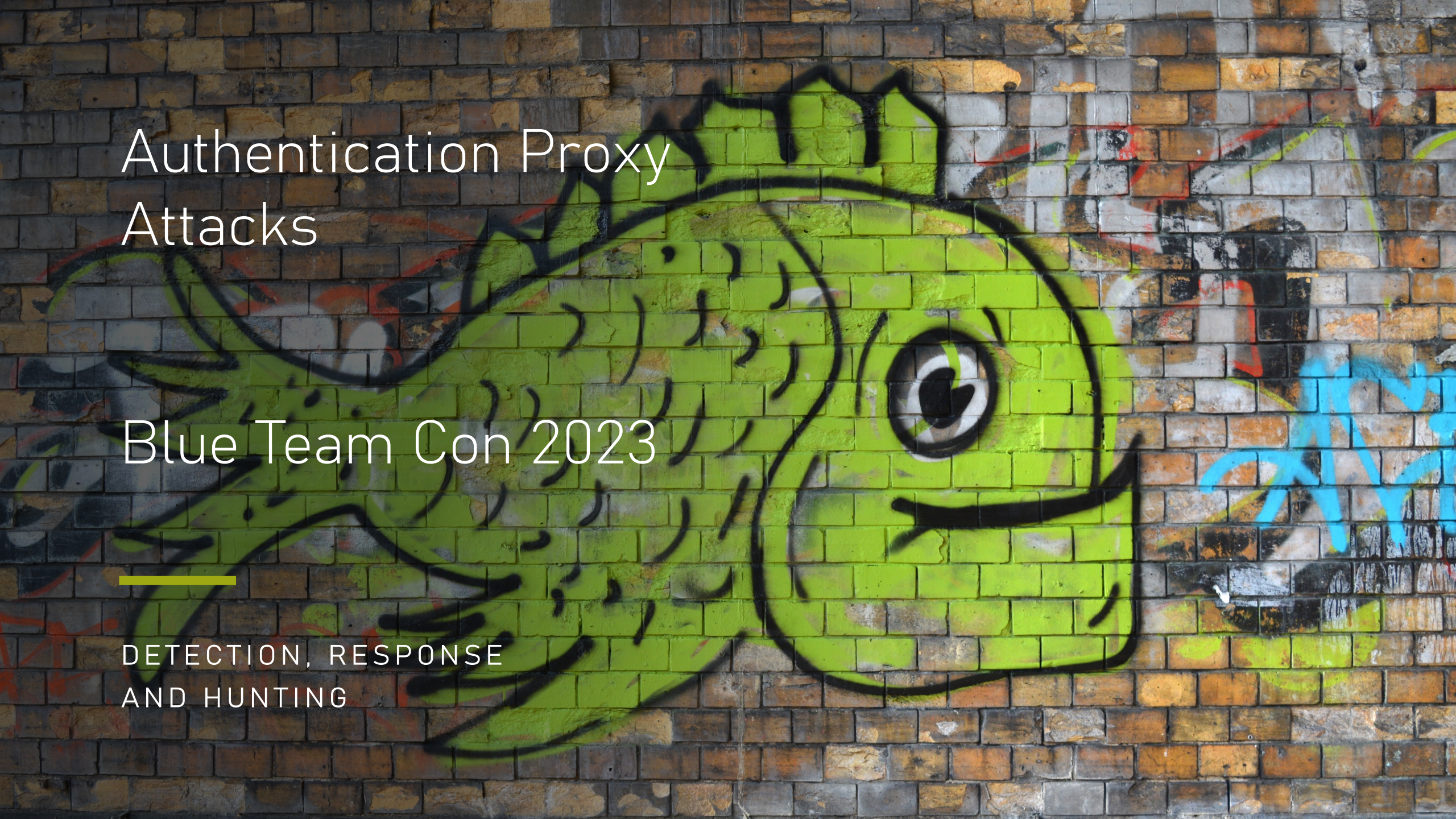


Authentication Proxy Attacks

Blue Team Con 2023

DETECTION, RESPONSE AND HUNTING

About

Chris Merkel

Senior Director, Cybersecurity Defense

Northwestern Mutual

@chrismerkel@infosec.exchange

@chris__merkel@threads.net

Chester Le Bron

Lead Engineer, Incident Response

Northwestern Mutual

@123Le_Bron

@chester-le-bron

Where we're at

"Typical" Enterprise Org:

- Has MFA enabled.
- May have moved past SMS and push approval.
- Using Azure AD for single-sign on.

Good News: you're protected against 99% of credential attacks.

Bad News: adversaries always operate one level above "typical".

CISA HAS ENTERED THE CHAT

CISA embraces the designation:

Phishing-Resistant MFA

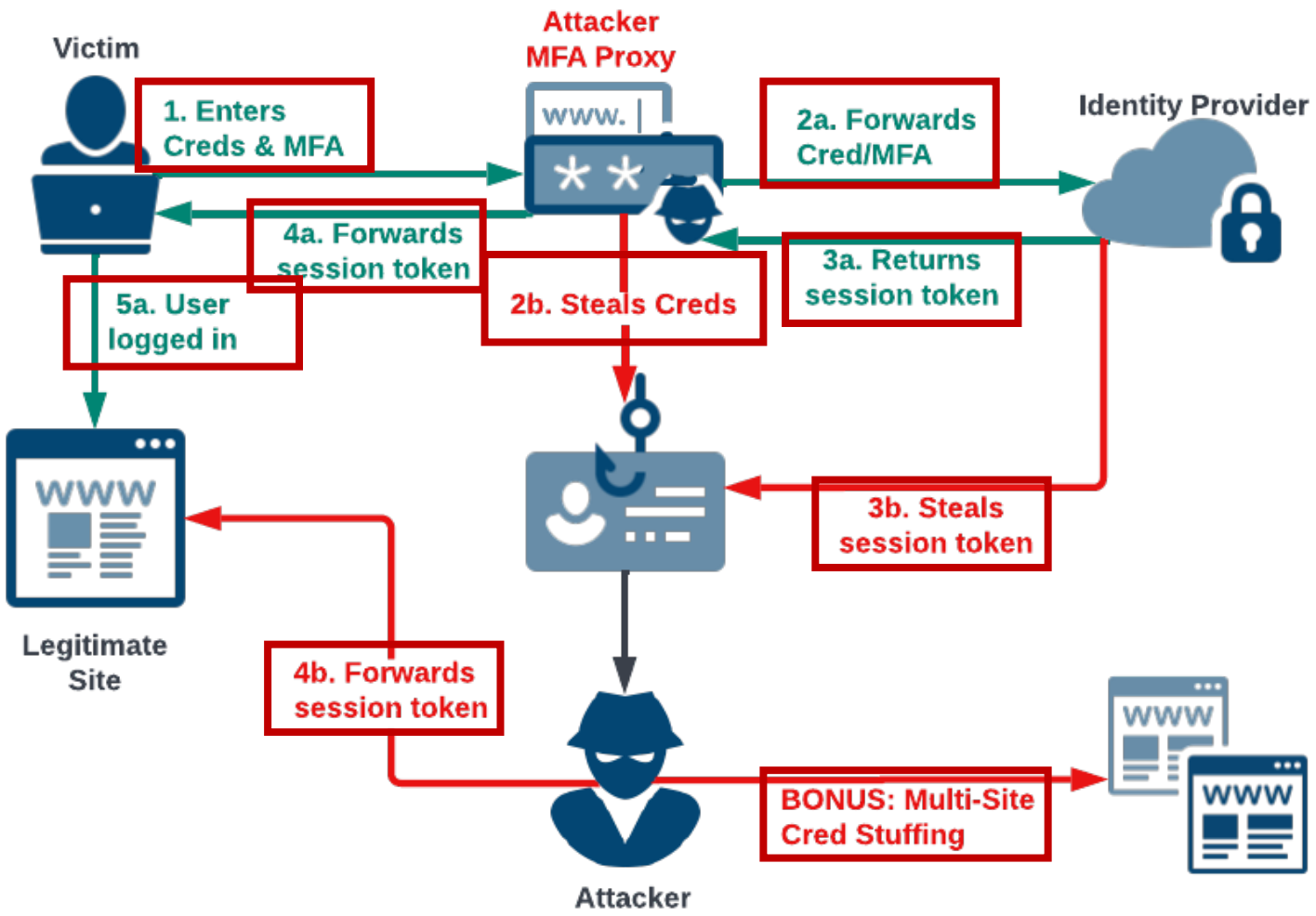
Guidance TL;DR:

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

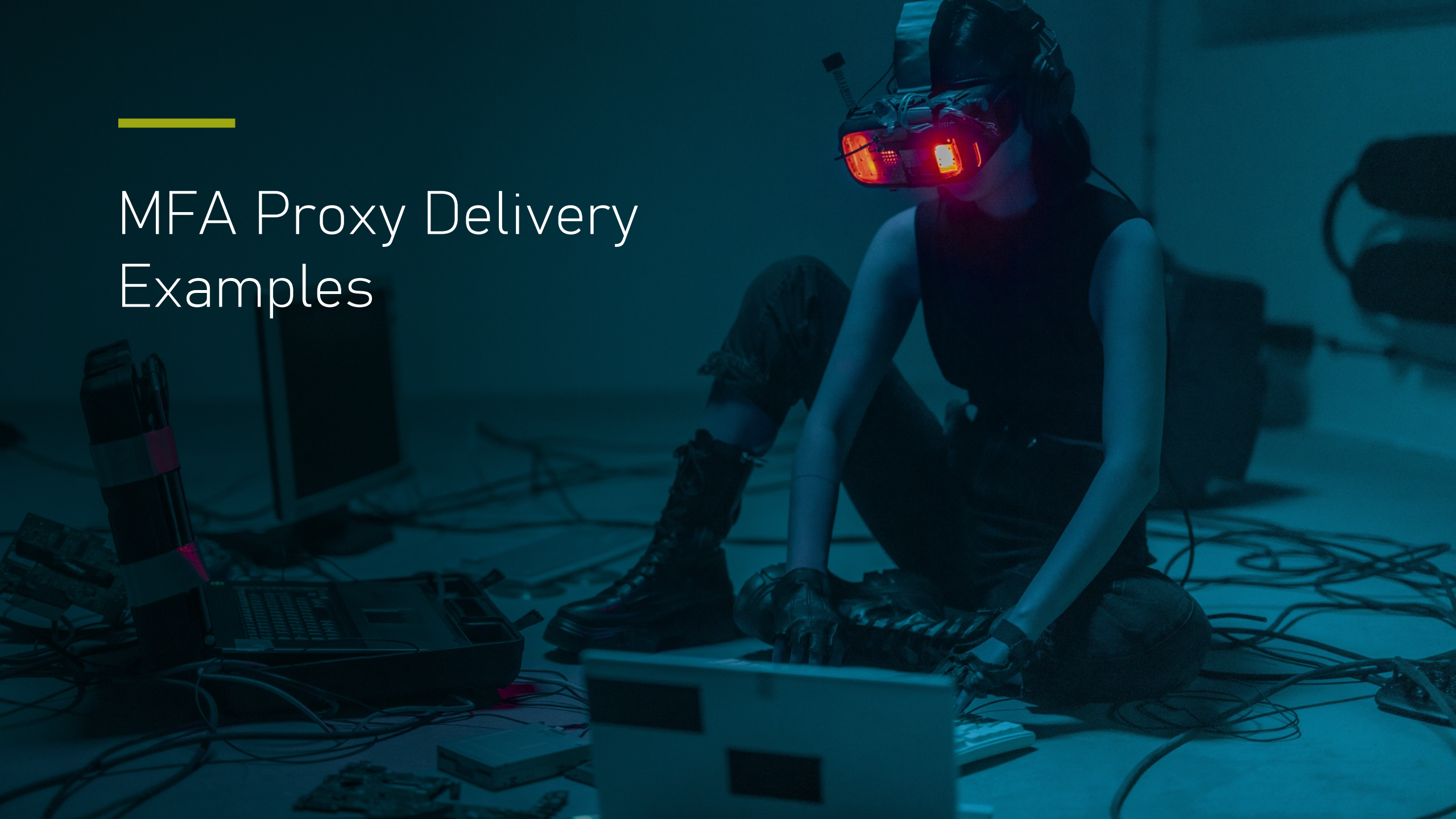
Security questions aren't on the list because they're not secondary factors to password knowledge.

