

The background of the slide is a photograph of a brick wall covered in graffiti. A large, stylized eye is painted in bright green and black, looking directly at the viewer. A hand holding a spray paint can is visible, as if it just finished painting the eye. The wall is made of dark brown and grey bricks.

# Authentication Proxy Attacks

---

DETECTION, RESPONSE  
AND HUNTING

---

# Introduction



Chris Merkel

Senior Director, Cybersecurity Defense

Northwestern Mutual

Link to slides will be posted:

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



# Anyone Can Cook!

*First, the bad news sandwich:*

**Good news:** Everyone has enabled MFA!

**Bad news:** This isn't enough anymore.

**Good news:** we're at Cyphercon, where you're going to learn how to cook up a defense against this attack!

---

# Mission Accomplished!

- 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 has made a new designation:  
*Phishing-Resistant MFA*

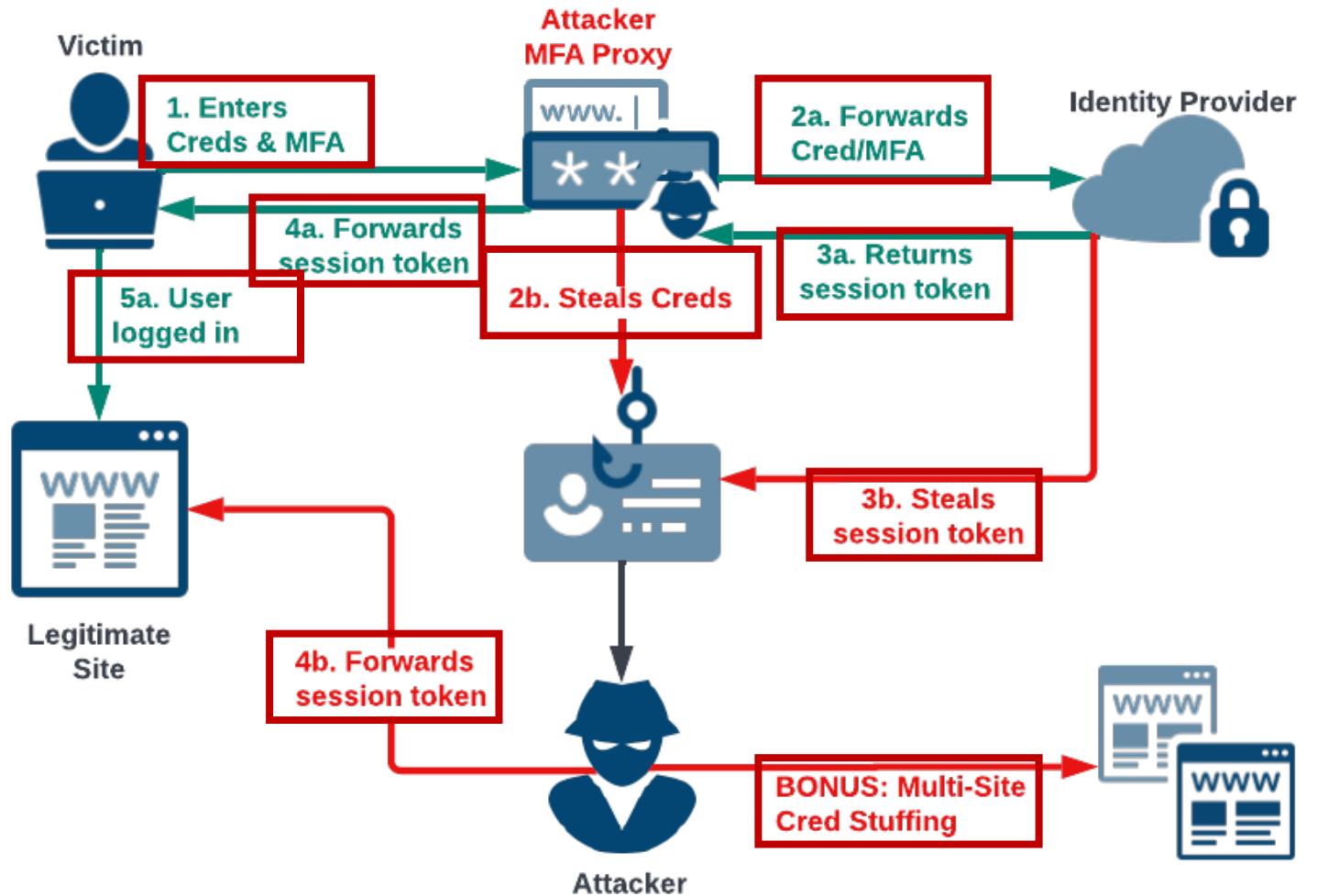
Guidance TL;DR:

