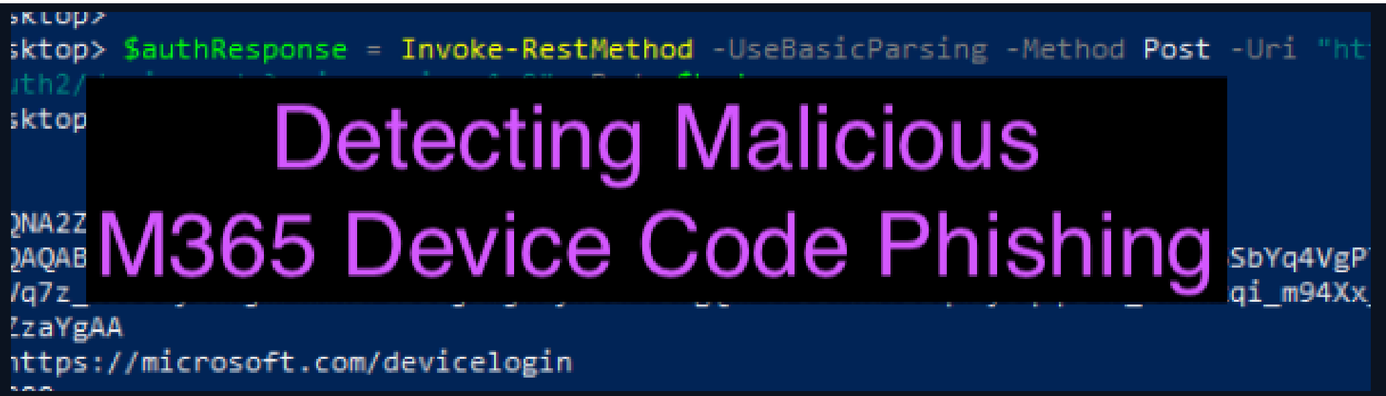
Microsoft Threat Intelligence blog

Attack

- Authentication happens in Microsoft space
- Trick users to log into apps and capture tokens
- Bypasses traditional phishing protections
  - MFA, phishing “resistant” auth
- Abuses a legitimate authentication flow
  - No fancy malware, suspicious URL, or exploitation

Research

Volexity blog
Charlie Gardner, Steven Adair, Tom Lancaster (2025)

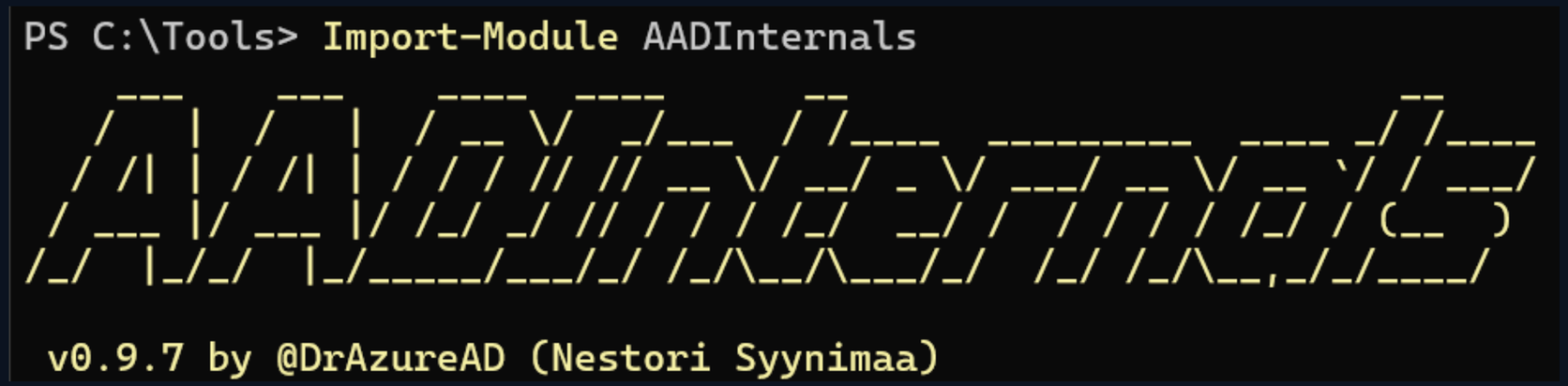


Detecting Malicious Device Code Phishing
Lina Lau (2022)

