

# Authentication Proxy Attacks

---

DETECTION, RESPONSE  
AND HUNTING

---

# About Me



Chris Merkel

Senior Director, Cybersecurity Defense

Northwestern Mutual

[@chrismerkel@infosec.exchange](mailto:@chrismerkel@infosec.exchange)

[@chris\\_merkel@threads.net](https://www.threads.net/@chris_merkel)

Been doing security for a long time

Frequent BSidesLV attendee

Reverses malware for fun

Prefers nano over vim

Recent convert to pineapple on pizza

Got to meet John McAfee here a few months after he killed someone and fled Belize but before he became a crypto grifter (RIP).

---

# You did it!

- Multi-factor authentication enabled!
- Migrated away from weak SMS and Push/Approve methods.
- **Most attacks** your org faces daily have been mitigated.



# The bad news

**BLEEPINGCOMPUTER** 

[Home](#) > [News](#) > [Security](#) > Microsoft accounts targeted with new MFA-bypassing phishing kit



---

## Microsoft accounts targeted with new MFA-bypassing phishing kit

By [Bill Toulas](#)

 August 3, 2022  02:02 PM  0

---

  
Previous article  Next article 

## Large-Scale Phishing Campaign Bypasses MFA

 Author:  
Elizabeth Montalbano  
July 13, 2022 / 7:45 am

**ars TECHNICA**  [SUBSCRIBE](#)   [SIGN IN](#)

[GOT MFA?](#) —

## Ongoing phishing campaign can hack you even when you're protected with MFA

Campaign that steals email has targeted at least 10,000 organizations since September.

DAN GOODIN - 7/12/2022, 5:58 PM

---

# CISA HAS ENTERED THE CHAT



CISA embraces the designation:  
*Phishing-Resistant MFA*

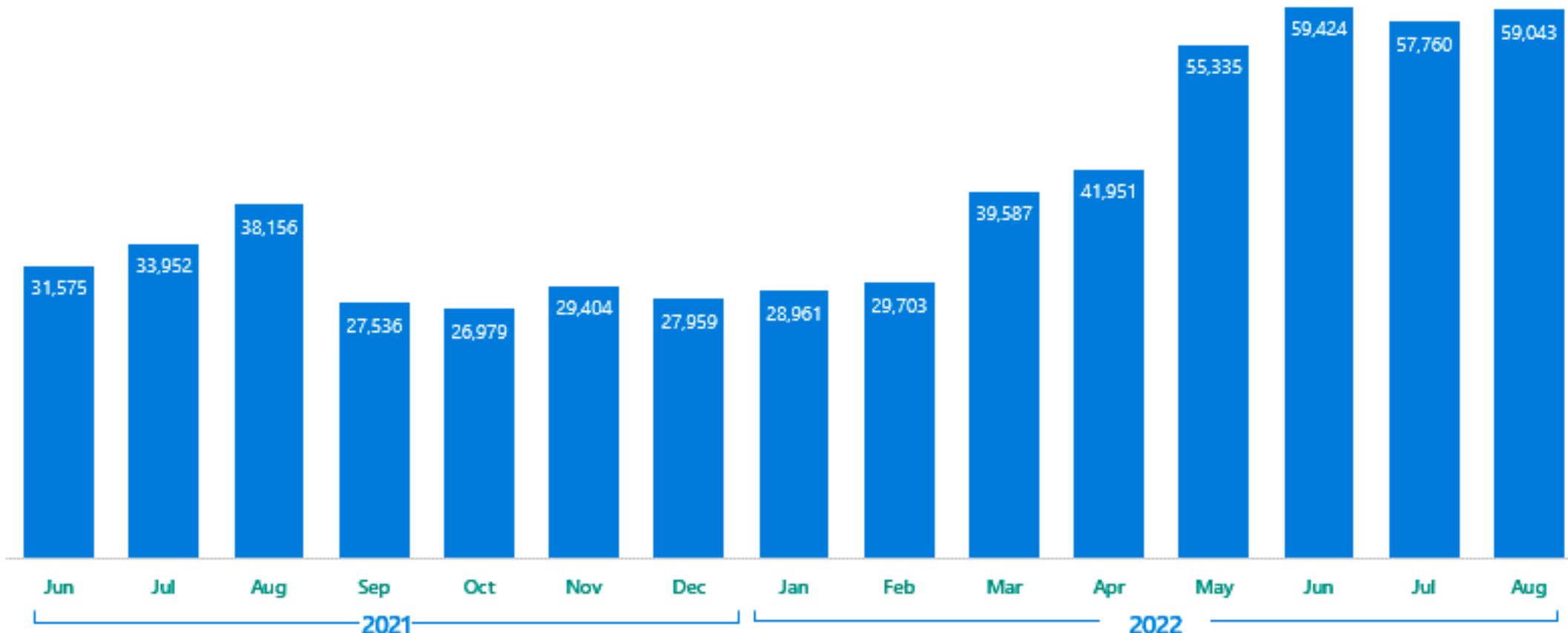
Guidance TL;DR:

Auth Type	Phishing Resistant?
FIDO2/WebAuthN	YES
OTP, Number Match	NOPE
Mobile App Push	LOL
SMS / Voice	LMAO

*Security questions aren't on the list because they're not secondary factors to password knowledge.*

