whennotif

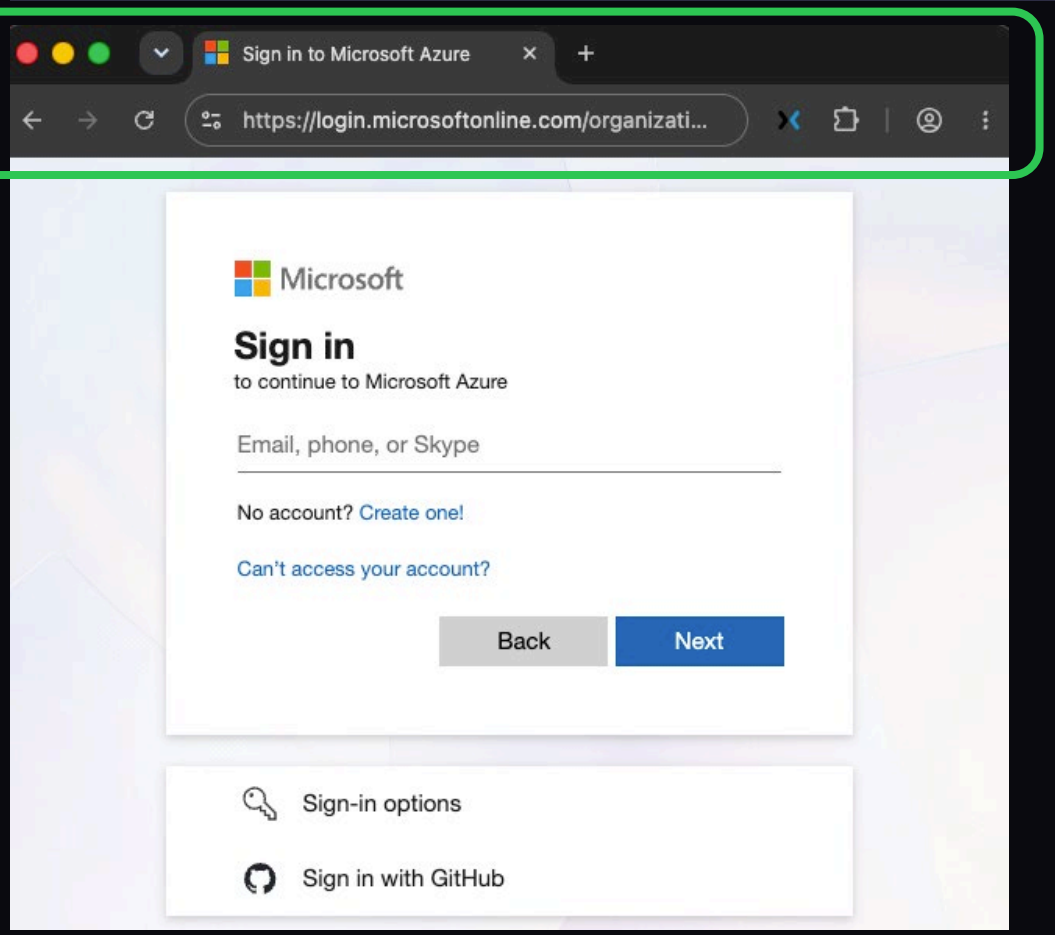
IT-SECX 2026

Detect, Defend, Disrupt

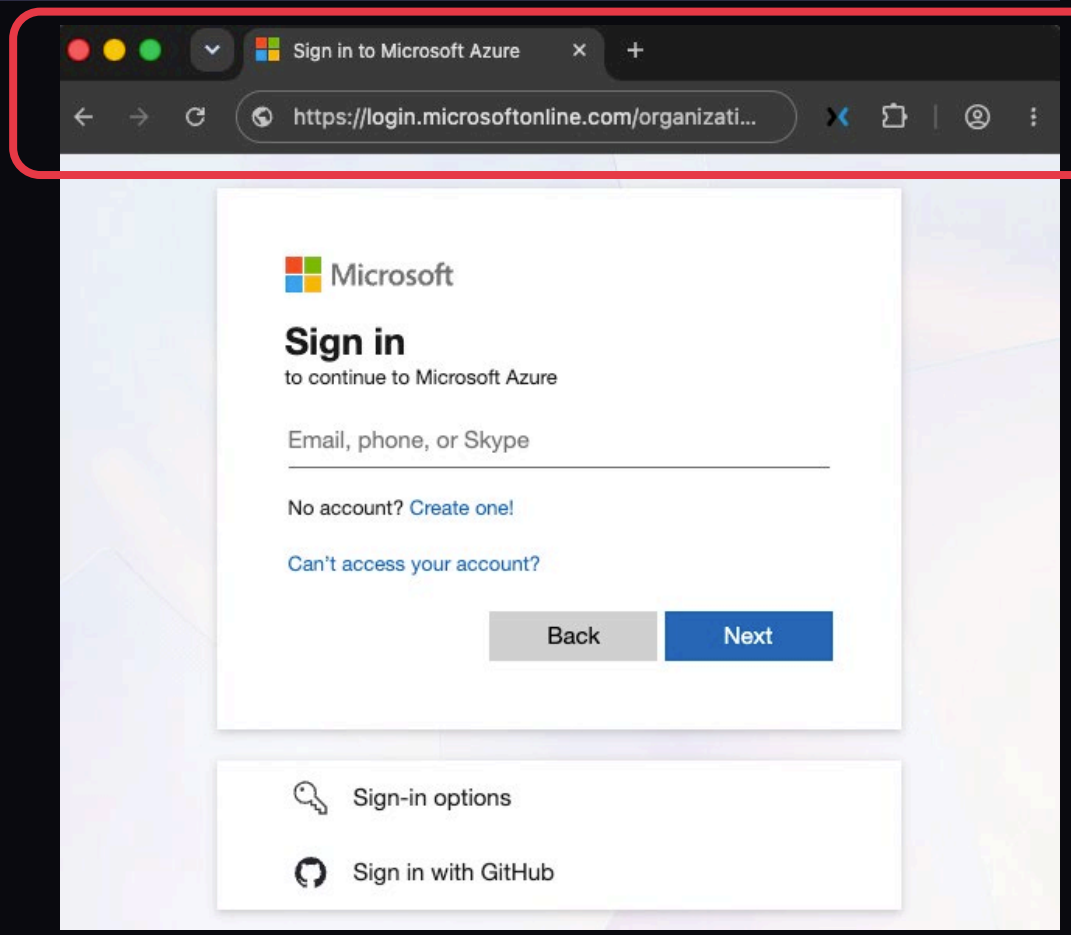
Ein Playbook gegen “Adversary in the middle“-Phishing

JÜRGEN WALDL, BSC · BASE-IT GMBH · WHENNOTIF.IO · 02.10.2026

Which one is fake?



vs.



About me



Blog: https://whennotif.io/

LinkedIn: walju juergen.waldl@baseit.at

Jürgen Waldl

LEAD ARCHITECT SECURITY · BASE-IT GMBH

> 20 Jahre IT Infrastruktur & Security Erfahrung | FHSTP Absolvent | MS Security Nerd | Sports Lover

- Entra ID & Active Directory Security
- Microsoft Sentinel und Detection Engineering
- Defender XDR & MS Zero Trust Architektur
- AI & Agent Security

Phishing erlebt seinen x-ten Frühling?

AB 1995

Credential Harvesting

AOHell – die Geburtsstunde des „Phishings“

2000+

Gefälschte Loginseiten

(schlecht), nachgebaute Loginportale

2018+

MFA im Vormarsch

Licht am Ende des Tunnels?

2020+

Reverse-Proxy-Frameworks

Evilginx, Modlishka & Co – “modernes“ Phishing

Der größte Einzelvektor ist der Login

28 %

PHISHING

und Social Engineering: größter Einzelvektor in DART-Engagements

17 %

VALID ACCOUNTS

Anmeldung mit gültigen, gestohlenen Credentials

18 %

PUBLIC-FACING APPS

nächstgrößerer Vektor, mit Abstand

Quelle: Microsoft Digital Defense Report 2025, CISO Executive Summary

> **These methods bypass MFA and enable long-term access and data exfiltration without triggering alerts.**

MICROSOFT DIGITAL DEFENSE REPORT 2025 · ÜBER AITM UND DEVICE CODE PHISHING

Drei Generationen - (k)eine Lösung?