The Art of the Device Code Phish
Bobby Cooke (2021)

History

- Discovered by Dr. Nestori Syynimaa (@DrAzureAD)
- New phishing technique: device code authentication



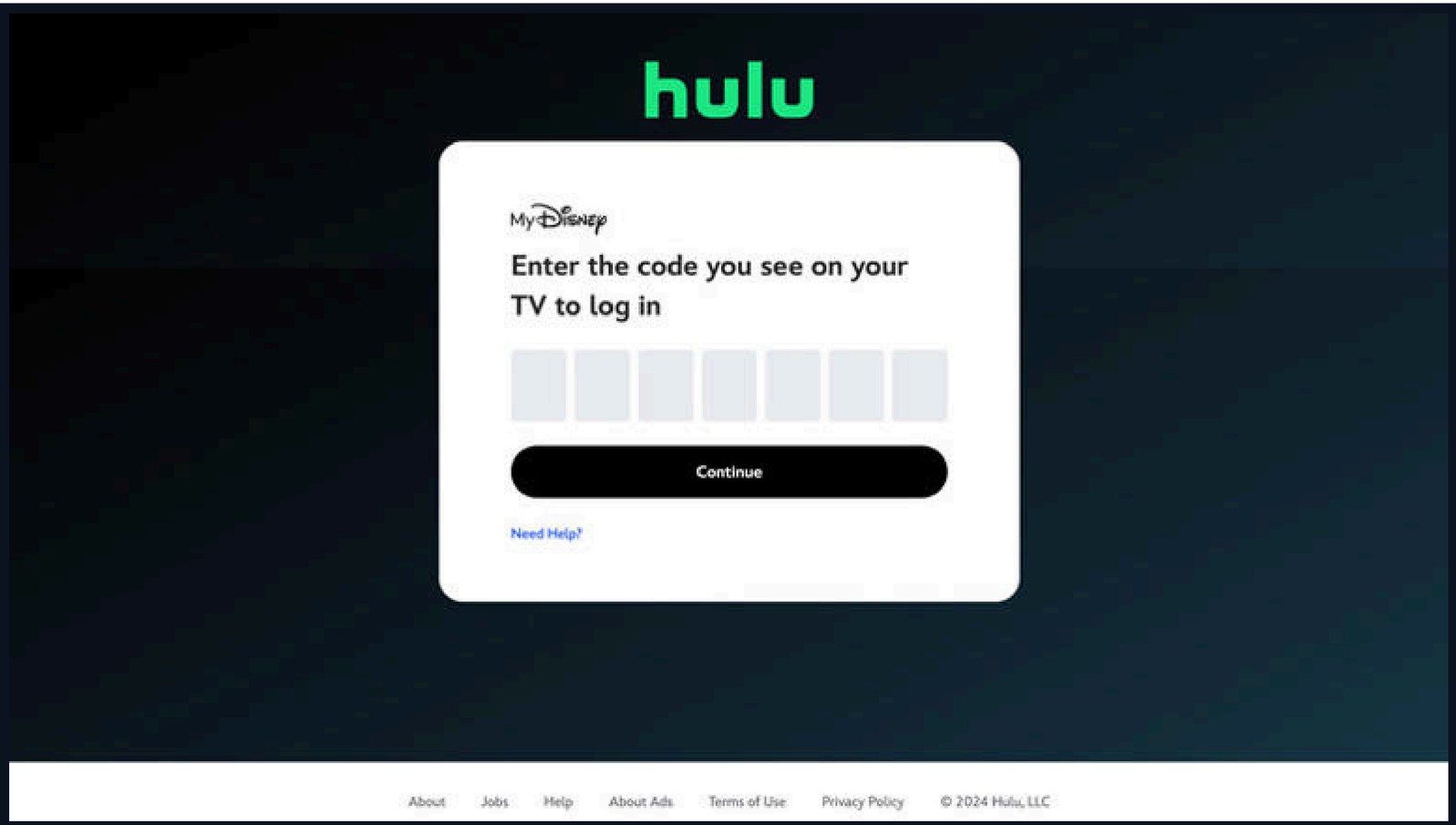
Purpose

OAuth 2.0 Device Authorization Grant

Abstract

> The OAuth 2.0 device authorization grant is designed for Internet-connected devices that either lack a browser to perform a user-agent-based authorization or are input constrained to the extent that requiring the user to input text in order to authenticate during the authorization flow is impractical. It enables OAuth clients