Background

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

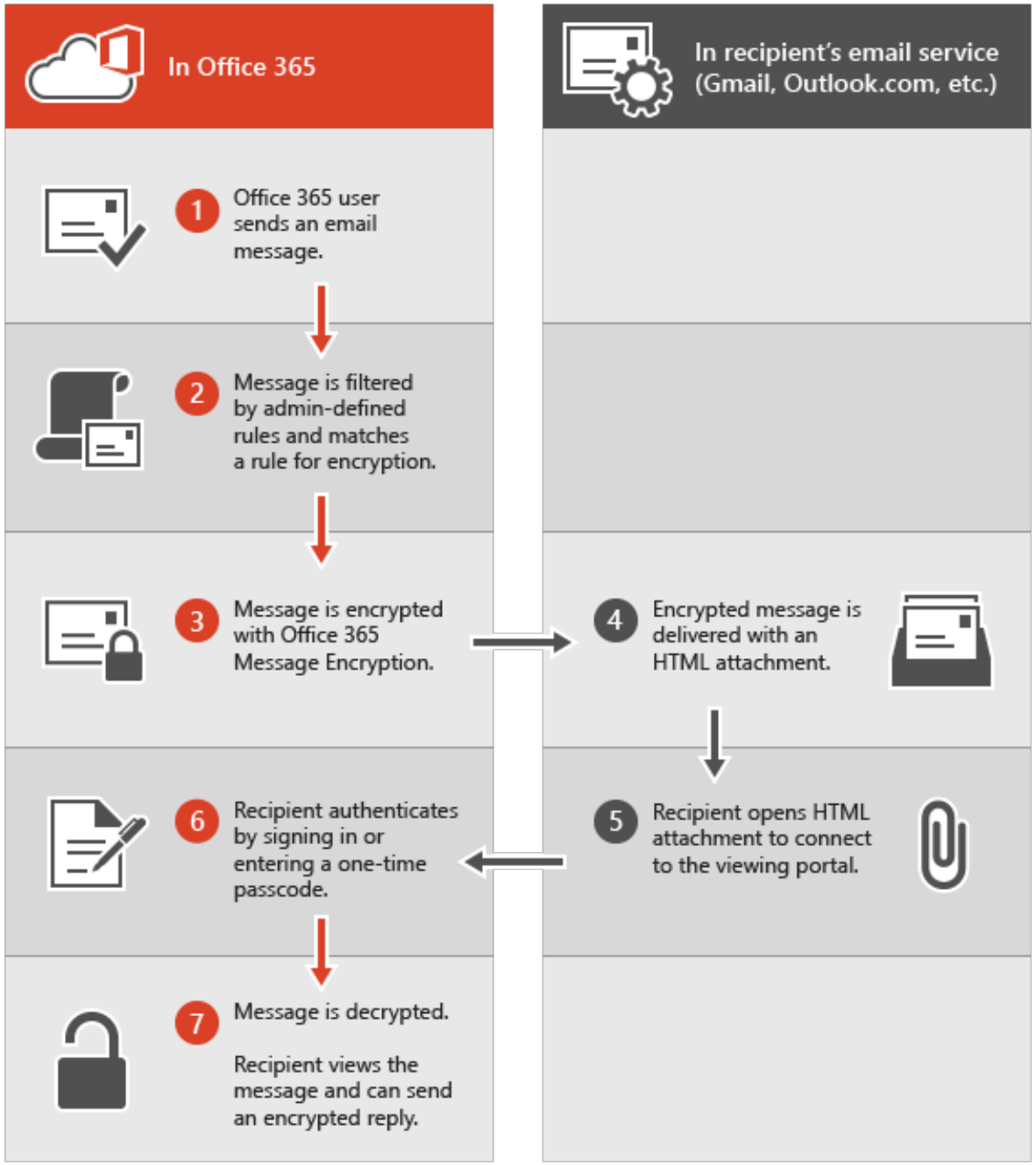


MFA Proxy Delivery Examples



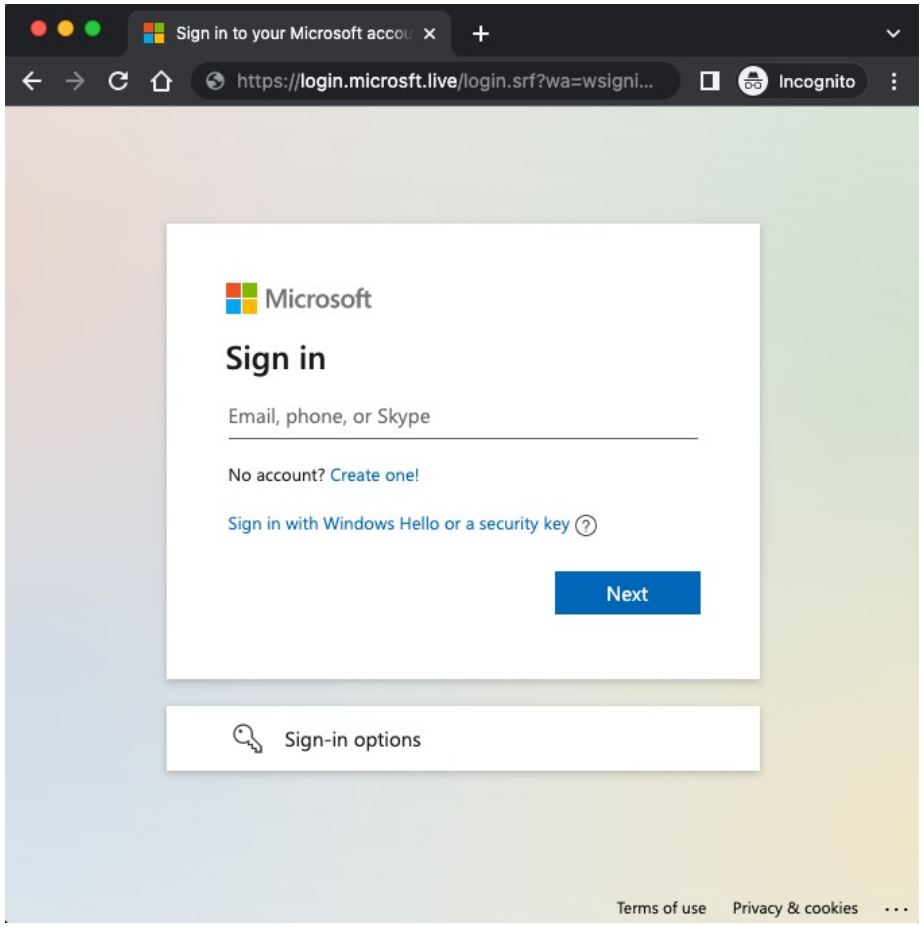
Delivery Methods

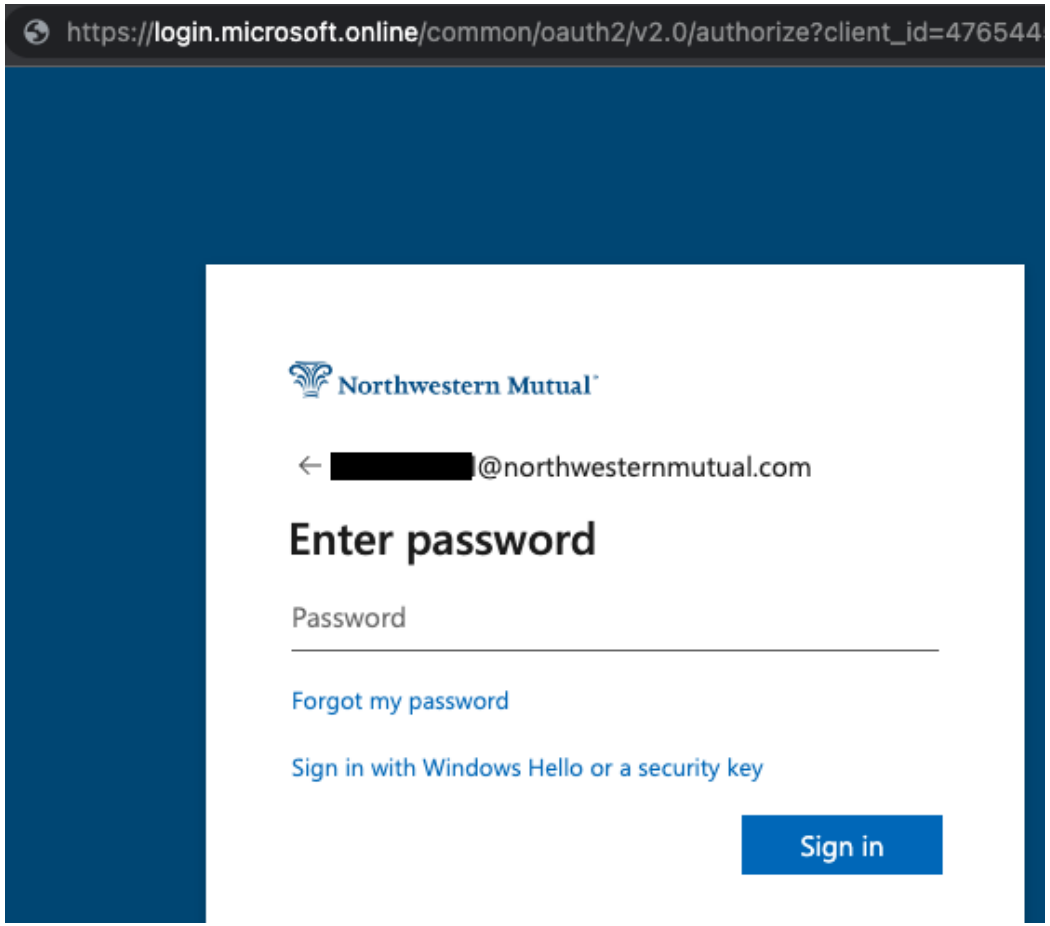
- Traditional Phishing Messages
- Encrypted Message Hollowing
- ATO + Microsoft Purview



https://learn.microsoft.com/en-us/purview/legacy-information-for-message-encryption