GEN 1 · Reverse Proxy

klassischer AitM Proxy.



GEN 2 · MFA Downgrade

AitM Proxy “with a twist“.



GEN 3 · Credential Relay Phishing

back to the past - but better!

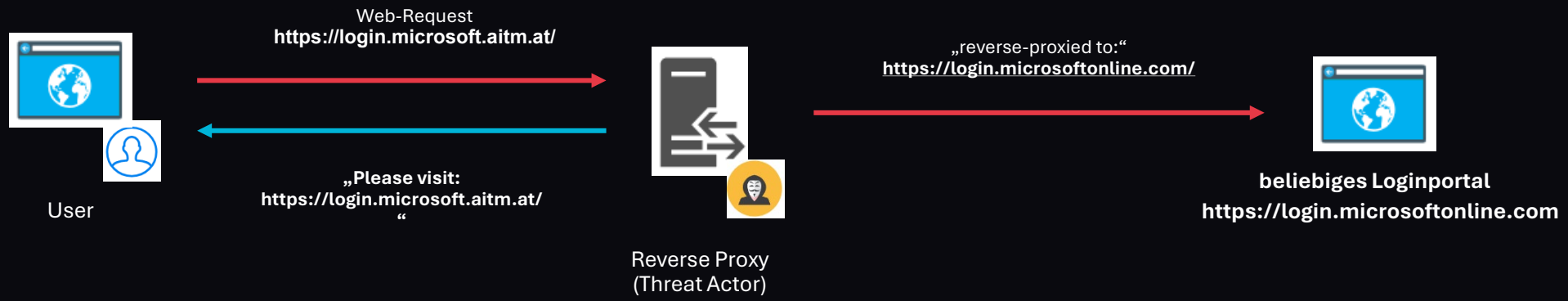
AKT I

Detect

01

Reverse-Proxy-AitM und die Grenzen clientseitiger Erkennung