on such devices (like smart TVs, media consoles, digital picture frames, and printers) to obtain user authorization to access protected resources by using a user agent on a separate device.

Example


hulu
MyDisney
Enter the code you see on your TV to log in
Continue
Need Help?
About
Jobs
Help
About Ads
Terms of Use
Privacy Policy
© 2024 Hulu, LLC

Legitimate Usage

Azure CLI

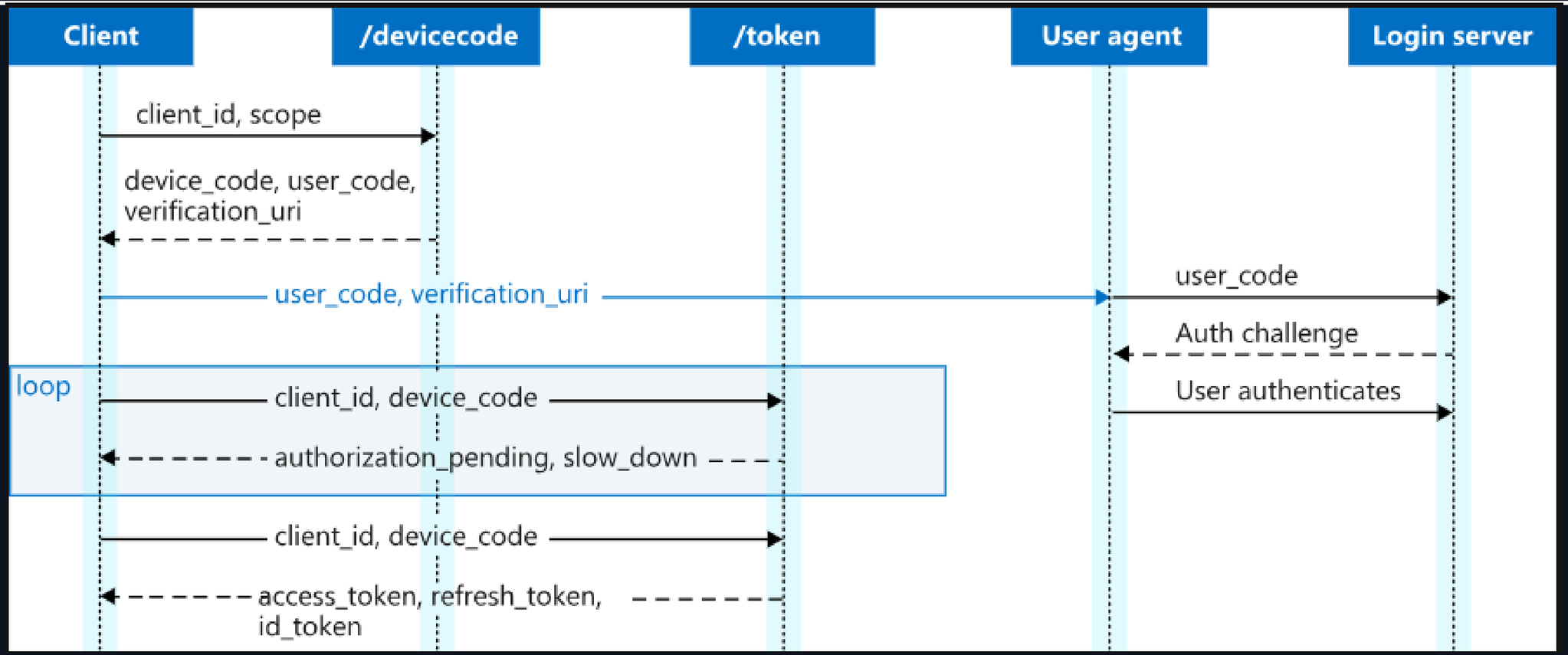
```
PS C:\Tools> az login --use-device-code
To sign in, use a web browser to open the page
https://microsoft.com/devicelogin and enter the
 code EB58NT4A2 to authenticate.
```