# Token Replay

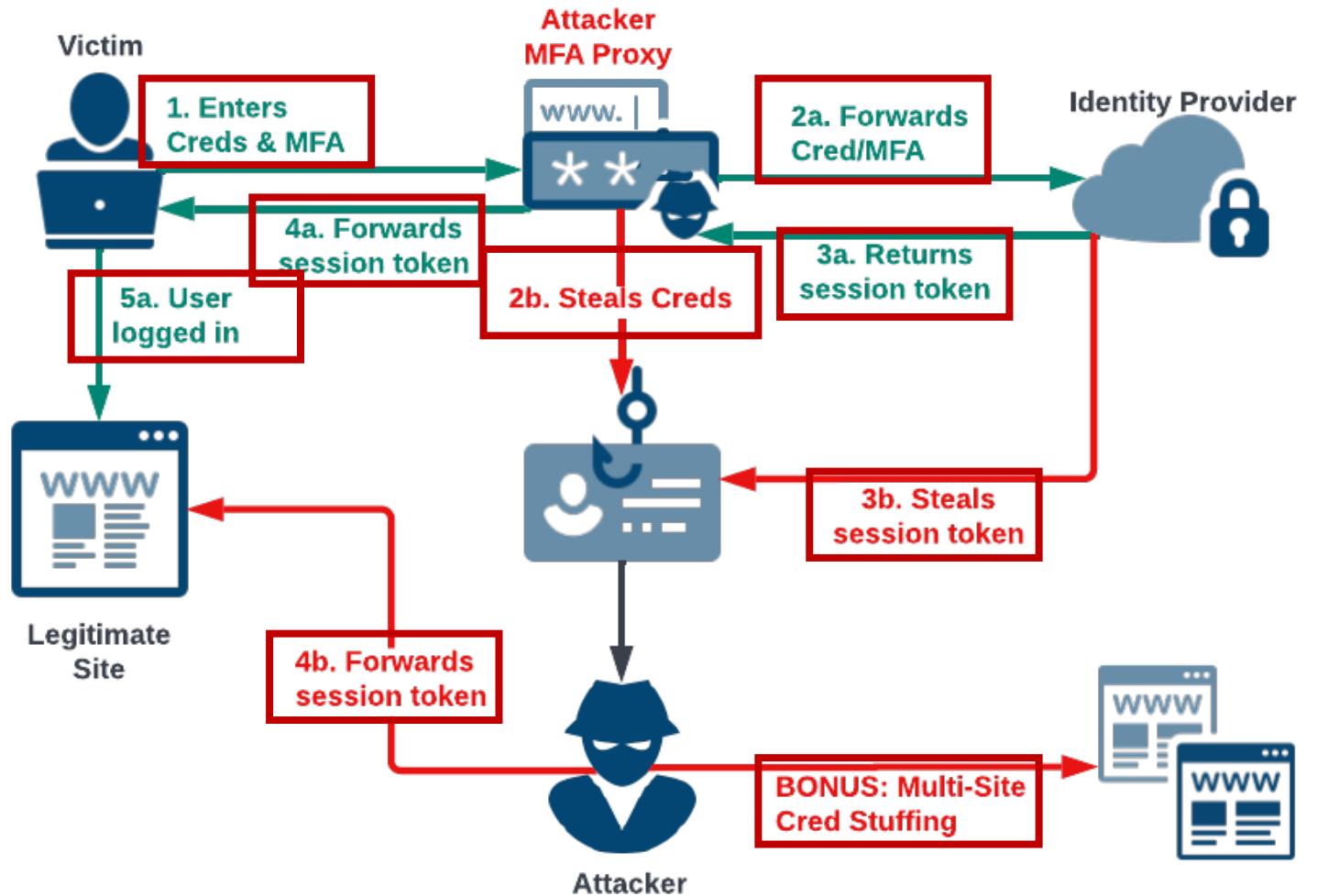
Detected token replay attacks per month



Source: Azure AD Identity Protection Anomalous Token detection

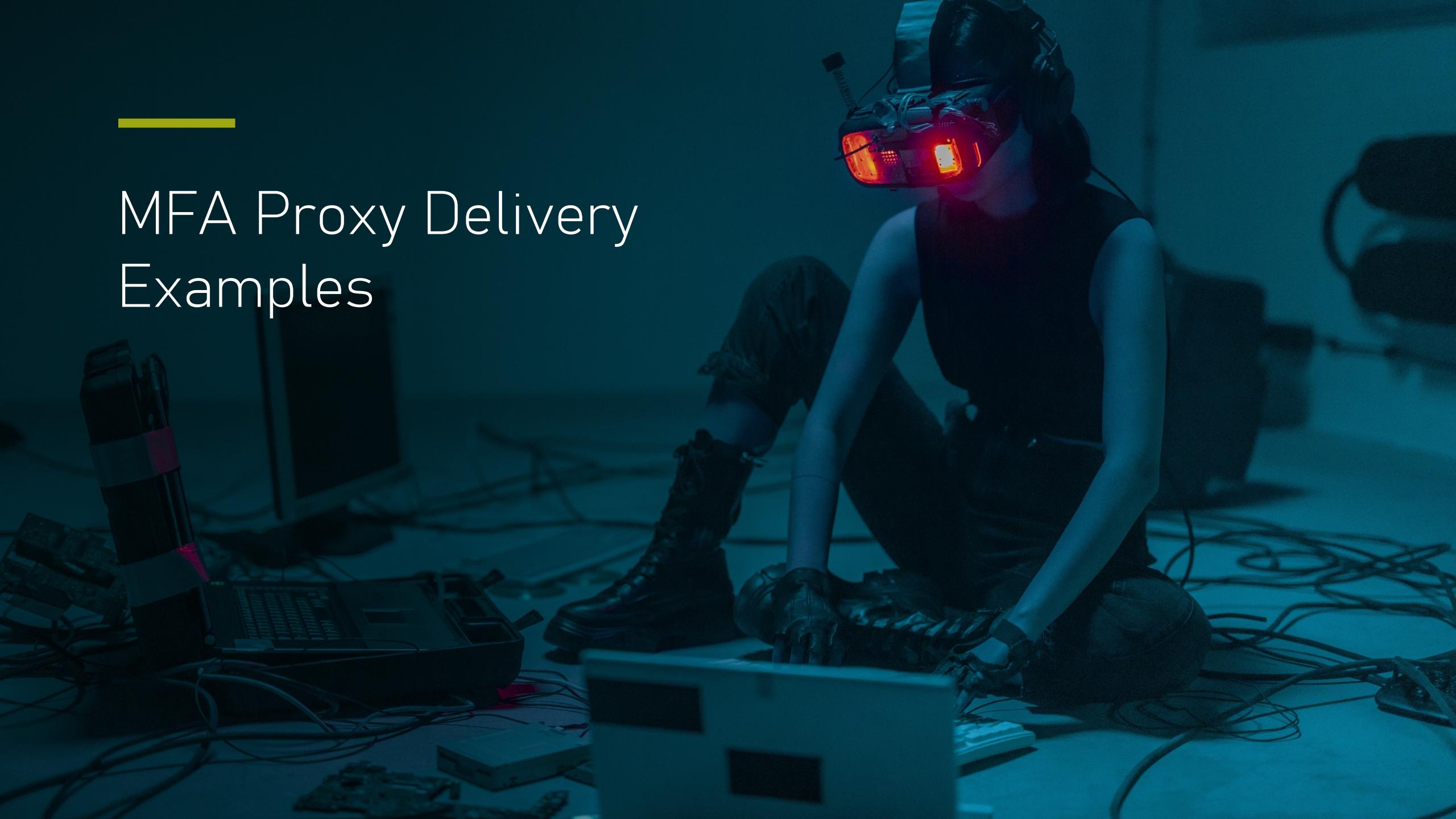
# Background

- Nov 2018 – Evilginx Released
- Easier than SIM Swapping
- Easier than push-griefing
- No effects on victim.



