# 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

# 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!

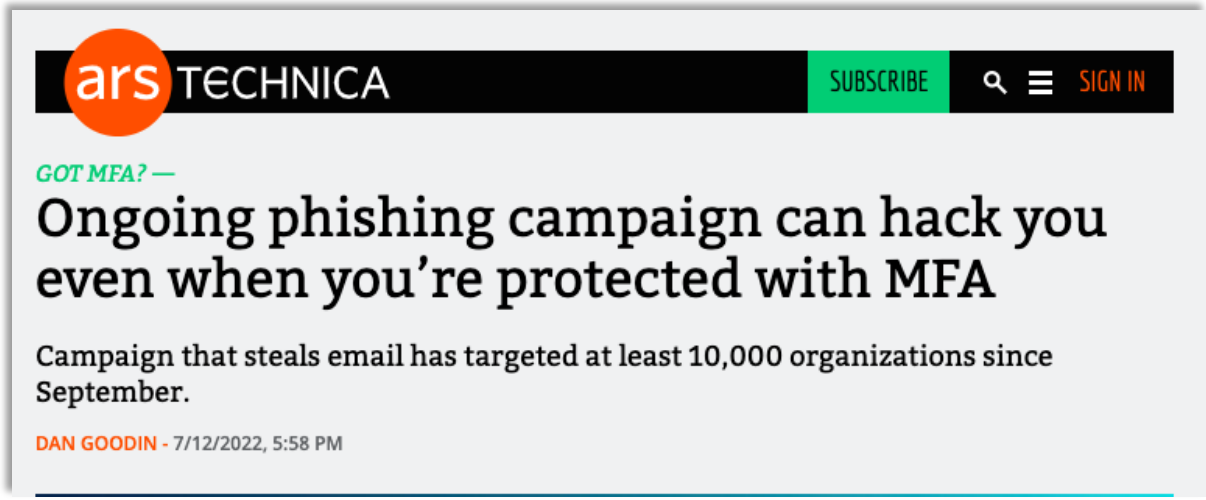
# Mission Accomplished!

- 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


threatpost
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*

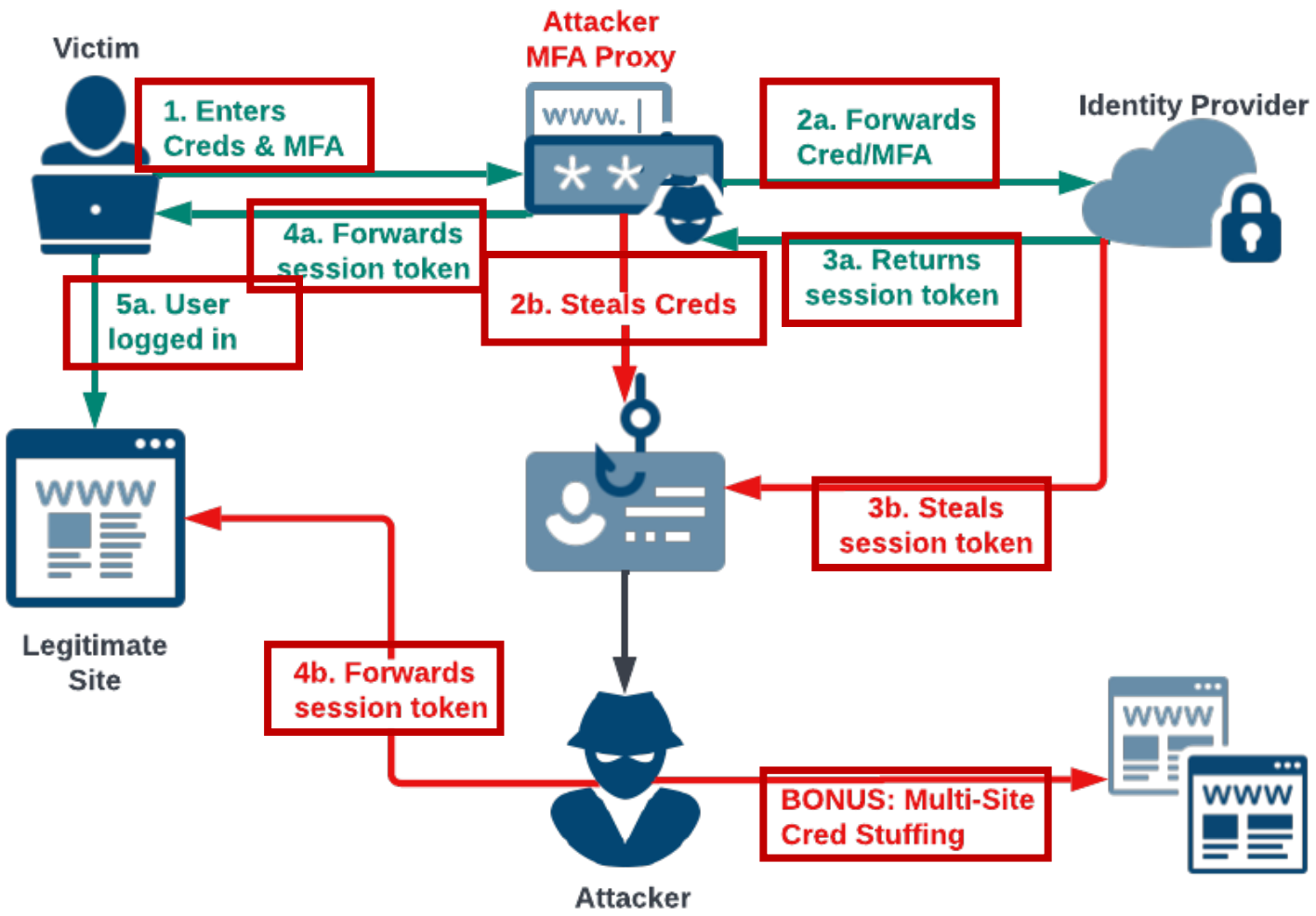
Guidance TL;DR:

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

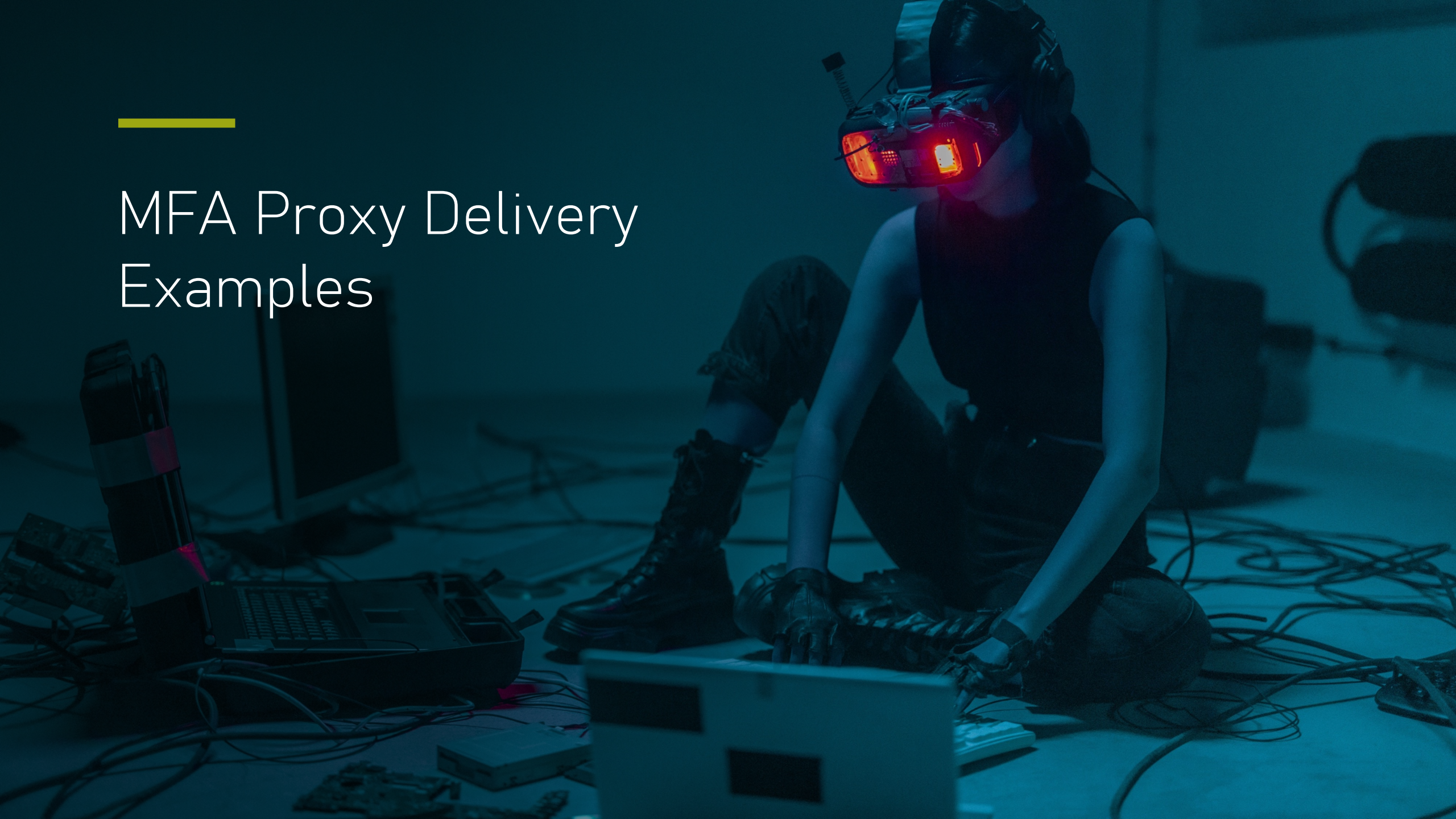
*Security questions aren't on the list because they're not secondary factors to password knowledge.*