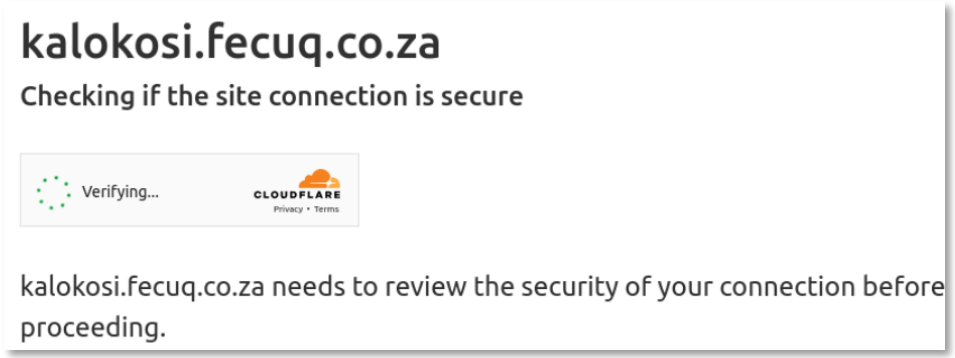
Victim experience





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



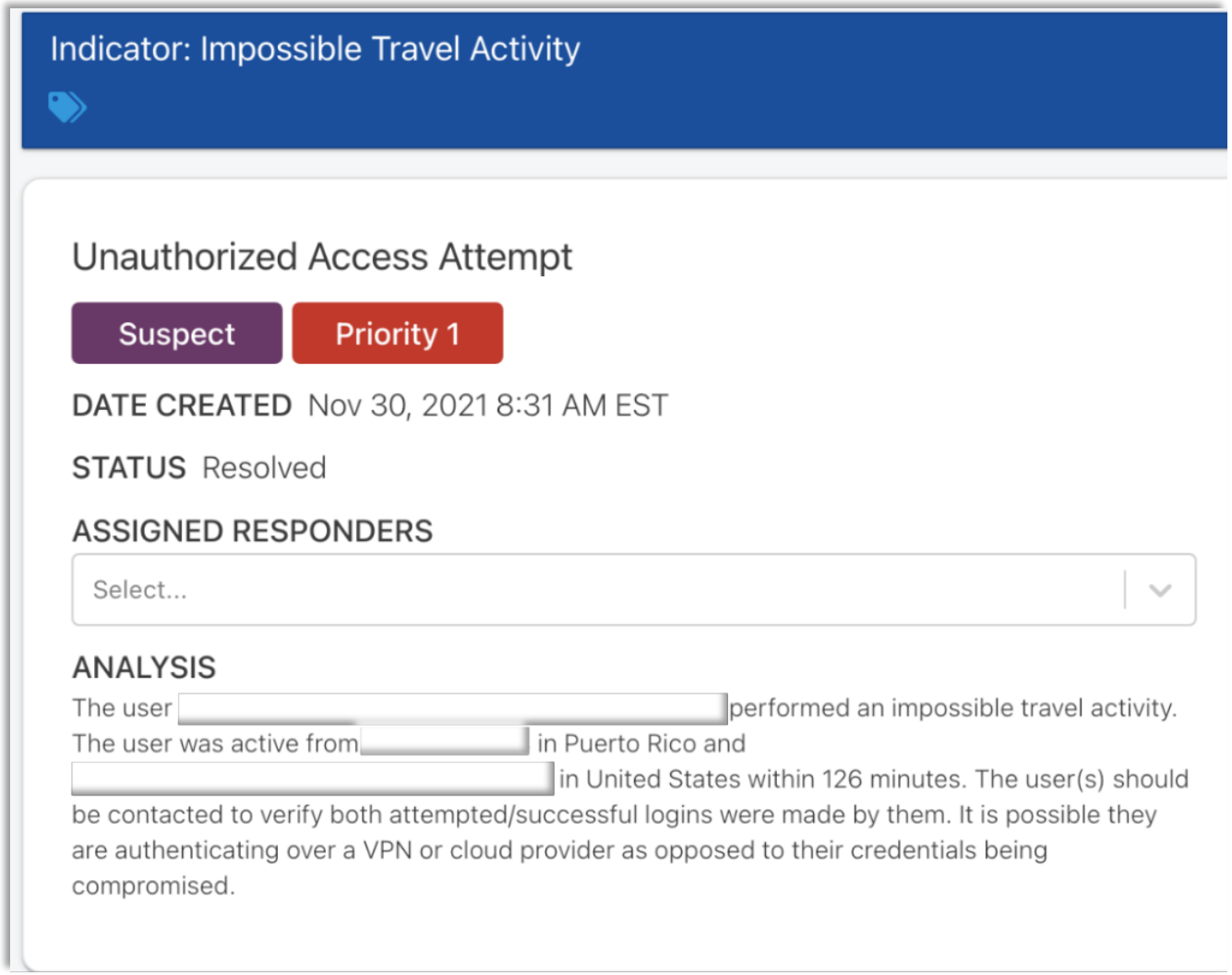
- Some adversaries are getting better about OSINT, less infrastructure re-use.
- Increased use of anti-inspection techniques
  - Referrer checking
  - Sandbox detection
  - Encrypted mail
  - Human checking (NEW)
- Increased use of SMS based phishing to bypass inspection