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.*

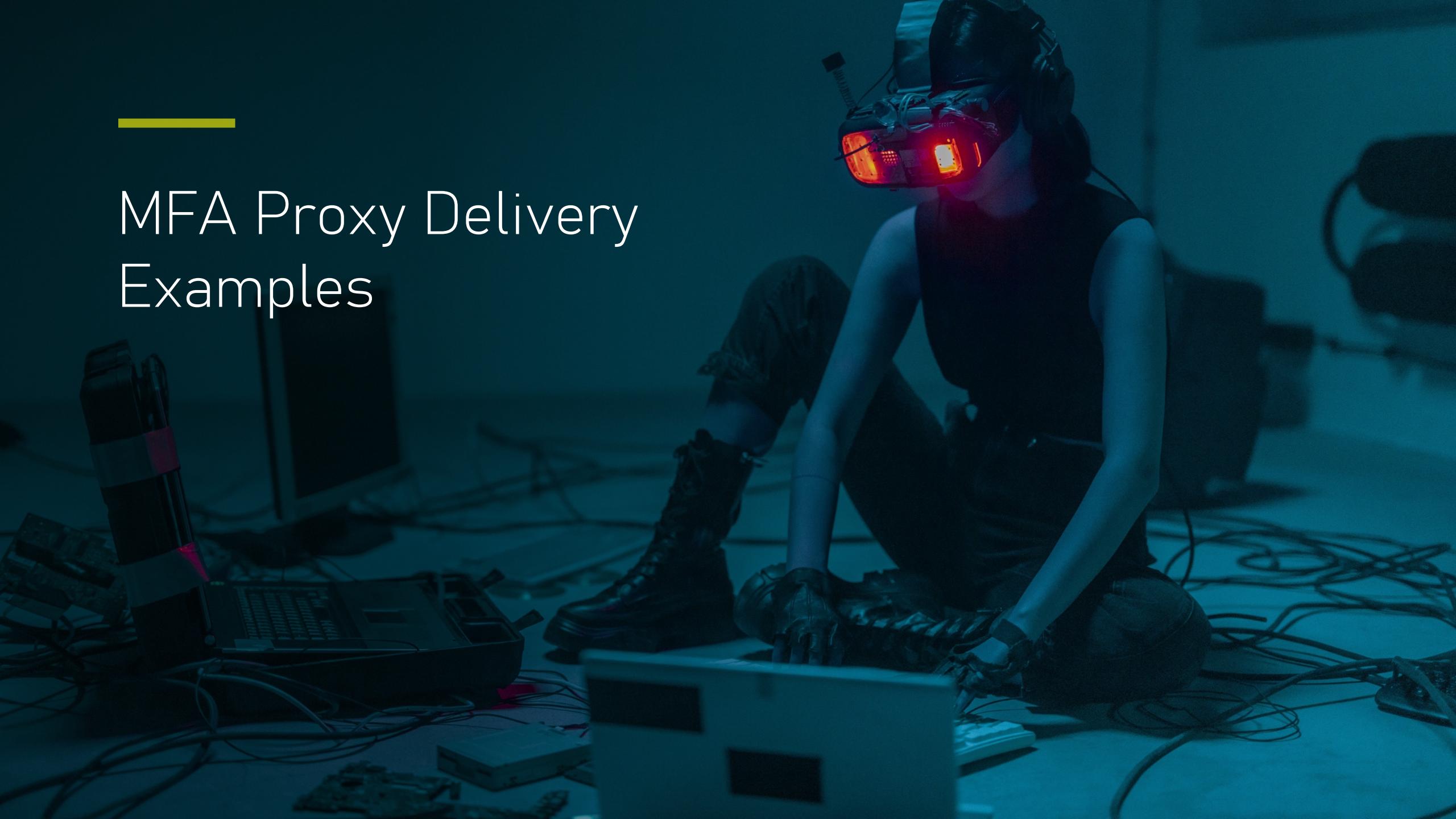
# Background

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



---

# MFA Proxy Delivery Examples



# Initial Access - Lookalike Domains

---

In this scenario, the threat actor compromises a trusted domain(BEC) and *simulates* their encryption product

- User receives email, typically from a trusted partner and simulates encryption product used by sender.
- These “copycat” domains typically are setup shortly prior to phishing campaigns to avoid detection or malicious URL categorization.

**From:** Joe Smith <jsmith@**anylawfirm.com**>  
**Sent:** Thursday, October 13, 2022 7:59:39 PM  
**Subject:** [EXTERNAL] 110572 Any Law HFT-UTA Review

**Any Law Firm, P.A. Encryption**

This is an encrypted message from Any Law Firm, P.A.

We have recently upgraded our secure message system. You are required to log in the first time you access it.

[Click here](#) to log into the Any Law's secure server and reply to this email.

 <https://lmo.anylawfirm.org/>

The encrypted message expires in 30 days.

# Message Encryption

---

- With access to a compromised tenant, the threat actor takes advantage of native message encryption.
- The message isn't inspected, by Microsoft or other 3<sup>rd</sup> party mail gateways.
- Message body is opened in a browser to Microsoft, evading your ingress firewall.

## Example Email Received Using Protected Message

**From:** Donna [REDACTED]@es.com>  
**Sent:** Thursday, January 12, 2023 7:46:50 PM  
**To:** Donna [REDACTED]@es.com>  
**Subject:** Incoming Document Received from <Sending Domain>

Donna [REDACTED]@es.com) has sent you a protected message.