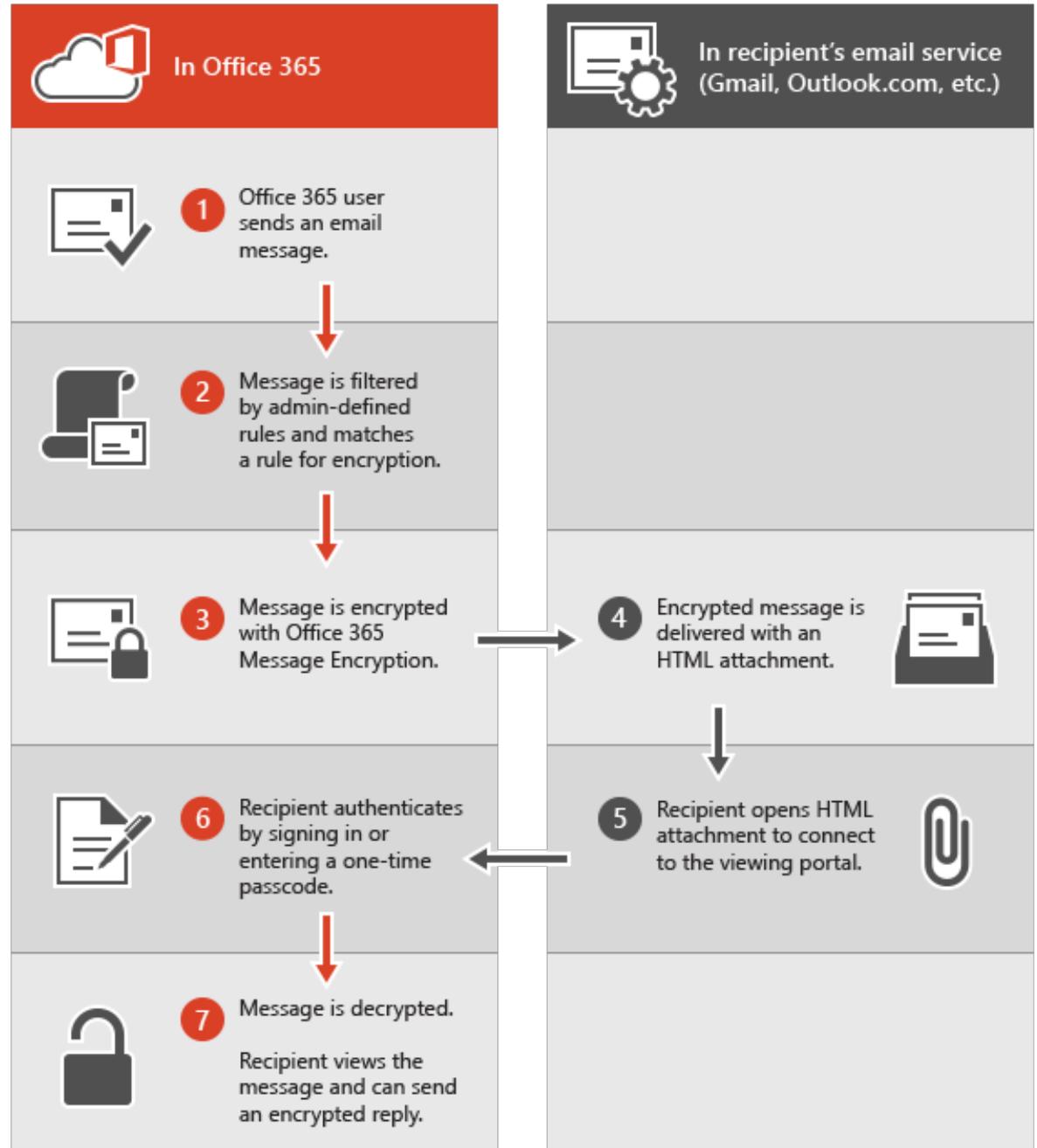
---

# MFA Proxy Delivery Examples

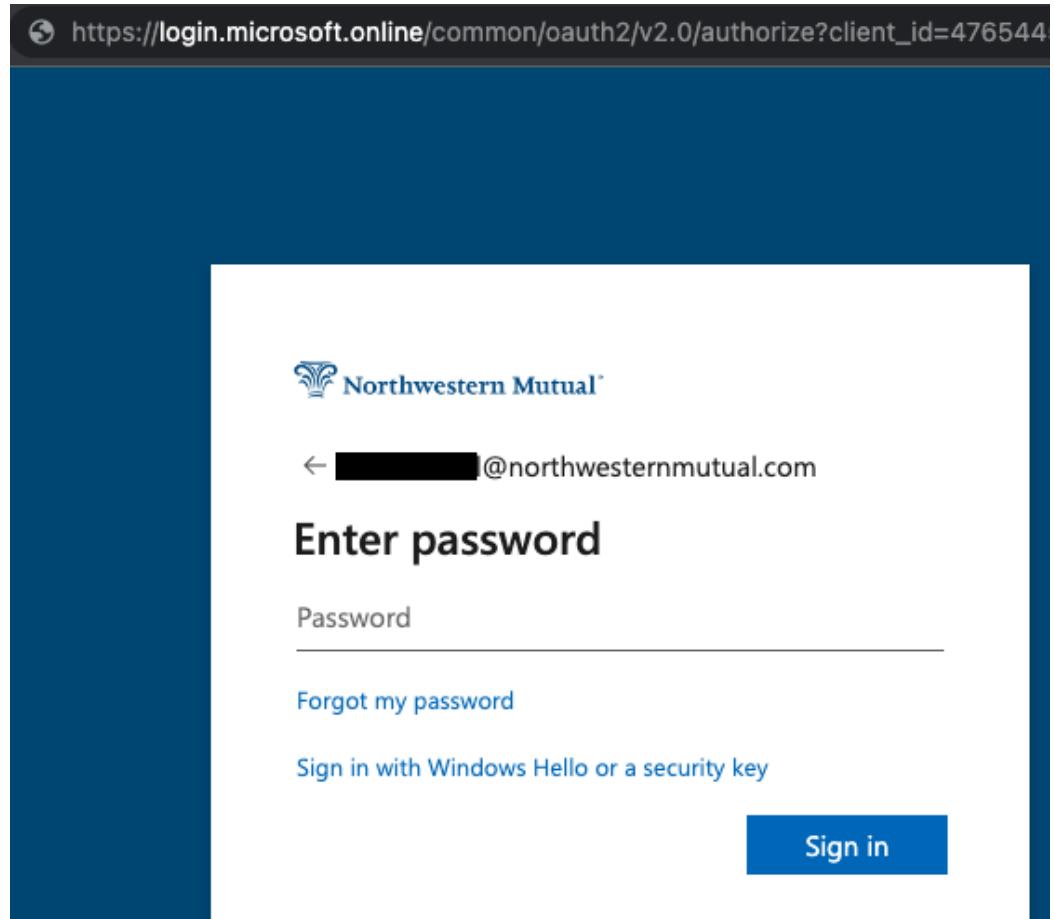
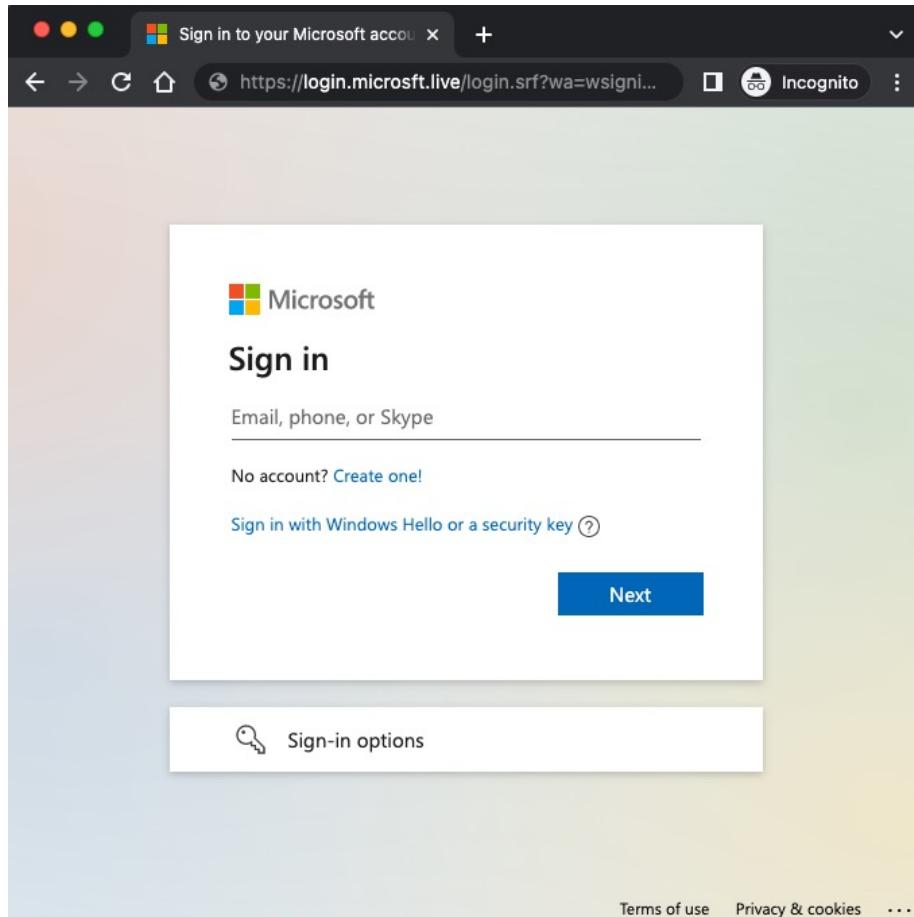


# Delivery Methods

- Traditional Phishing Messages
- Encrypted Message Hopping
- ATO + Microsoft Purview



# Victim experience



Generic and custom branding remains intact. The only tell is in the browser bar.  
What's your org's click % rate on fake logon pages?

---

# Tradecraft Evolution



- Some adversaries are getting better about OSINT, less infrastructure re-use.
- Increased use of anti-inspection techniques
  - Referrer checking
  - Sandbox detection
  - Encrypted mail
- Increased use of SMS based phishing to bypass inspection

# Detecting Attacks

---



# Detecting Attacks

## Impossible Travel

- Reasonably Accurate
- Use of consumer VPNs create false positives.
- Geo-local proxy access frequently sold on dark web markets.