Detecting Attacks

Detecting Attacks

- **Impossible Travel**
- Anonymized IP

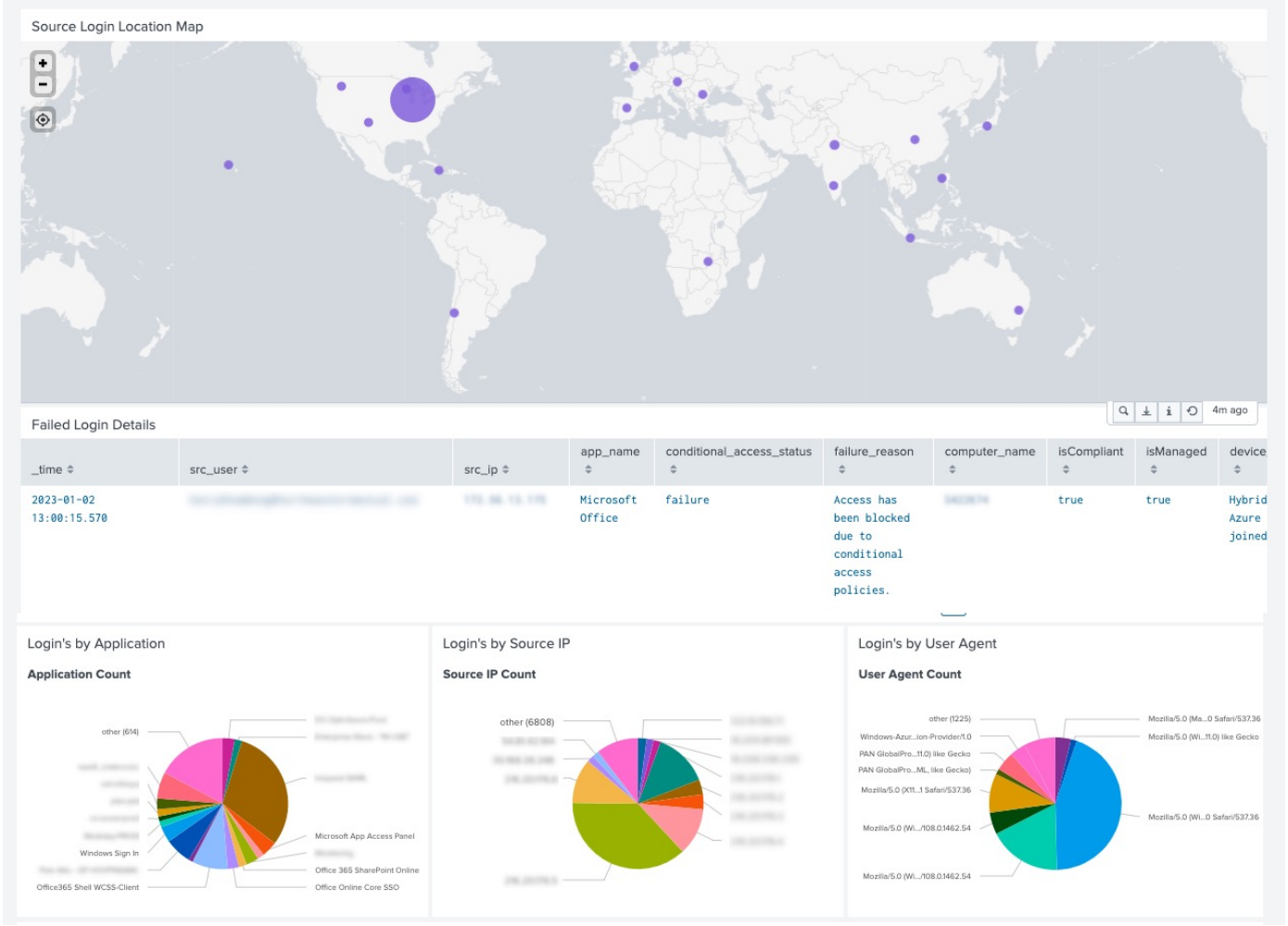
  Use of consumer VPNs create false positives.
- Geo-local proxy access frequently sold on dark web markets.
- Signins from IPs that resolve to recently registered domain(s)



Detecting Attacks

Changes to users and devices:

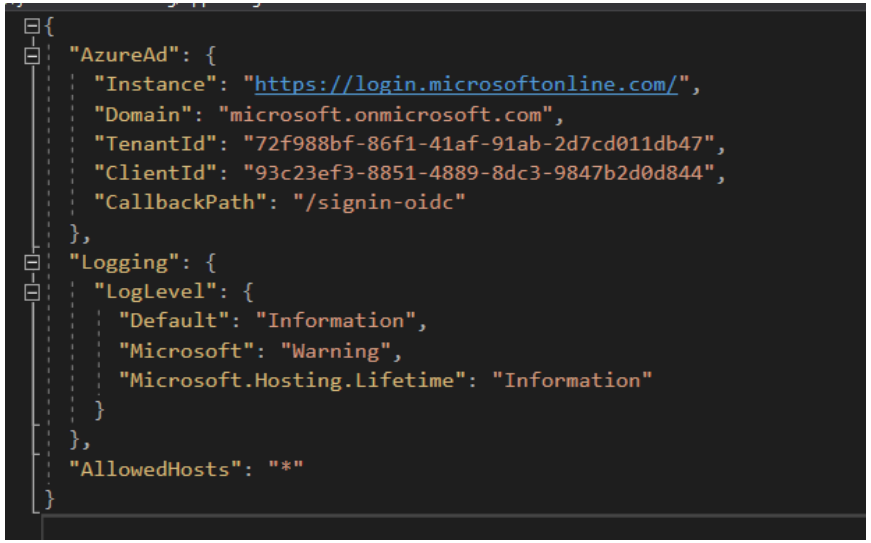
- Logon from previously unseen IP + authenticator change
- New device registration attempts: Azure AD join / inTune enrollment



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

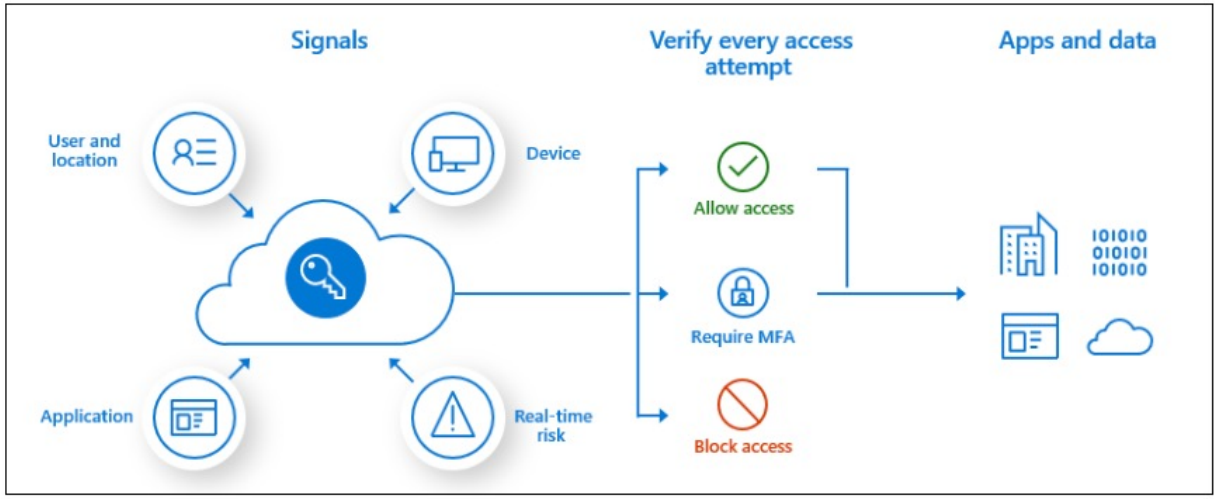
⚠ Terminating **all** access to resources, especially in response to a compromised account, requires revoking refresh tokens, not just refreshing the password.

Investigating and Responding to Attacks

- Reviewing M365 logs for evidence of access:
  - Sign-in logs
  - OneDrive logs
  - Mail forwarding rules
  - Authenticator changes
  - User creation

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

https://learn.microsoft.com/en-us/azure/active-directory/conditional-access/concept-conditional-access-policies