# Background

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



# MFA Proxy Delivery Examples



# Initial Access – Lookalike Domains

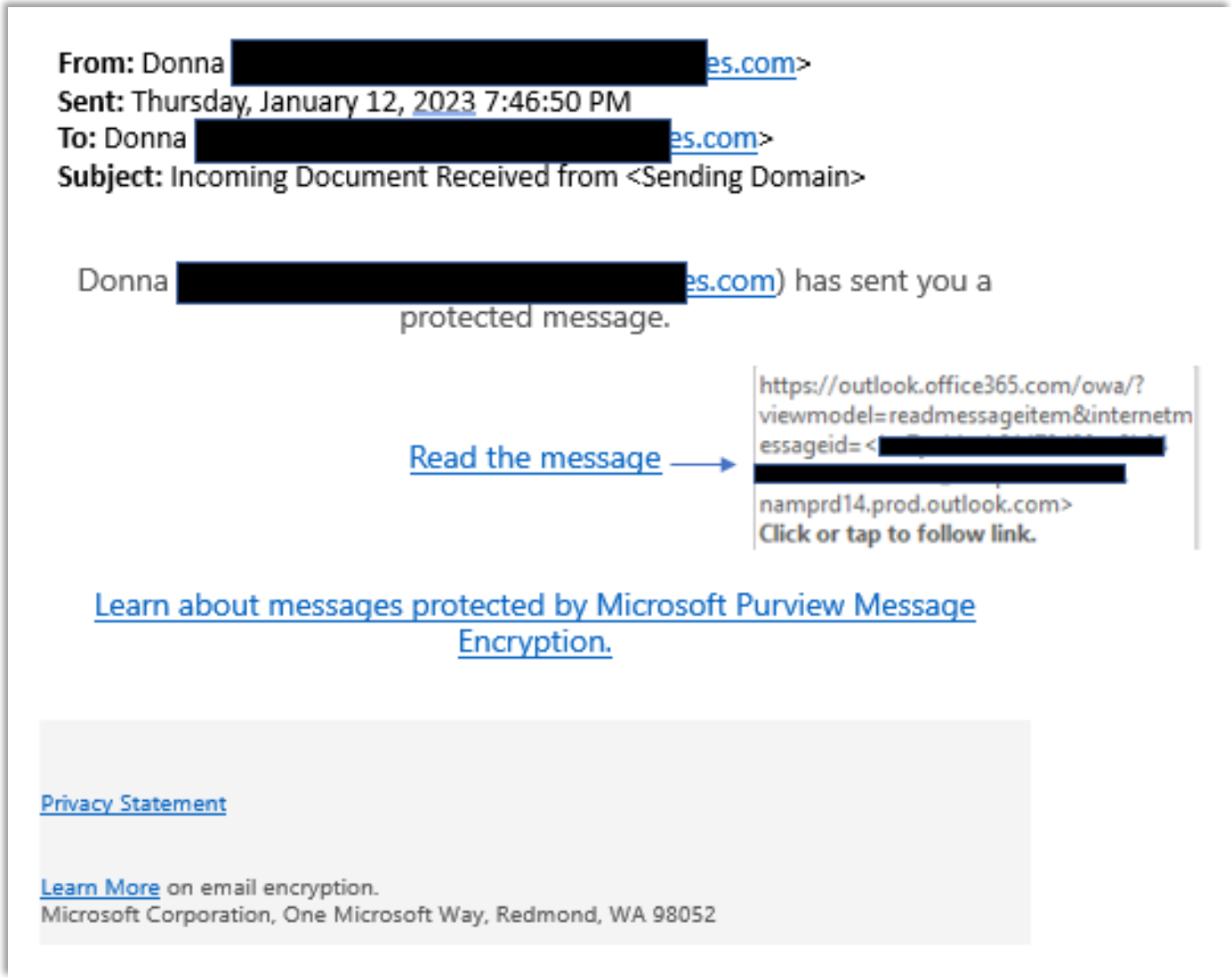
In this scenario, the threat actor compromises a trusted domain(BEC) and *simulates* their encryption product

- 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.