Az PowerShell

```
PS C:\Tools> Connect-AzAccount -UseDeviceAuthentication
WARNING: You may need to login again after updating "En
ableLoginByWam".
Please select the account you want to login with.

[Login to Azure] To sign in, use a web browser to open
the page https://microsoft.com/devicelogin and enter th
e code BZRDVF2BH to authenticate.
```

Device Code Flow



Microsoft identity platform and the OAuth 2.0 device authorization grant flow

Verification URI

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

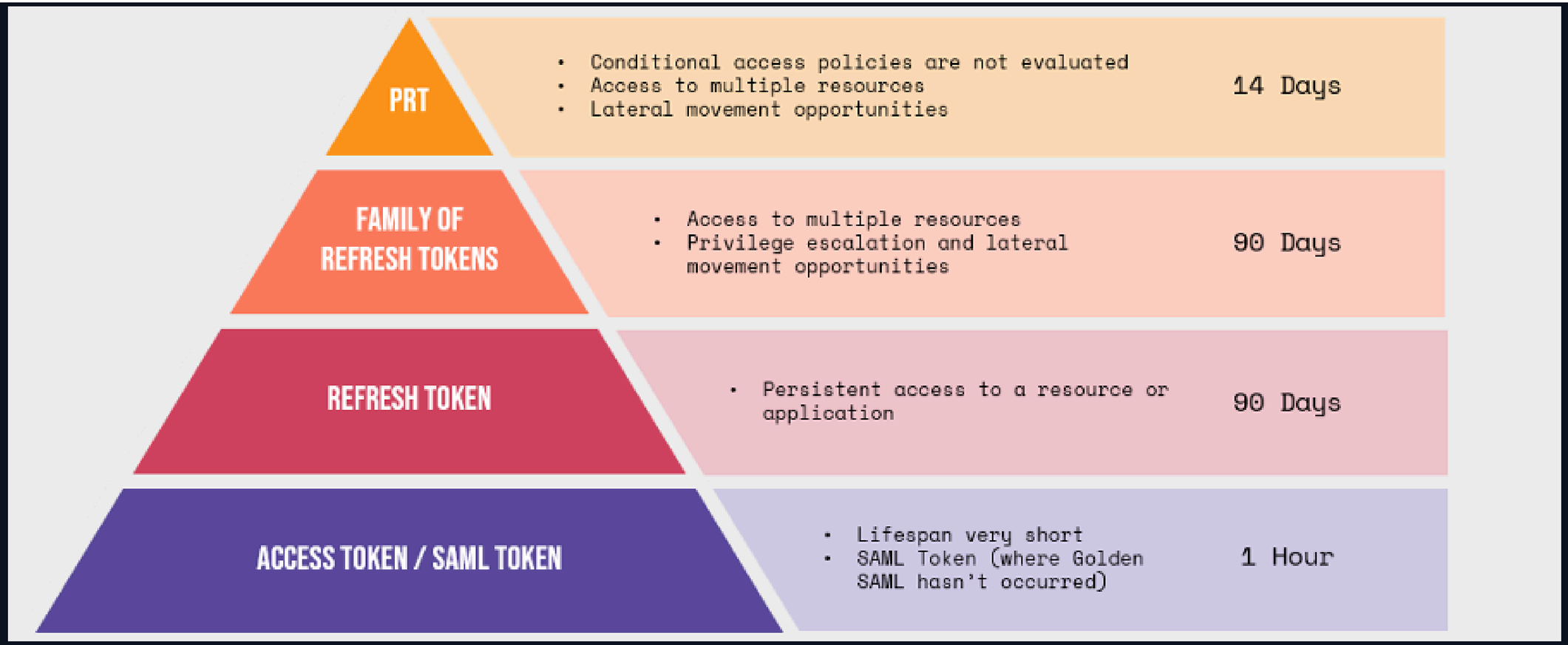
Attack Demo

PRT Phish

February 14, 2025 update:

Within the past 24 hours, Microsoft has observed Storm-2372 shifting to using the specific client ID for Microsoft Authentication Broker in the device code sign-in flow. Using this client ID enables Storm-2372 to receive a refresh token that can be used to request another token for the device registration service, and then register an actor-controlled device within Entra ID. With the same refresh token and the new device identity, Storm-2372 