Indicator: Impossible Travel Activity

Unauthorized Access Attempt

Suspect Priority 1

DATE CREATED Nov 30, 2021 8:31 AM EST

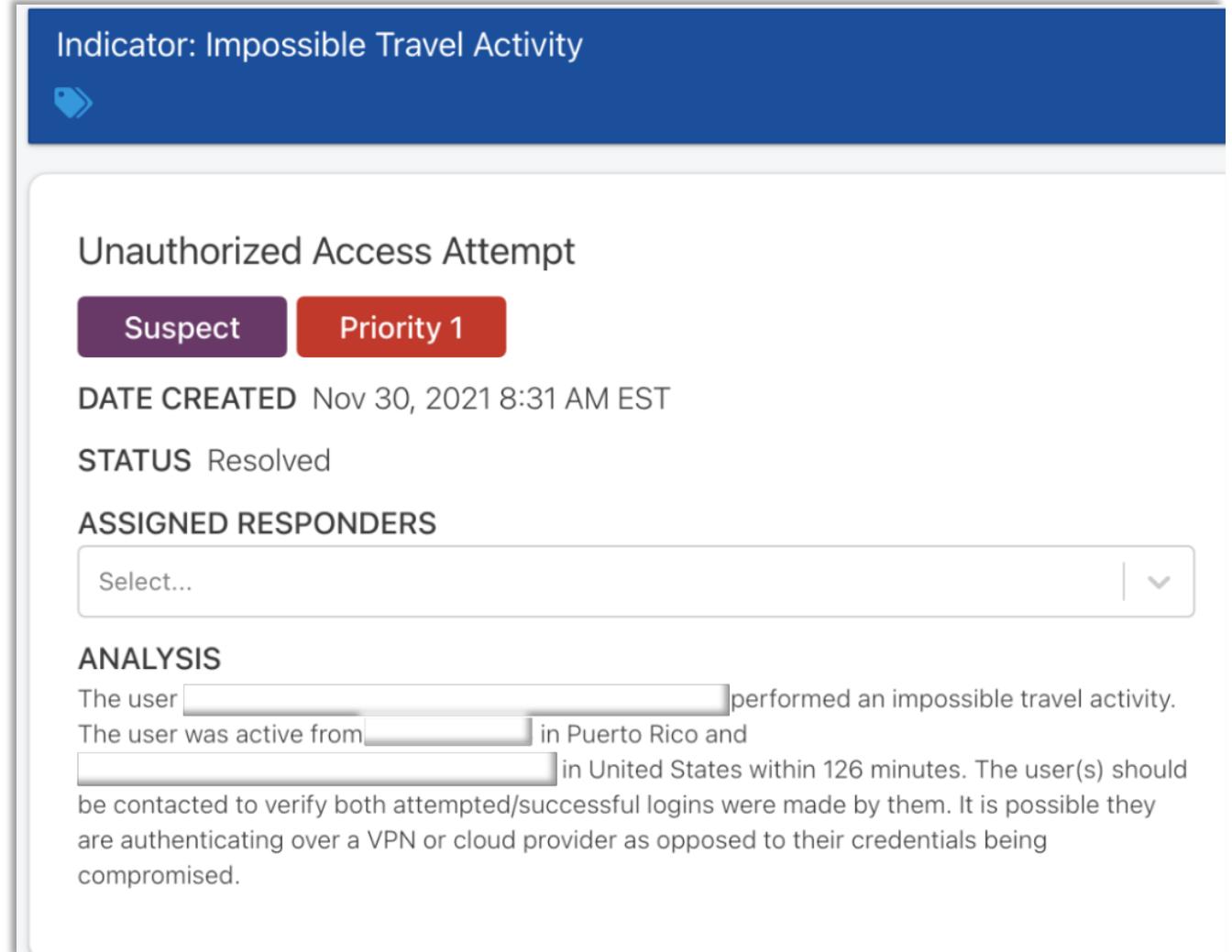
STATUS Resolved

ASSIGNED RESPONDERS

Select... ▾

ANALYSIS

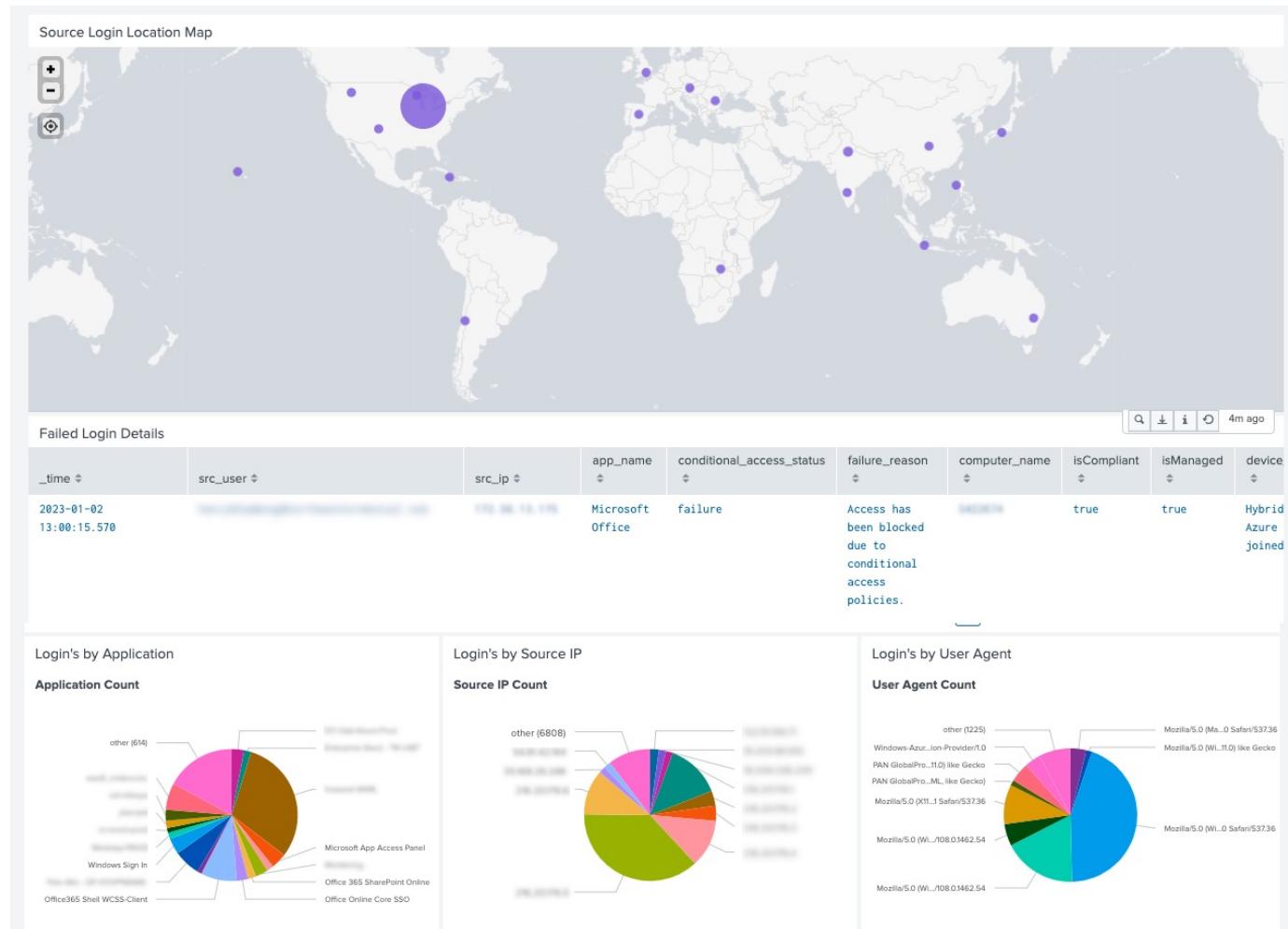
The user [REDACTED] performed an impossible travel activity. The user was active from [REDACTED] in Puerto Rico and [REDACTED] in United States within 126 minutes. The user(s) should be contacted to verify both attempted/successful logins were made by them. It is possible they are authenticating over a VPN or cloud provider as opposed to their credentials being compromised.



# Detecting Attacks

Changes to users and devices:

- Logon from previously unseen IP + authenticator change
- New device registration attempts: Azure AD join / inTune enrollment



A dramatic photograph of two firefighters in full protective gear, including silver reflective suits and helmets, battling a large fire. They are spraying a powerful stream of water from a hose onto a massive wall of orange and red flames. Thick white smoke billows from the fire, partially obscuring the firefighters. The scene is set against a dark background.

Investigation, Hunting and Response

---

# Investigating and Responding to Attacks

- Has successful MFA occurred? Identity providers have confusing log messages around MFA.
- Do you know how to invalidate session tokens?
- Hard password resets, triggering a session invalidation

```
  "AzureAd": {  