[Read the message](#) →

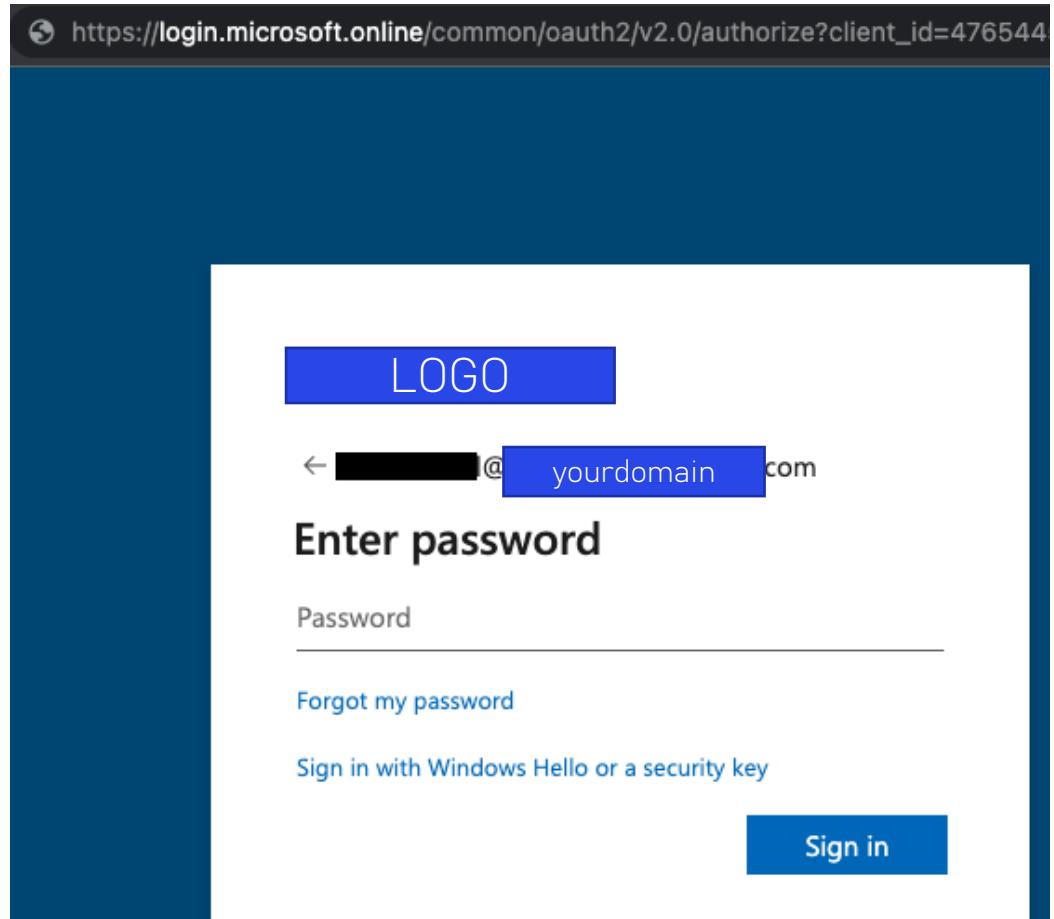
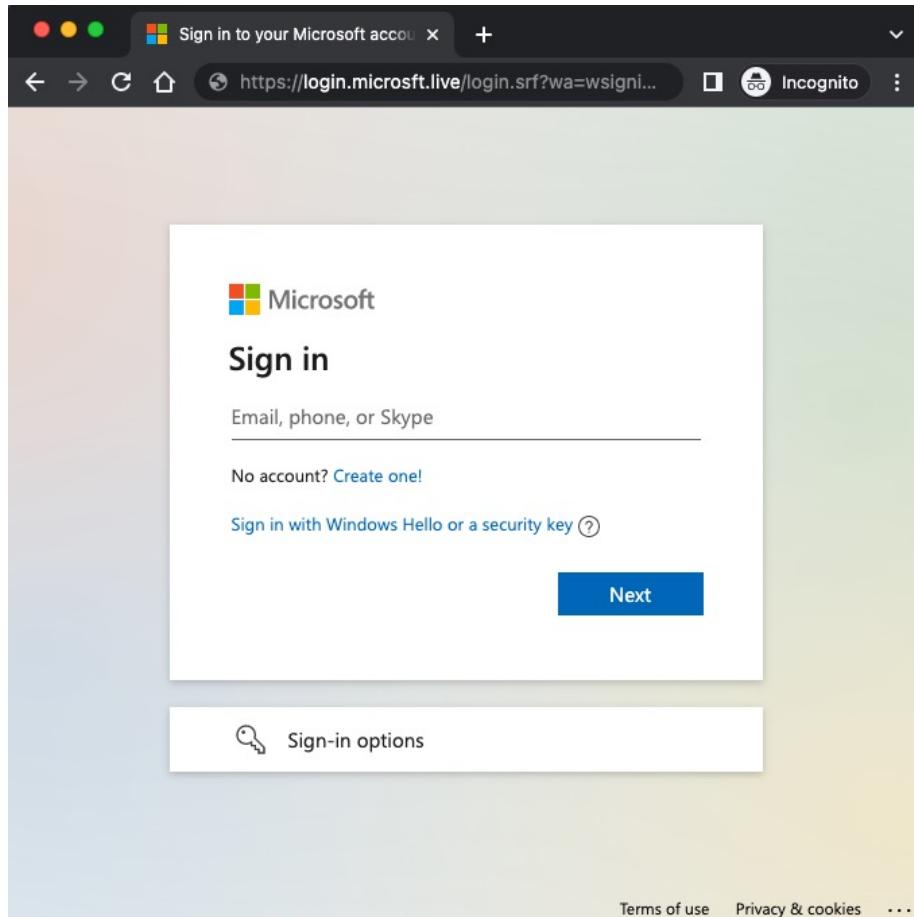
<https://outlook.office365.com/owa/?viewmodel=readmessageitem&internetmessageid=<REDACTED>namprd14.prod.outlook.com>  
Click or tap to follow link.