is able to obtain a Primary Refresh Token (PRT) and access an organization's resources. We have observed Storm-2372 using the connected device to collect emails.

Tokens


PRT
• Conditional access policies are not evaluated
• Access to multiple resources
• Lateral movement opportunities
14 Days
FAMILY OF REFRESH TOKENS
• Access to multiple resources
• Privilege escalation and lateral movement opportunities
90 Days
REFRESH TOKEN
• Persistent access to a resource or application
90 Days
ACCESS TOKEN / SAML TOKEN
• Lifespan very short
• SAML Token (where Golden SAML hasn't occurred)
1 Hour

Primary Refresh Tokens

- Primary Refresh Tokens are Single Sign On tokens
- Unique to each **device/user** combination
- Functions like a long-term ticket-granting ticket (TGT)
  - Valid for 14 days
- Can be used to sign in to **any application**
  - any **Entra connected website**
- Rather than per application

Attack Demo 2

Upcoming Changes

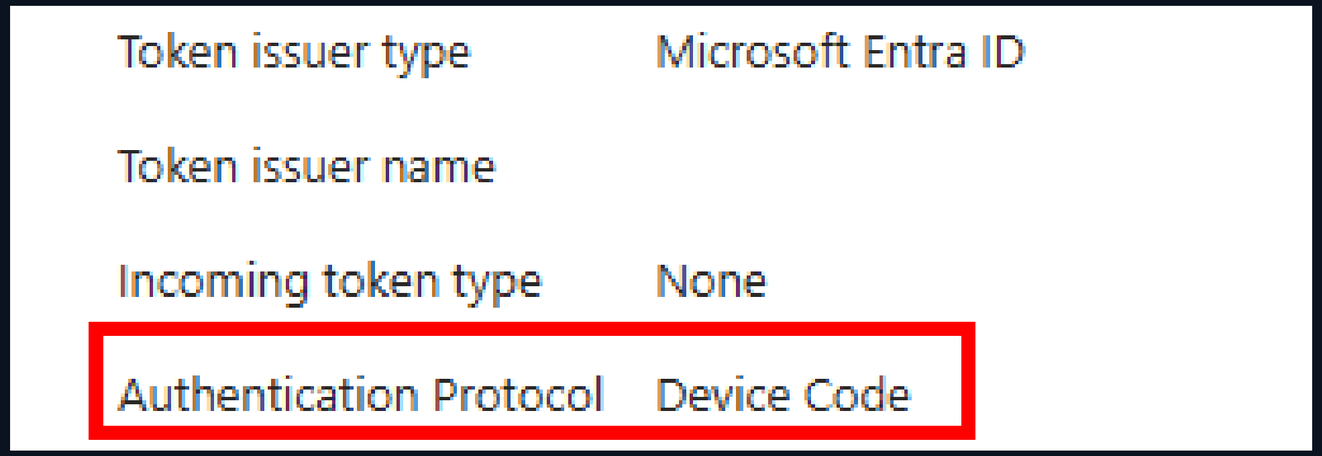
- New Microsoft-managed Policy
  - **Block Device Code Flow**