    "Instance": "https://login.microsoftonline.com/",  
    "Domain": "microsoft.onmicrosoft.com",  
    "TenantId": "72f988bf-86f1-41af-91ab-2d7cd011db47",  
    "ClientId": "93c23ef3-8851-4889-8dc3-9847b2d0d844",  
    "CallbackPath": "/signin-oidc"  
  },  
  "Logging": {  
    "LogLevel": {  
      "Default": "Information",  
      "Microsoft": "Warning",  
      "Microsoft.Hosting.Lifetime": "Information"  
    }  
  },  
  "AllowedHosts": "*"
```

Password-based browser session	Password based token	Non-password-based browser session	Non-password-based browser token	Enterprise application token
Password changed/reset or admin center sign-out	Revoked	Revoked	Not revoked	Not revoked
Revoked via AAD portal, PowerShell, Graph	Revoked	Revoked	Revoked	Revoked



Terminating **all** access to resources, especially in response to a compromised account, requires revoking refresh tokens, not just refreshing the password.

# Investigating and Responding to Attacks

- Reviewing M365 logs for evidence of access:
  - OneDrive logs
  - Mail forwarding rules
  - Authenticator changes
  - User creation
  - Exchange mail transport rules





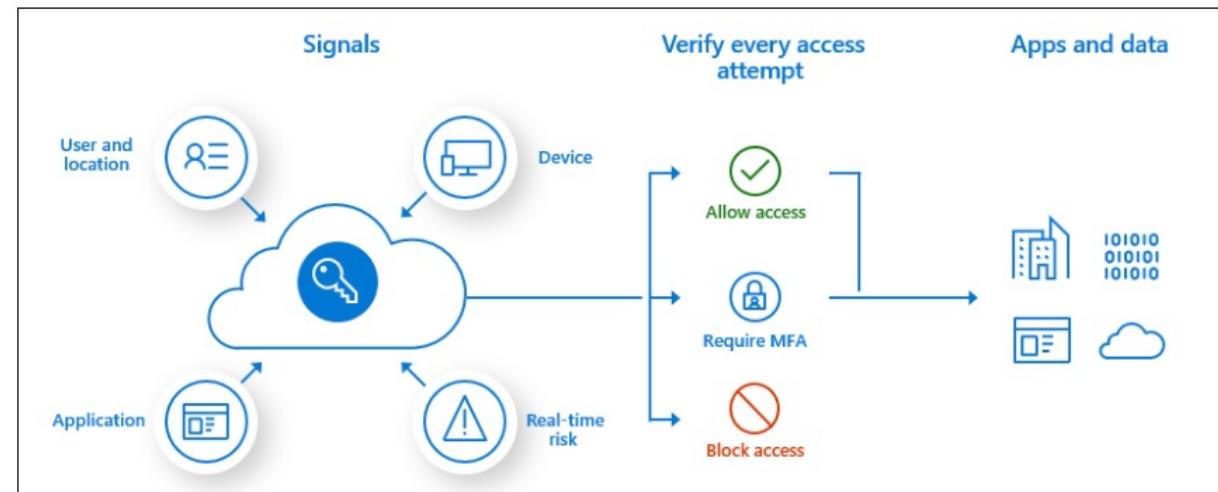
---

## Threat Hunting

- Attack surface monitoring – know all your known good authentication endpoints.
- Shodan hunts for Evilngnix and EvilProxy TTPs.
- Search firewall logs for typosquats, page titles, URI paths related to authentication
- Identify threat actors most likely to use MFA proxy, monitor their associated IOCs