[Learn about messages protected by Microsoft Purview Message Encryption.](#)

[Privacy Statement](#)

[Learn More](#) on email encryption.  
Microsoft Corporation, One Microsoft Way, Redmond, WA 98052

# 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?

# 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

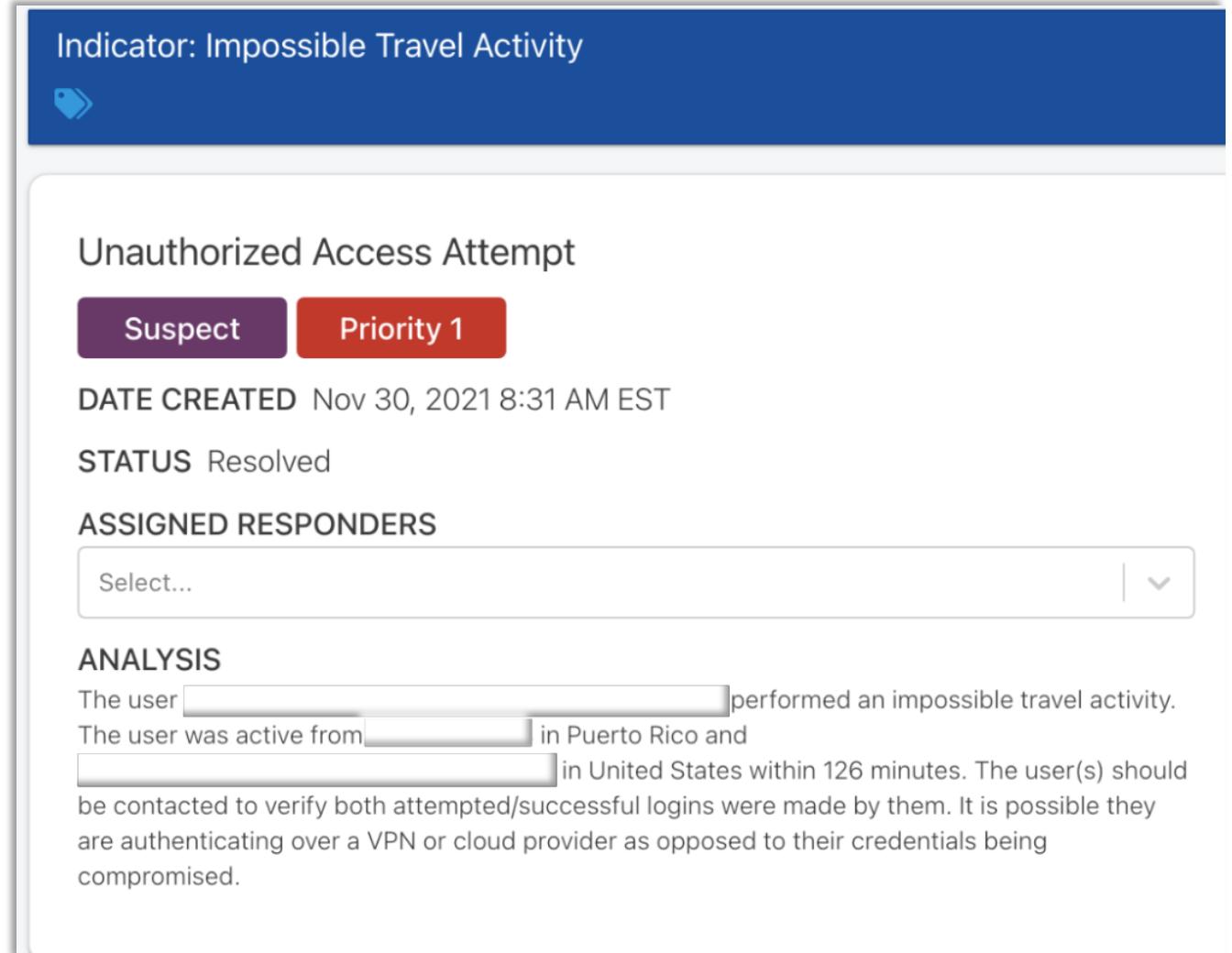
STATUS Resolved

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

## Reputation-based

- Some identity providers can warn / block network ranges or ASNs.
- Use threat feeds to identify “bad neighborhoods” and feed via API.
- Use SOAR to send end-user notifications on risky sign-ins.