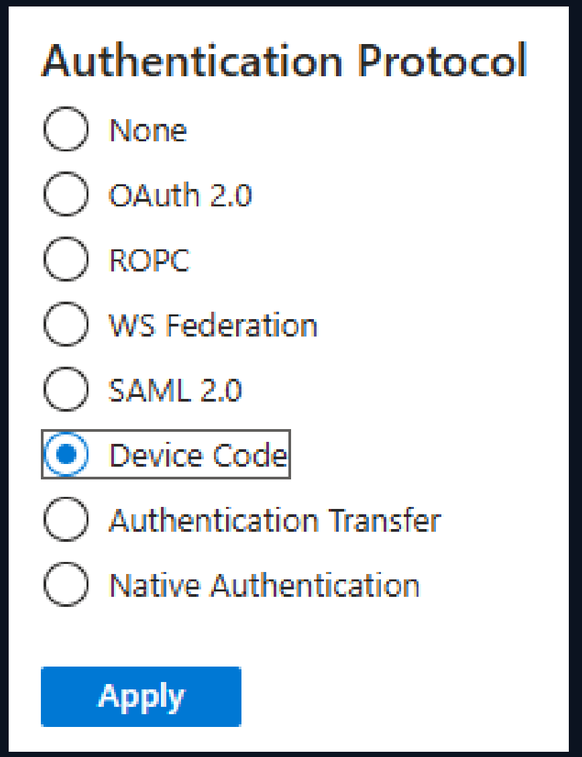
their device, thereby sending the user's tokens to the attacker. Given the security risks and the infrequent use of device code flow across our customer base, we are introducing a policy to block this flow by default for customers that have not used device code flow in the past 25 days.

New Microsoft-managed policies to raise your identity security posture

Detection

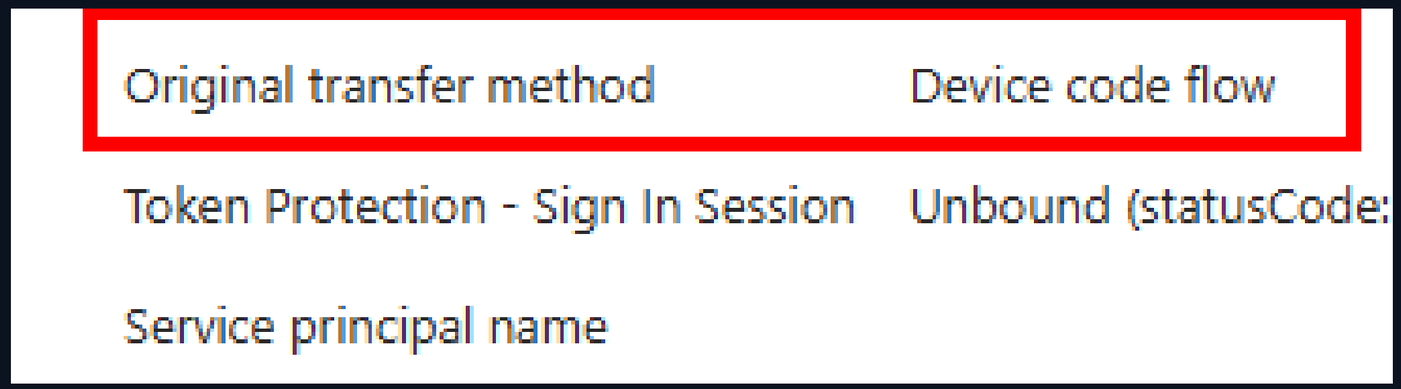
- **Authentication Protocol** = **Device Code**
- Interactive Sign-in Logs