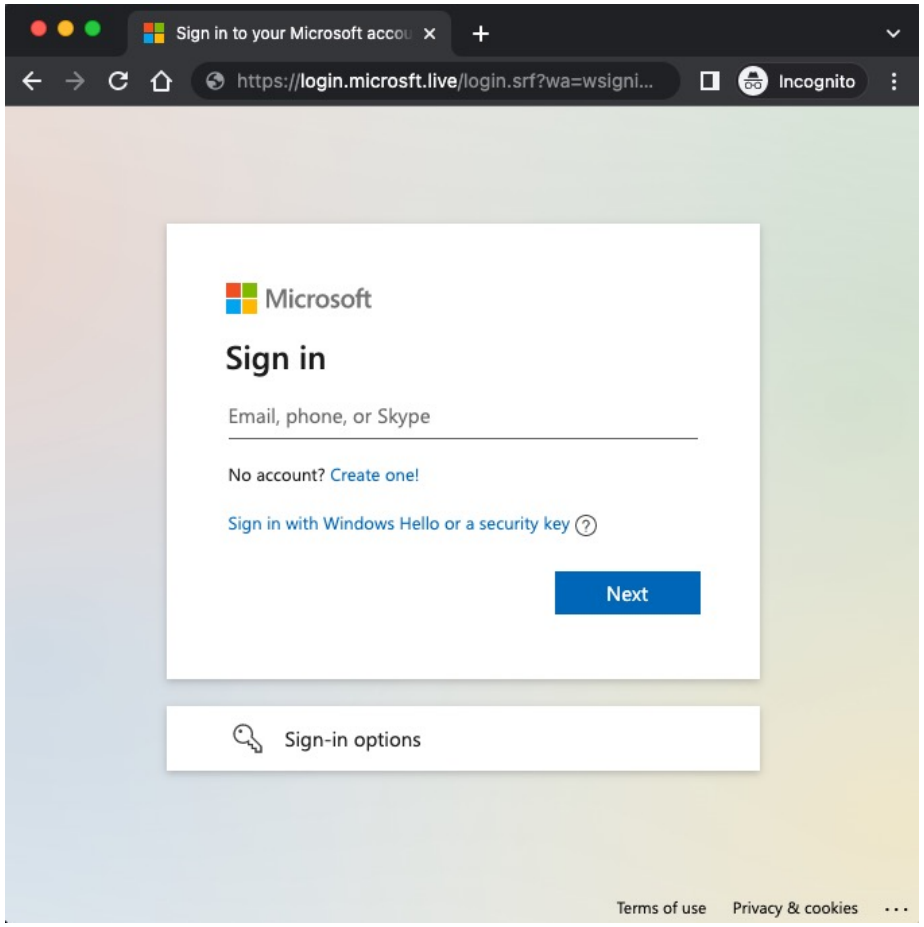
# Message Encryption

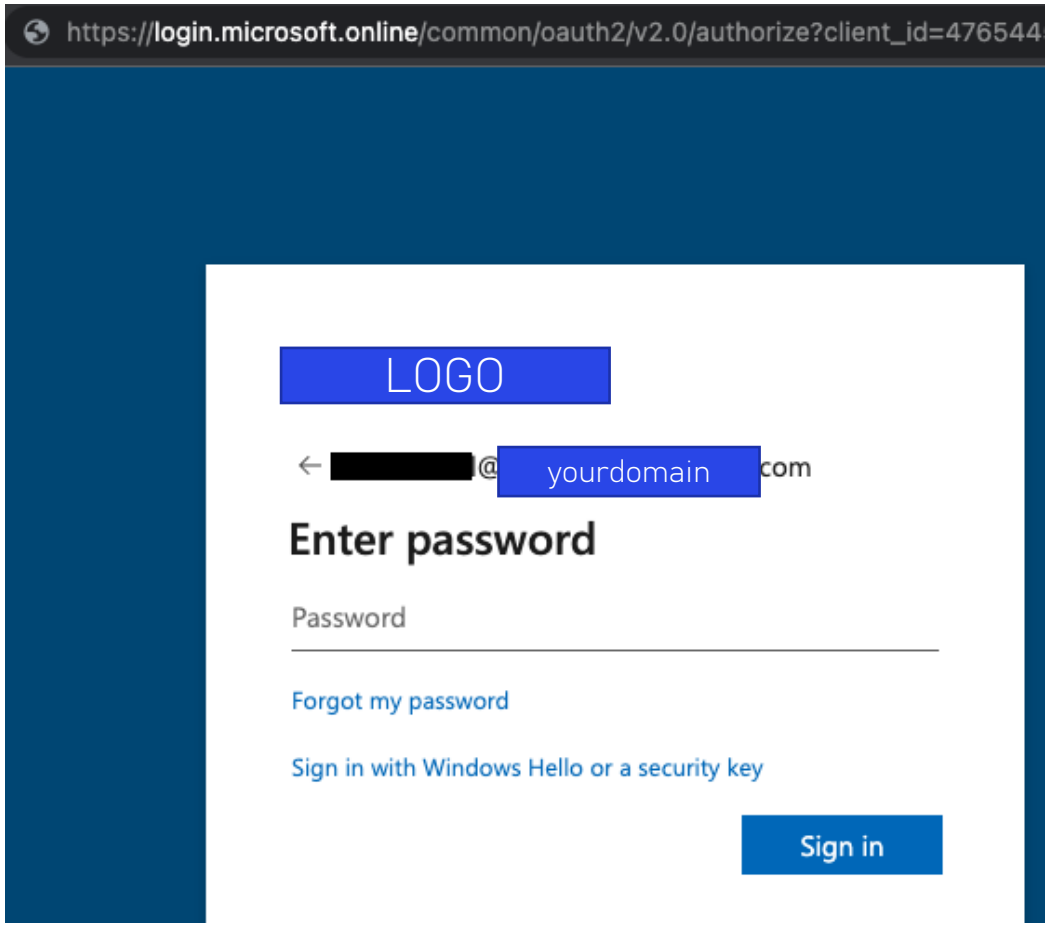
- With access to a compromised tenant, the threat actor takes advantage of native message encryption.
- The message isn't inspected, by Microsoft or other 3rd party mail gateways.
- Message body is opened in a browser to Microsoft, evading your ingress firewall.