The screenshot shows the Okta Security interface with the left sidebar expanded to show various security modules: Dashboard, Directory, Customizations, Applications, Security (selected), General, HealthInsight, Authenticators, Authentication Policies, Global Session Policy, Profile Enrollment, Identity Providers, Delegated Authentication, Networks (selected), Behavior Detection, Device Integrations, Administrators, and API. The main content area is titled "Networks" and displays a table of network zones. The table has columns for Name, Zone Type, Details, and IP Type. It lists several entries:

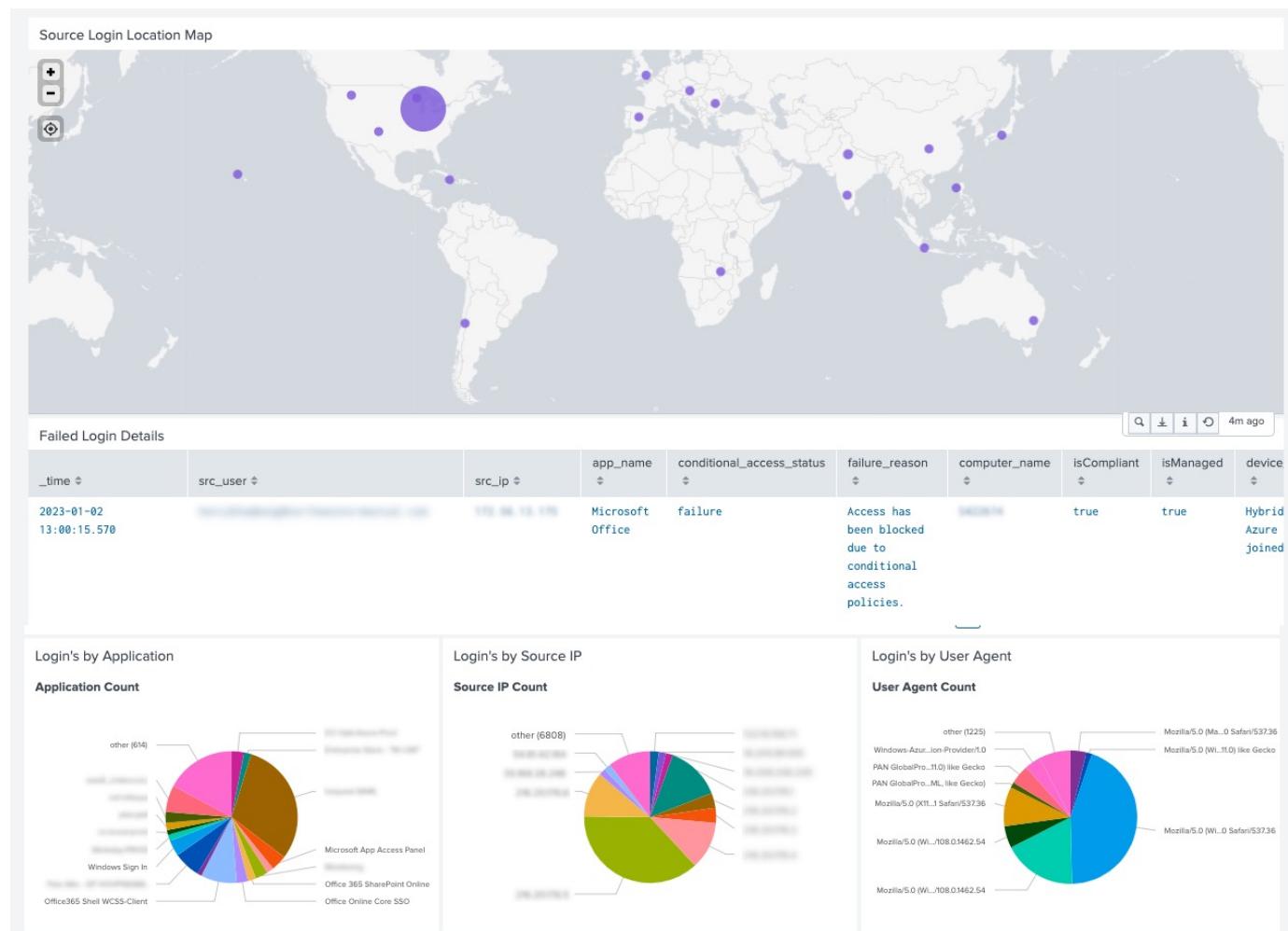
Name	Zone Type	Details	IP Type
Allowlist for trusted countries	Dynamic	Locations: Australia, Belgium, Canada, Czech Republic	Any
Block TOR	Dynamic Block list	IP Type: Tor anonymizer proxy	
Blocked countries	Dynamic	Locations: Belarus	Any
BlockedIpZone	IP Block list		
Internal network	IP	Gateway IPs: [redacted]	
LegacyIpZone	IP		