# Know your attack surface

- Do you know where your authentication endpoints are?
- Look inside your Microsoft Conditional Access Policies (CAP)
- Understand when CAP failures are areas of opportunity for threat actors
  - Often many orgs have an array of CAP policies across different applications and configurations
  - Use tools like caOptics to find gaps in your CAP policies. <https://github.com/jsa2/caOptics>



*Conditional Access Policies*

# Hunt for Attempts to Target your Org

- Have alerts setup for typosquat registration related to SSO
  - sso-yourorg.com
  - yourorg-sso.com
- Hunt inside your firewall logs for page titles, URI paths related to authentication  
These are hidden behind referrers but will show up in firewall
- Passive DNS is your friend

URLS - 20 / 176		Pro +143 results
Detections		
<input type="checkbox"/>	<a href="https://lmo.danpearlman.click/common/oauth2/v2.0/authorize?client_id=4765445b-32c6-49b0-83e6-1d93765276ca...">https://lmo.danpearlman.click/common/oauth2/v2.0/authorize?client_id=4765445b-32c6-49b0-83e6-1d93765276ca...</a>	8 / 89
<input type="checkbox"/>	lmo.danpearlman.click 45.11.183.76	
<input type="checkbox"/>	<a href="https://lmo.stmties.com/common/oauth2/v2.0/authorize?client_id=4765445b-32c6-49b0-83e6-1d93765276ca&amp;redi...">https://lmo.stmties.com/common/oauth2/v2.0/authorize?client_id=4765445b-32c6-49b0-83e6-1d93765276ca&amp;redi...</a>	11 / 89
<input type="checkbox"/>	lmo.stmties.com 168.119.109.0	
<input type="checkbox"/>	<a href="https://lmo.acquirarealty.net/common/oauth2/v2.0/authorize?client_id=4765445b-32c6-49b0-83e6-1d93765276ca...">https://lmo.acquirarealty.net/common/oauth2/v2.0/authorize?client_id=4765445b-32c6-49b0-83e6-1d93765276ca...</a>	10 / 89
<input type="checkbox"/>	lmo.acquirarealty.net 143.198.24.108	
<input type="checkbox"/>	<a href="https://lmo.acquirarealty.net/common/oauth2/v2.0/authorize?client_id=4765445b-32c6-49b0-83e6-1d93765276ca...">https://lmo.acquirarealty.net/common/oauth2/v2.0/authorize?client_id=4765445b-32c6-49b0-83e6-1d93765276ca...</a>	9 / 89
<input type="checkbox"/>	lmo.acquirarealty.net 143.198.24.108	
<input type="checkbox"/>	<a href="http://lmo.acquirarealty.net/common/oauth2/v2.0/authorize?client_id=4765445b-32c6-49b0-83e6-1d93765276ca...">http://lmo.acquirarealty.net/common/oauth2/v2.0/authorize?client_id=4765445b-32c6-49b0-83e6-1d93765276ca...</a>	8 / 89
<input type="checkbox"/>	lmo.acquirarealty.net 143.198.24.108	
<input type="checkbox"/>	<a href="http://lmo.acquirarealty.net/common/oauth2/v2.0/authorize?client_id=4765445b-32c6-49b0-83e6-1d93765276ca...">http://lmo.acquirarealty.net/common/oauth2/v2.0/authorize?client_id=4765445b-32c6-49b0-83e6-1d93765276ca...</a>	11 / 89
<input type="checkbox"/>	lmo.acquirarealty.net 143.198.24.108	

# Hunt Externally

Your logon page has elements unique to you or your identity provider.

- Identify unique strings in logon page DOM.
- Alert with string is in HTTP stream but not in a list of known good domains.
- If you use custom branding, identify CSS elements specific only to your logon page to alert whenever it's seen on a non-corp domain.
- Your identity provider has specific metadata in their TLS certificate that can't be easily faked.

SHODAN | Explore | Downloads | Pricing ↗ | http.html:"msauth"

TOTAL RESULTS: 17

TOP COUNTRIES:

Country	Count
United States	9
Ireland	4
Switzerland	2
Estonia	1
Singapore	1

TOP PORTS:

Port	Count
443	15
80	2

TOP ORGANIZATIONS:

Organization	Count
Amazon Technologies Inc.	5
Amazon Data Services Ireland Li...	2
Amazon Data Services NoVa	2
Amazon.com, Inc.	2

**52.71.88.174**

ec2-52-71-88-174.compute-1.amazonaws.com

Amazon Technologies Inc.

United States, Ashburn

cloud

**SSL Certificate**

Issued By: Amazon

J- Common Name: \*.booklick.net

Connection: keep-alive

Server: nginx/1.16.1

X-Powered-By: Express

ETag: W/"1c79-Erx6M2fCdijWWFBSh69Zy5kcY+0"