Example Email Received Using Protected Message



# Victim experience



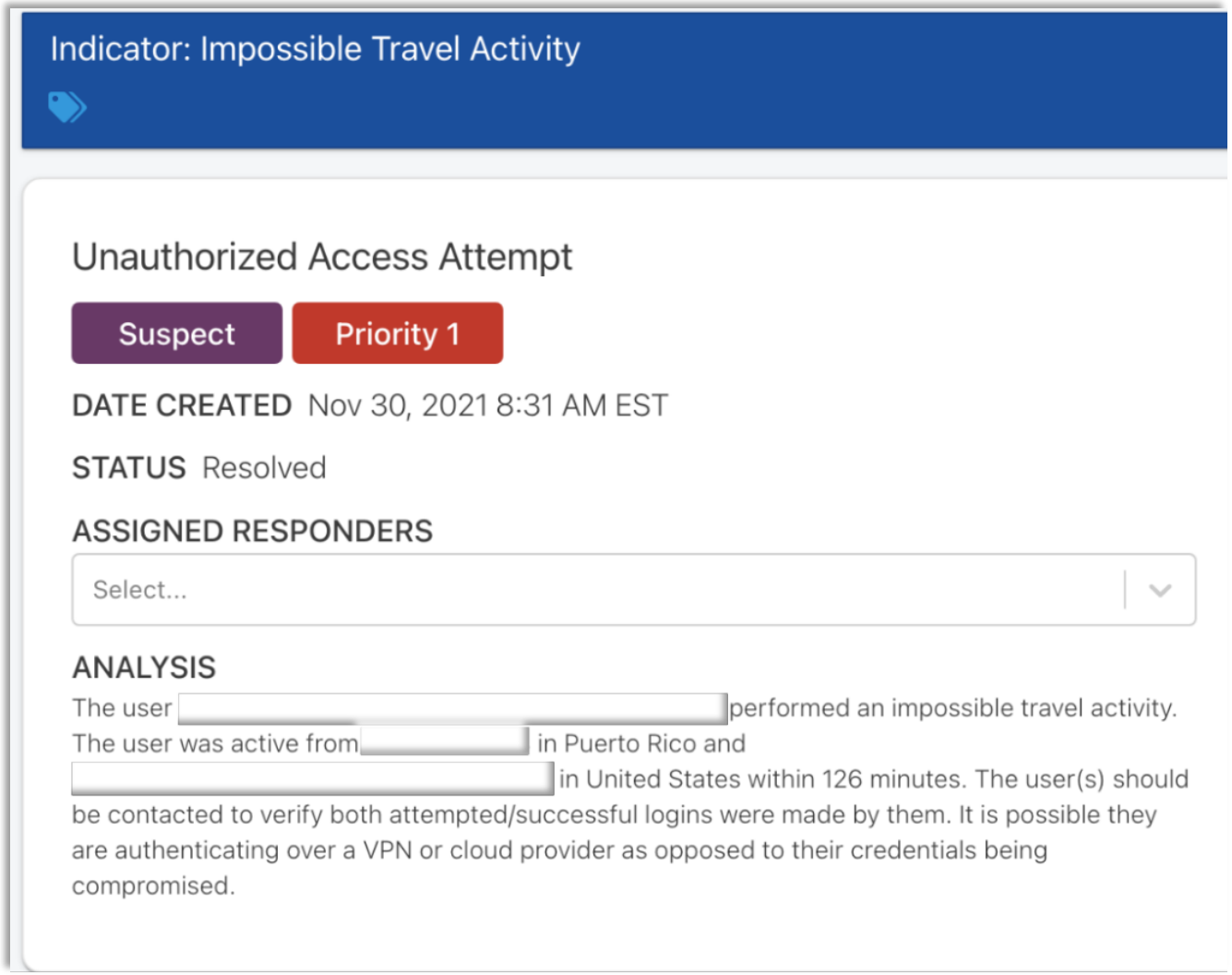

Generic and custom branding remains intact. The only tell is in the browser bar.
What's your org's click % rate on fake logon pages?