At the bottom of the page, there are links for "© 2022 Okta, Inc.", "Privacy", "Version 2022.03.0 E", "OPT Preview Cell (US)", "Status site", and "Do".

# Detecting Attacks

Changes to users and devices:

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



# Detecting Attacks

**The fatal flaw:** 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.

TOTAL RESULTS  
17

TOP COUNTRIES

COUNTRY	RESULTS
United States	9
Ireland	4
Switzerland	2
Estonia	1
Singapore	1
<a href="#">More...</a>	

TOP PORTS

PORT	RESULTS
443	15
80	2

TOP ORGANIZATIONS

ORGANIZATION	RESULTS
Amazon Technologies Inc.	5
Amazon Data Services Ireland Li...	2
Amazon Data Services NoVa	2
Amazon.com, Inc.	2

**52.71.88.174**

SSL Certificate

Issued By:  
- Common Name: Amazon Technologies Inc.  
- Organization: Amazon

Issued To:  
- Common Name: \*.booklick.net

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

HTTP/1.1 200 OK  
Date: Fri, 30 Dec 2022 22:19:09 GMT  
Content-Type: text/html; charset=utf-8  
Content-Length: 7289  
Connection: keep-alive  
Server: nginx/1.16.1  
X-Powered-By: Express  
ETag: W/"1c79-Erx6M2fCdiJWWFBSh69Zy5kcY+0"  
Vary: Accept-Encoding

**31.10.252.13**

SSL Certificate

Issued By:  
- Common Name: Go Daddy Secure Certificate Authority - G2

Issued To:  
- Common Name: sagex3v12.uhlmann.ch

Supported SSL Versions:  
TLSv1.2

HTTP/1.1 200 OK  
content-type: text/html  
set-cookie: syracuse.sid.443=946ec89a-e3e1-4e  
set-cookie: client.id=9ec7600b-cf53-4206-97a4  
content-language: en-US  
x-frame-opti...

---

# 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/\***

# 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

## Script Canaries

- If your logon page allows enough customization, implant content that should only be called from a specific domain.

The screenshot shows the Canary Tokens website interface. At the top right are links for "Documentation" and "What is this and why should I care?". Below that is a dropdown menu set to "Cloned website". Underneath are four input fields containing "http://your.webhook.broker", "Cloned website token for mycorp.com", and "auth.myidp.com". At the bottom is a large green button labeled "Create my Canarytoken".

CANARY TOKENS

What is this and why should I care?

Documentation

Cloned website

http://your.webhook.broker

Cloned website token for mycorp.com

auth.myidp.com

Create my Canarytoken

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, emphasizing the intensity of the fire.

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	Not revoked
Revoked via AAD portal, PowerShell, Graph	Revoked	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



- 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.

---

That's it!



---

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

Bonus slides





## Preventing Attacks – Advanced

- Browser plugins to identify use of corp credentials on non-corp IDPs.
- Threat hunt-to-block pipelining.
- Most of the methods here are accessible for organizations with a SIEM, firewall and authentication service logs.
- Test -> Telemetry -> Alert cycles are critical.
- You don't need to be a "red teamer" to conduct telemetry-generating attacks.
- Monitoring all conditional access policy changes and new app registration policies.
- Using device registration and other "proof of ownership" traits to risk-score authentication