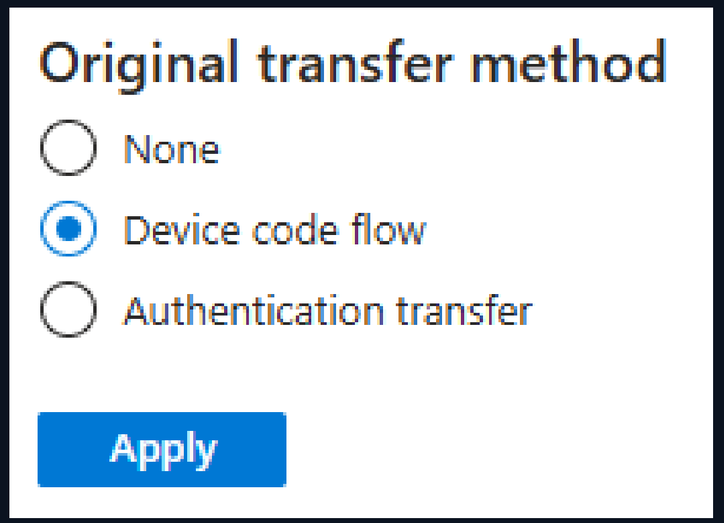




Detection

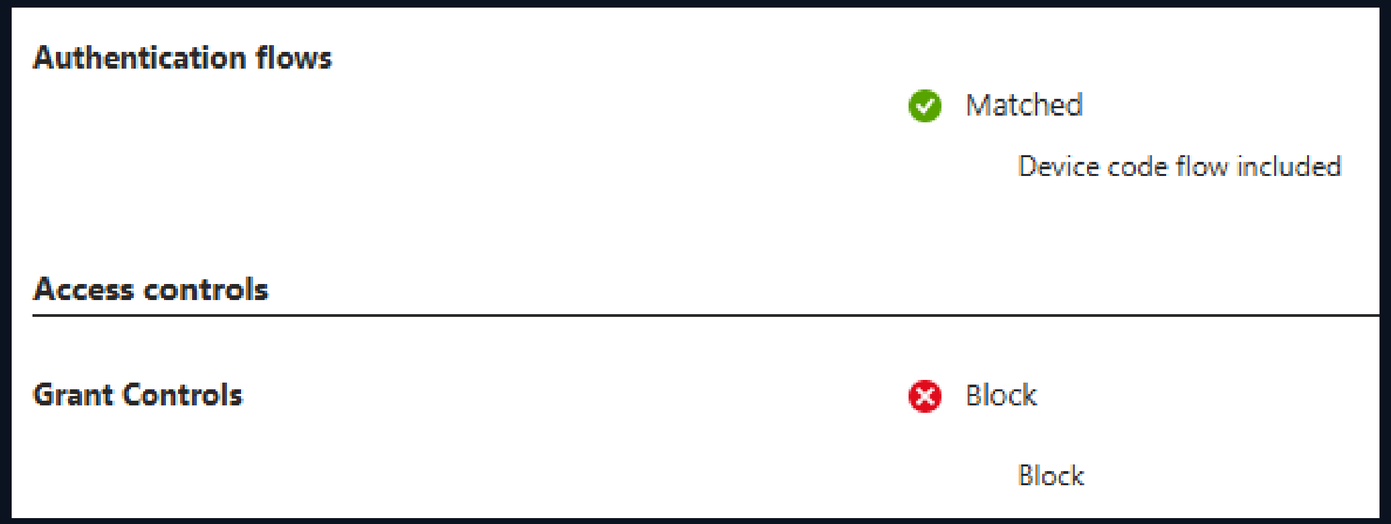
- **Original transfer method** = **Device code flow**
- Interactive Sign-in Logs
- Non-Interactive Sign-in Logs