# Detecting Attacks

# Detecting Attacks

Impossible Travel

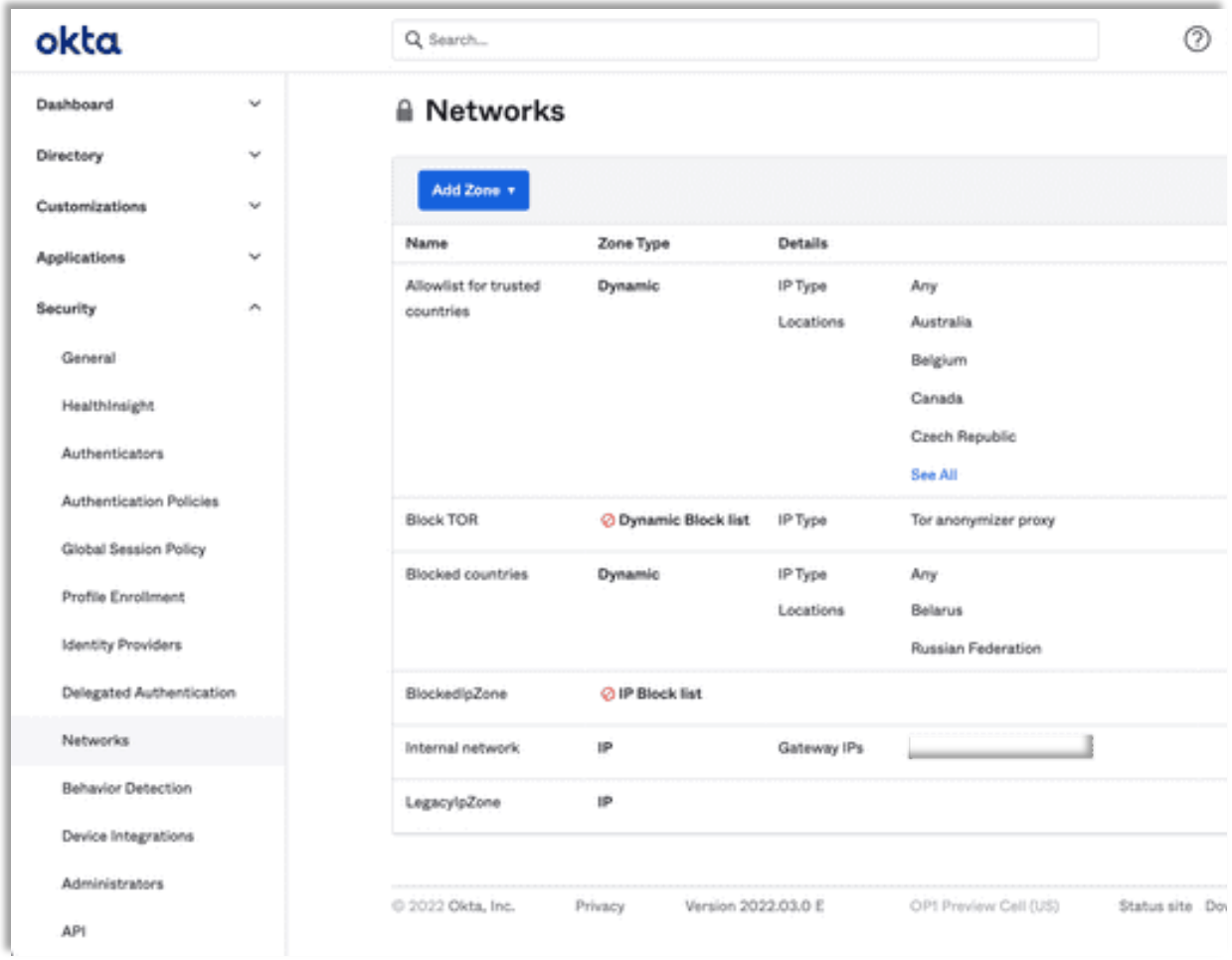
- Reasonably Accurate
- Use of consumer VPNs create false positives
- Geo-local proxy access frequently sold on dark web markets.