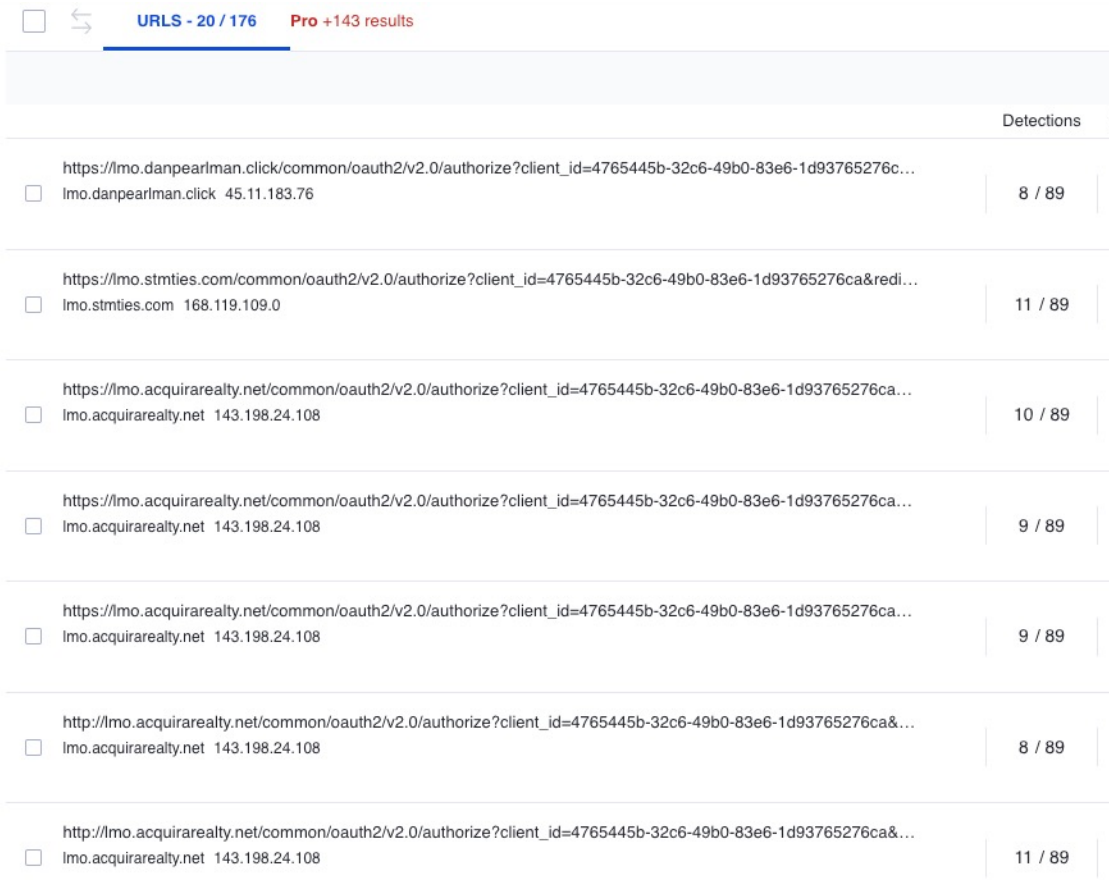
Threat Hunting

- 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

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

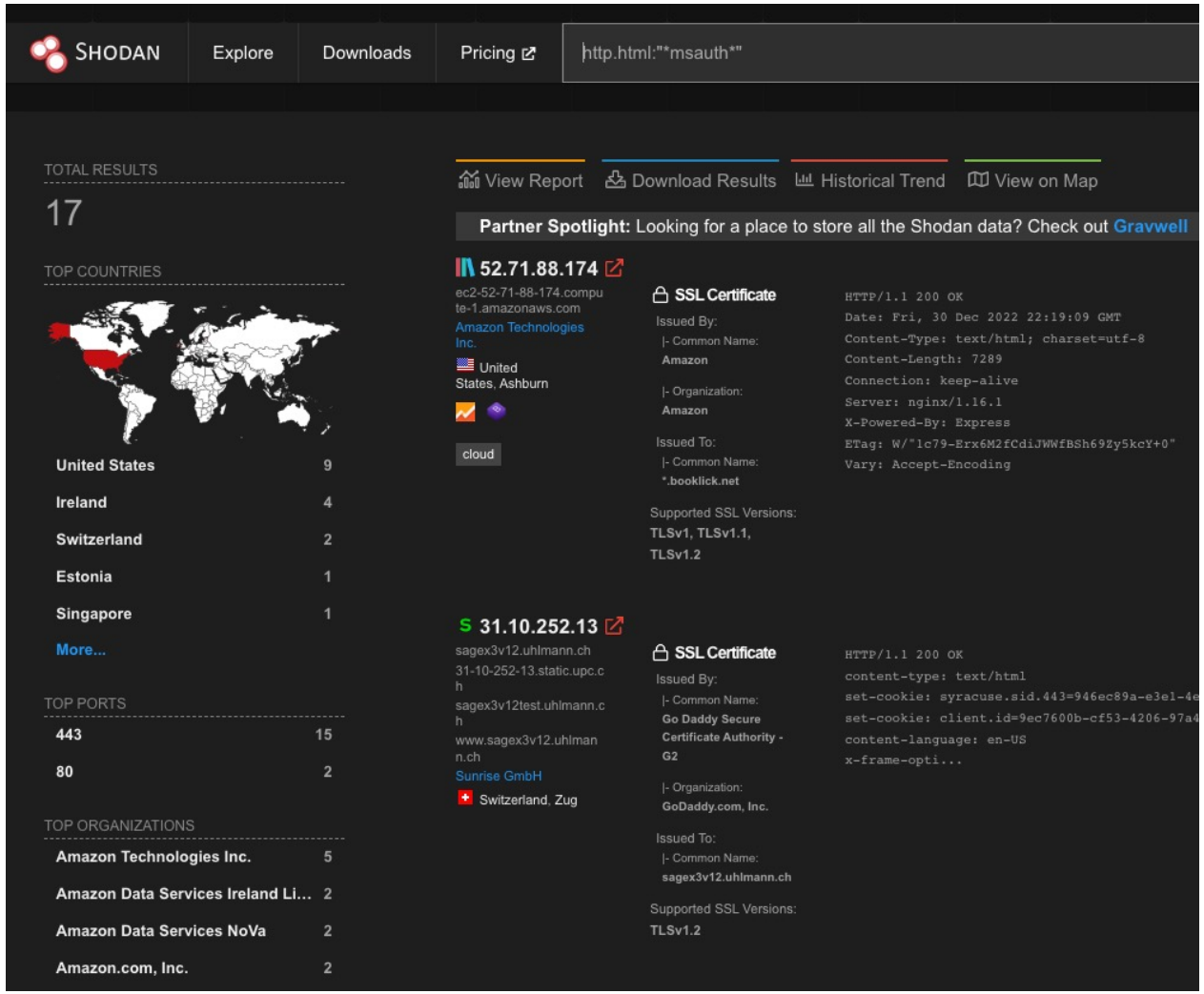
  These are hidden behind referrers but will show up in firewall
- Passive DNS is your friend



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.



- 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

Let's chat in the lounge!