Der Proxy forwarded den gesamten Traffic

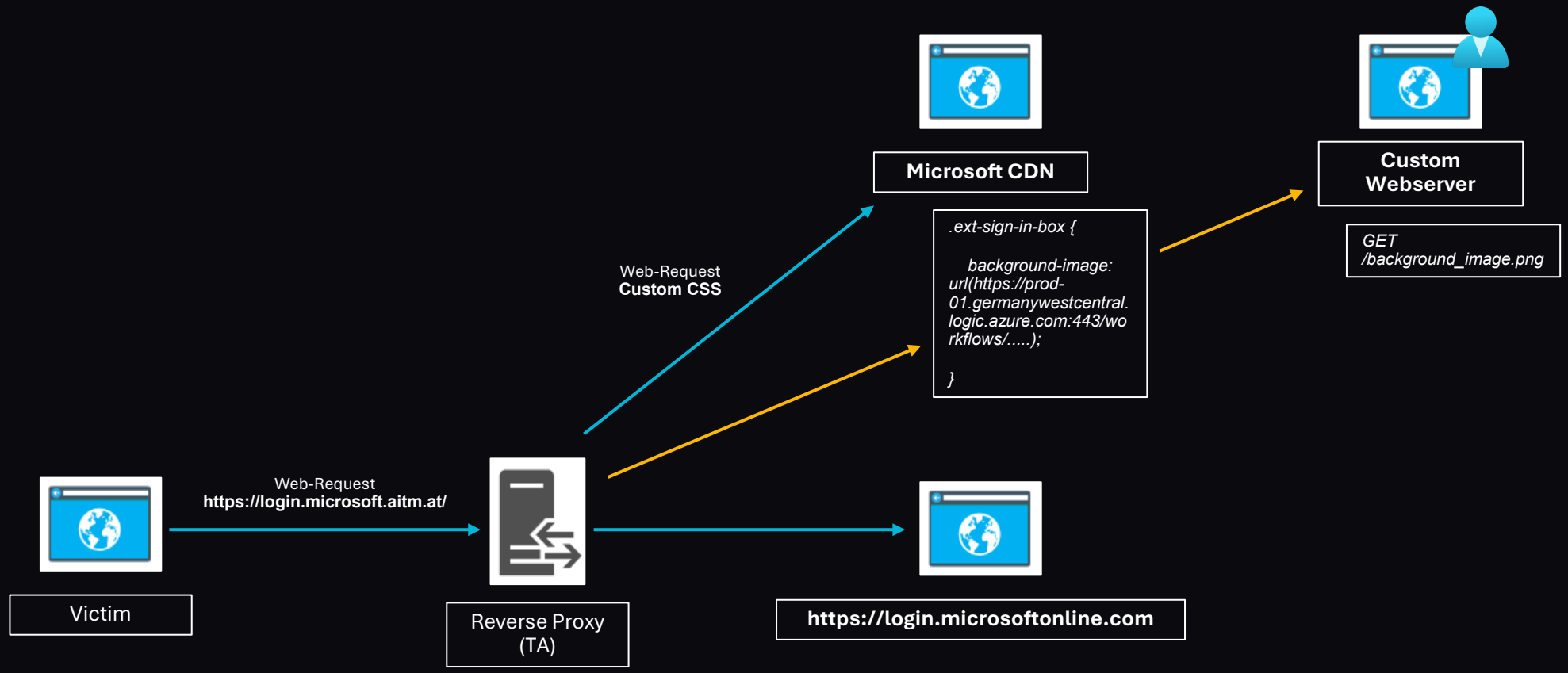


CSS for the win?

CSS

```
.ext-sign-in-box {
  background-image: url(
    https://prod-194.westeurope.logic.azure.com/workflows/…/invoke?…
  );
}
```

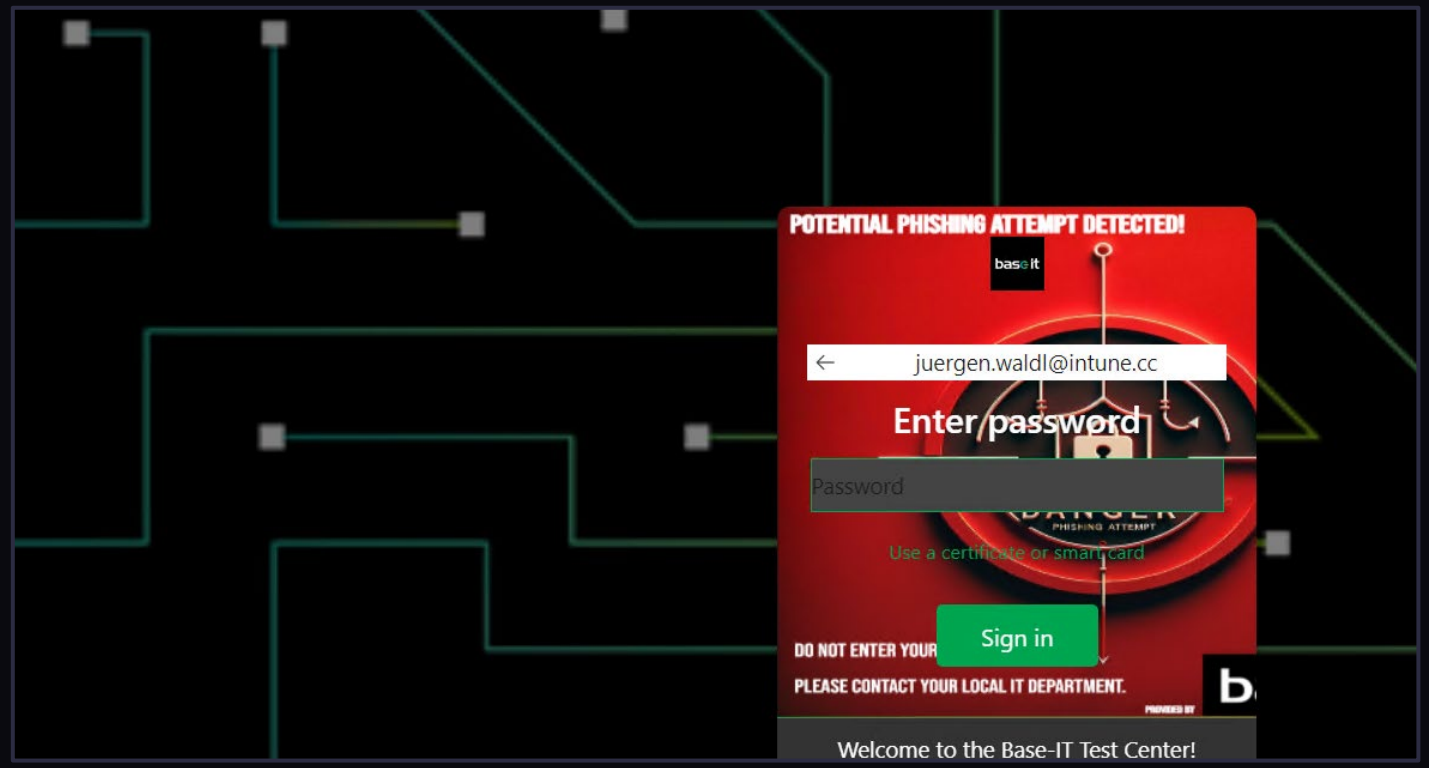
CSS for the win?