Vary: Accept-Encoding

Supported SSL Versions: TLSv1, TLSv1.1, TLSv1.2

**31.10.252.13**

sage3v12.uhlmann.ch

31-10-252-13.static.upc.ch

sage3v12test.uhlmann.ch

www.sage3v12.uhlmann.ch

Sunrise GmbH

Switzerland, Zug

**SSL Certificate**

Issued By: Go Daddy Secure Certificate Authority - G2

J- Common Name: sage3v12.uhlmann.ch

x-frame-options: SAMEORIGIN

content-type: text/html

set-cookie: syracuse.sid.443=946ec89a-e3e1-4e

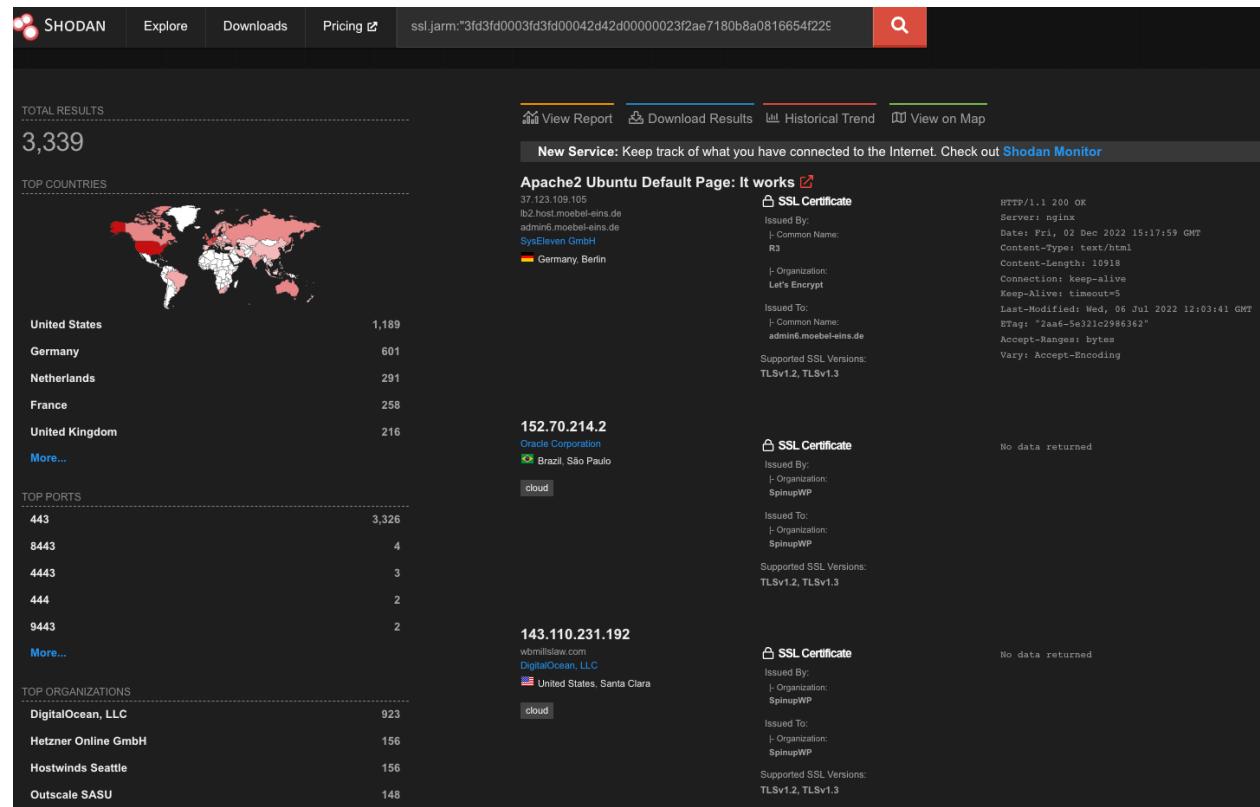
set-cookie: client.id=9ec7600b-cf53-4206-97a4

content-language: en-US

Supported SSL Versions: TLSv1.2

# EvilProxy profiling

- Target the tool – Adversaries are lazy and make mistakes
  - Popular toolkits to generate AiTM attacks are
    - EvilProxy
    - Evilnginx
  - Use the jarm hash, oftentimes the attackers forget to change the settings in Evilproxy and generate similar site configurations



This JARM was in use for ~4 months



- Start looking for bad while you formulate your MFA game plan.
- Move to phishing-resistant MFA.
- Monitor for your unique authentication signature in unexpected places.
- Look for unexpected account management events.
- Simulate an attack and identify indicators of activity relevant to your org.

---

# Wrap-Up

- Questions
- Will Post Slides on:

Masto: @chrismerkel@infosec.exchange

Zucko: @chris\_\_merkel@threads.net



---

THINGS WE HAD TO CUT FOR  
TIME BUT THOUGHT WERE  
PRETTY COOL

Bonus slides



# Detecting Attacks – Advanced Methods

- Microsoft app token swaps
- Purple team testing:
  - Various methods of MFA proxy
  - Alert thresholds for MFA failures
  - Non-typical auth endpoints



no nginx - pure evil  
by Kuba Gretzky (@mrgretzky) version 2.3.3

```
[22:13:45] [inf] loading phishlets from: /usr/share/evilginx/phishlets/
[22:13:45] [inf] loading configuration from: /root/.evilginx
[22:13:46] [err] failed to load phishlet 'razer.yaml': force_post: unknown type - only 'post' is
[22:13:47] [war] server domain not set! type: config domain <domain>
[22:13:47] [war] server ip not set! type: config ip <ip_address>
```

phishlet	author	active	status	hostname
amazon	@customsync	disabled	available	
cloudflare	@hash3liZer	disabled	available	
stackoverflow	@hash3liZer	disabled	available	
yahoo	@hash3liZer	disabled	available	
citrix	@424f424f	disabled	available	
freelancer	@hash3liZer	disabled	available	
github	@audibleblink	disabled	available	
linkedin	@mrgretzky	disabled	available	
reddit	@customsync	disabled	available	
twitter-mobile	@white_fi	disabled	available	
twitter	@white_fi	disabled	available	
facebook	@mrgretzky	disabled	available	
google	@hash3liZer	disabled	available	
instagram	@prrrinncee	disabled	available	
outlook	@mrgretzky	disabled	available	
upwork	@hash3liZer	disabled	available	
o365	@jamescullum	disabled	available	
okta	@mikesiegel	disabled	available	
protonmail	@jamescullum	disabled	available	

---

# Detecting Attacks

## Token to User Agent Ratio

- Session tokens are stored in a single browser instance. The user agent should not change.

## Bad User Agents

- Look for signs of automation:  
**Go-http-client/\***  
**python-requests/\***  
**Java/\***  
**Boto3/\***  
**curl/\***