Slides:
github.com/
p0rkchop/
presentations/

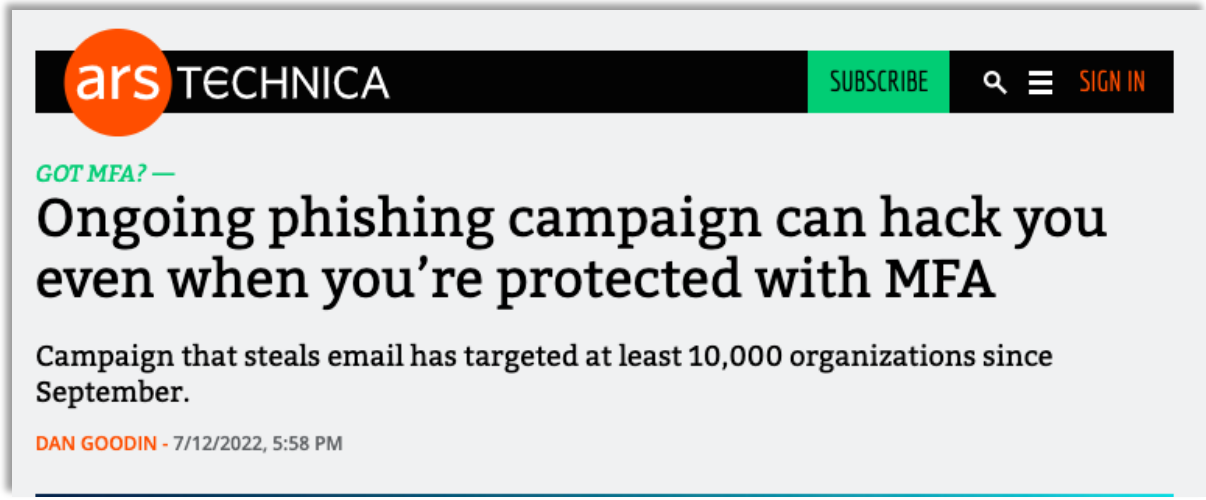
THINGS WE HAD TO CUT FOR TIME BUT THOUGHT WERE PRETTY COOL

Bonus slides

The bad news

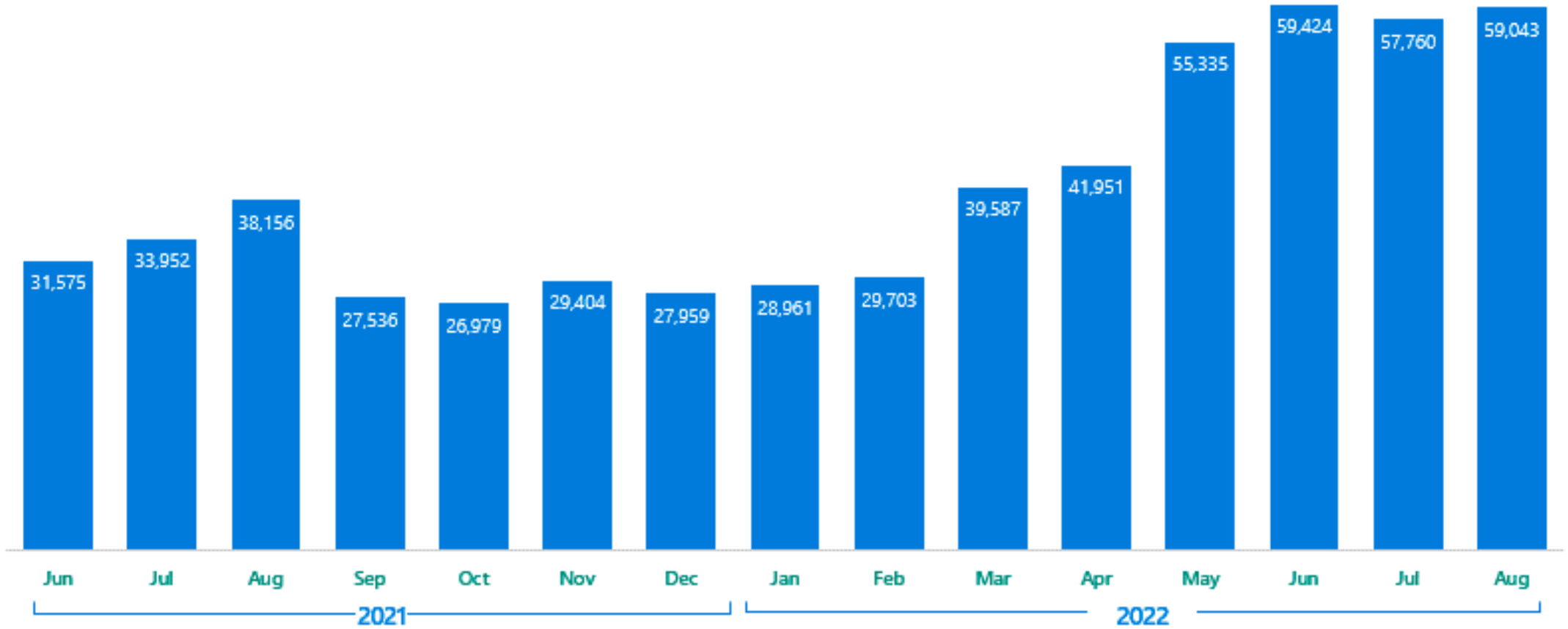

BLEEPINGCOMPUTER
Home > News > Security > Microsoft accounts targeted with new MFA-bypassing phishing kit
Microsoft accounts targeted with new MFA-bypassing phishing kit
By Bill Toulas
August 3, 2022
02:02 PM
0


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

Token Replay

Detected token replay attacks per month



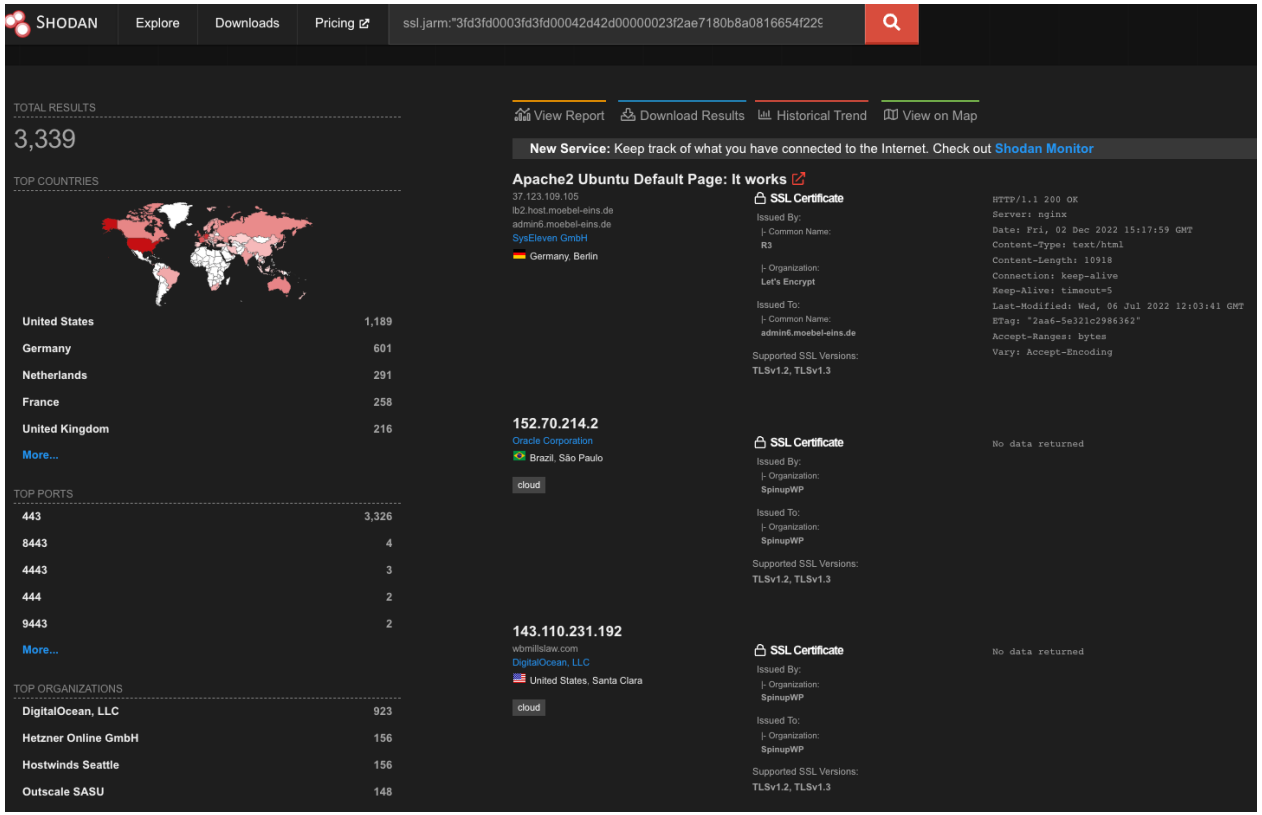
Source: Azure AD Identity Protection Anomalous Token detection

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

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

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/*`