# Detecting Attacks

## Reputation-based

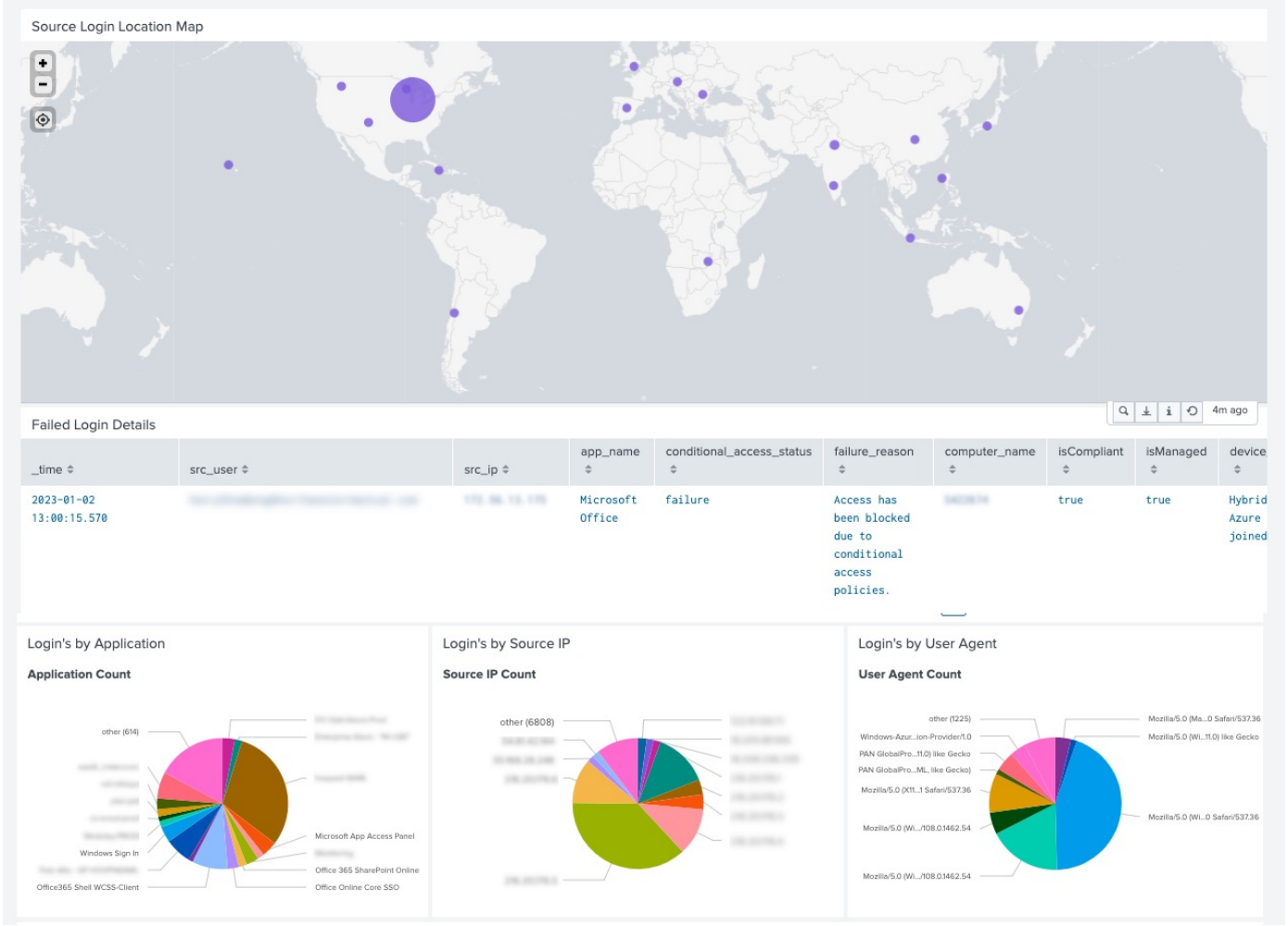
- Some identity providers can warn / block network ranges or ASNs.
- Use threat feeds to identify “bad neighborhoods” and feed via API.
- Use SOAR to send end-user notifications on risky sign-ins.



# Detecting Attacks

Changes to users and devices:

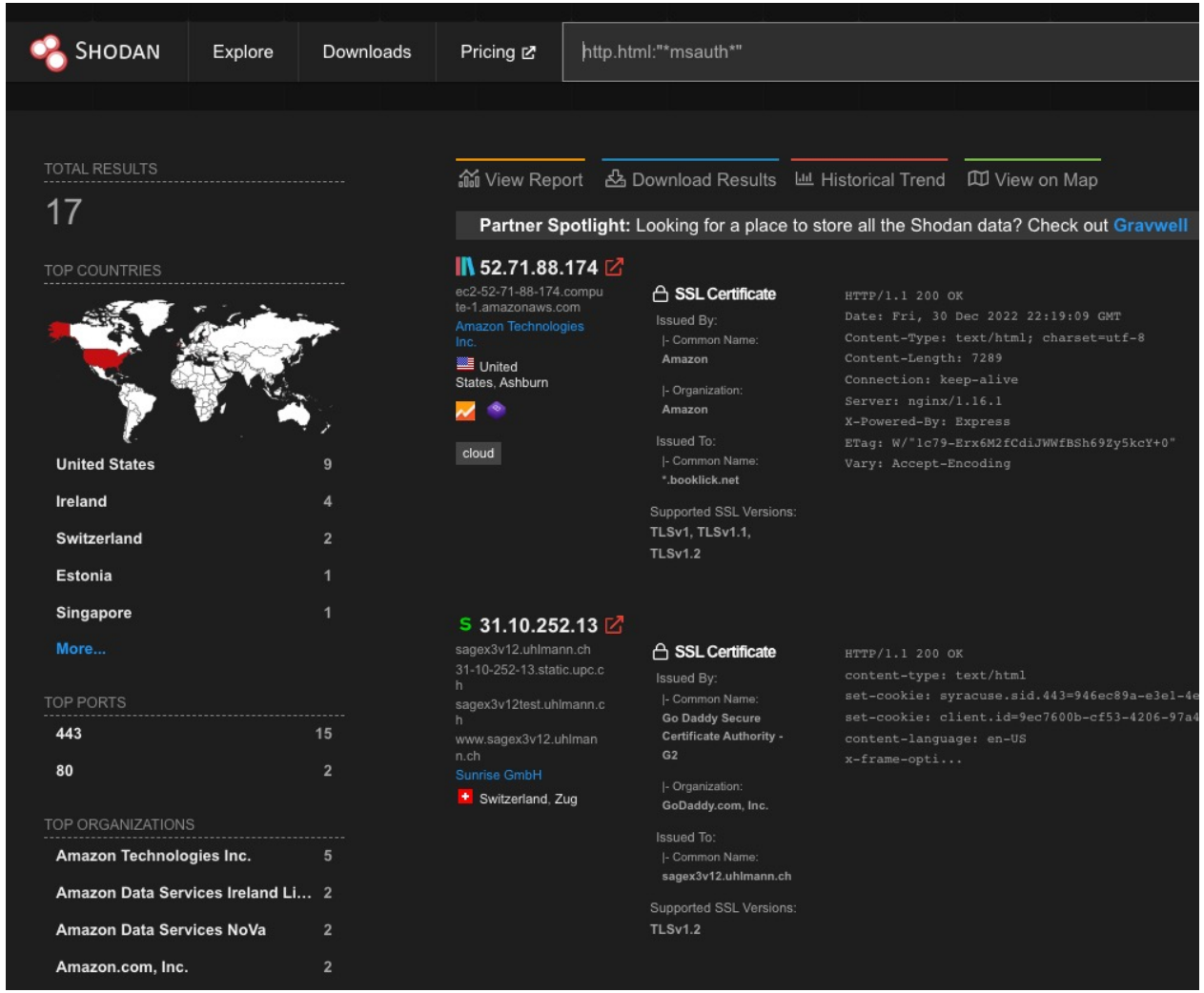
- Logon from previously unseen IP + authenticator change
- New device registration attempts: Azure AD join / inTune enrollment