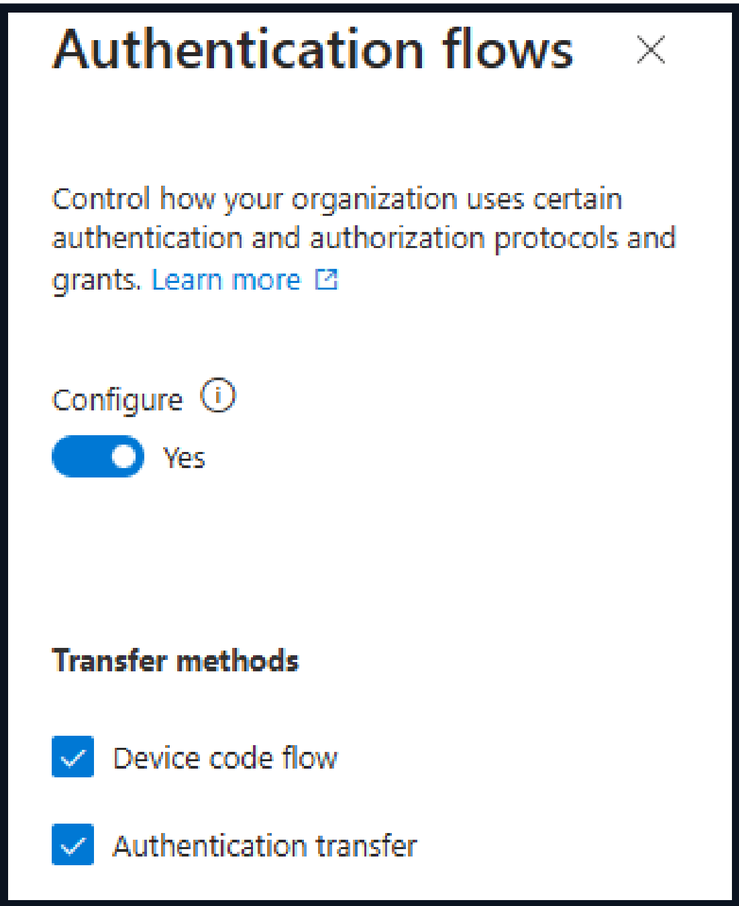




Prevention

- Conditional Access Policy
  - **Block Device Code Flow**





Tools

- **TokenTacticsV2**
  - https://github.com/f-bader/TokenTacticsV2
- **AADInternals**
  - https://github.com/Gerenios/AADInternals
- **GraphRunner**
  - https://github.com/dafthack/GraphRunner
- **ROADTools**
  - https://github.com/dirkjanm/ROADtools

Resources

- **Storm-2372 conducts device code phishing campaign**
  - https://www.microsoft.com/en-us/security/blog/2025/02/13/storm-2372-conducts-device-code-phishing-campaign/
- **Multiple Russian Threat Actors Targeting Microsoft Device Code Authentication**
  - https://www.volexity.com/blog/2025/02/13/multiple-russian-threat-actors-targeting-microsoft-device-code-authentication/
- **Introducing a new phishing technique for compromising Office 365 accounts**
  - https://aadinternals.com/post/phishing/#new-phishing-technique-device-code-authentication
- **Microsoft identity platform and the OAuth 2.0 device authorization grant flow**
  - https://learn.microsoft.com/en-us/entra/identity-platform/v2-oauth2-device-code
- **New Microsoft-managed policies to raise your identity security posture**
  - https://techcommunity.microsoft.com/blog/microsoft-entra-blog/new-microsoft-managed-policies-to-raise-your-identity-security-posture/4286758

Resources

- **The Art of the Device Code Phish**
  - https://0xboku.com/2021/07/12/ArtOfDeviceCodePhish.html
- **How to Detect Malicious OAuth Device Code Phishing**
  - https://www.inversecos.com/2022/12/how-to-detect-malicious-oauth-device.html
- **Hacking Your Cloud: Tokens Edition 2.0**
  - https://www.trustedsec.com/blog/hacking-your-cloud-tokens-edition-2-0
- **How to protect against Device Code Flow abuse and block the authentication flow**
  - https://jeffreyappel.nl/how-to-protect-against-device-code-flow-abuse-storm-2372-attacks-and-block-the-authentication-flow/
- **Dynamic Device Code Phishing**
  - https://www.blackhillsinfosec.com/dynamic-device-code-phishing/
- **Detect Device Code Authentication Phishing**
  - https://www.linkedin.com/pulse/detect-device-code-authentication-phishing-kloudynet-i0rpc/