# 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.



# 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/*`**

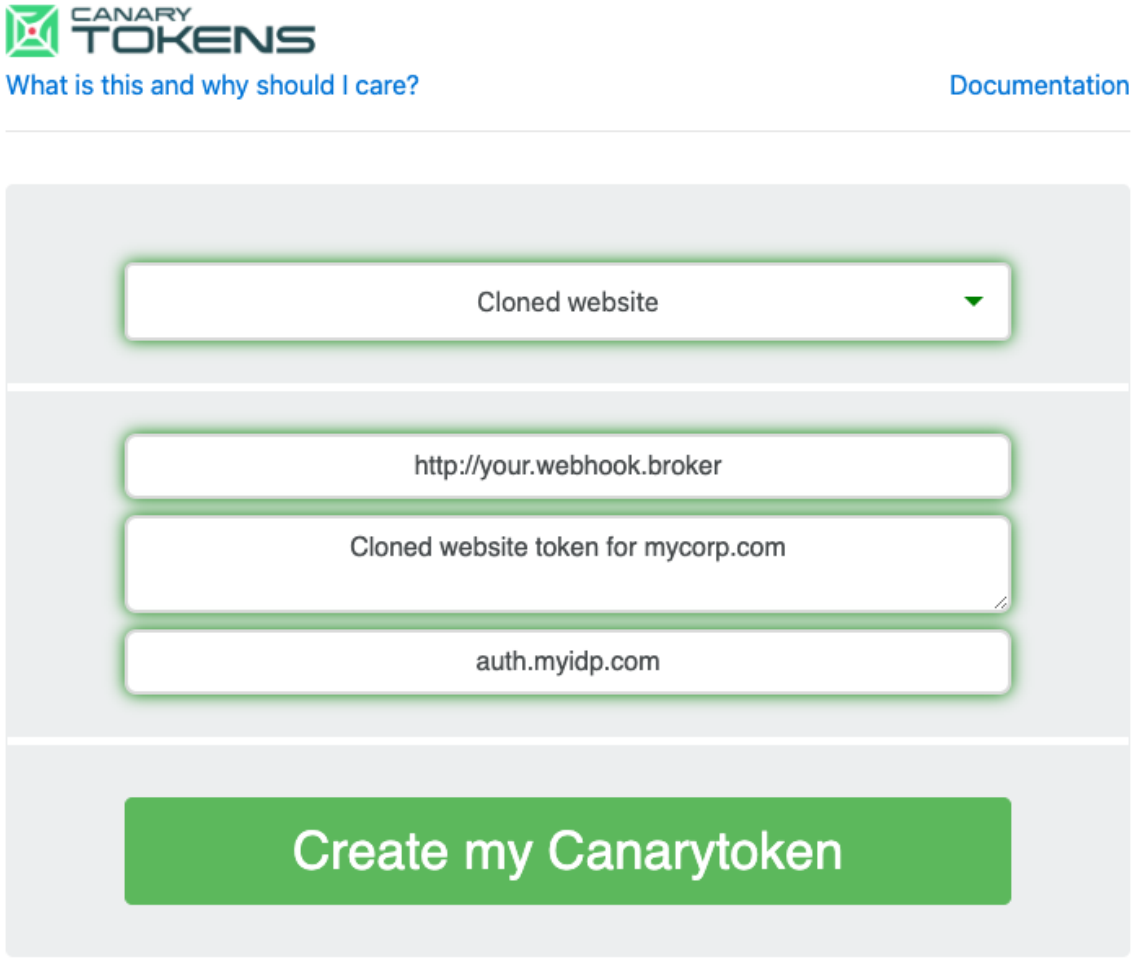
# Detecting Attacks – Advanced Methods

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

# Detecting Attacks

Script Canaries

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



# 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


| | 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 SEIM, 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