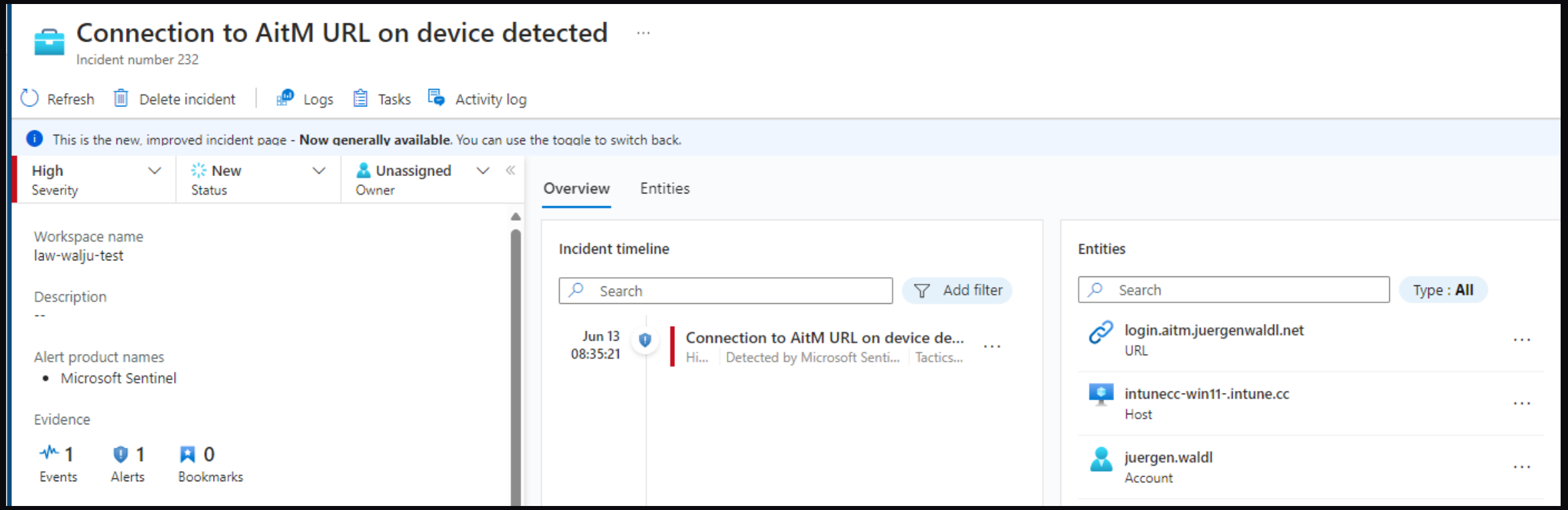
No magic – just CSS

Vom Tenant Branding zum Incident

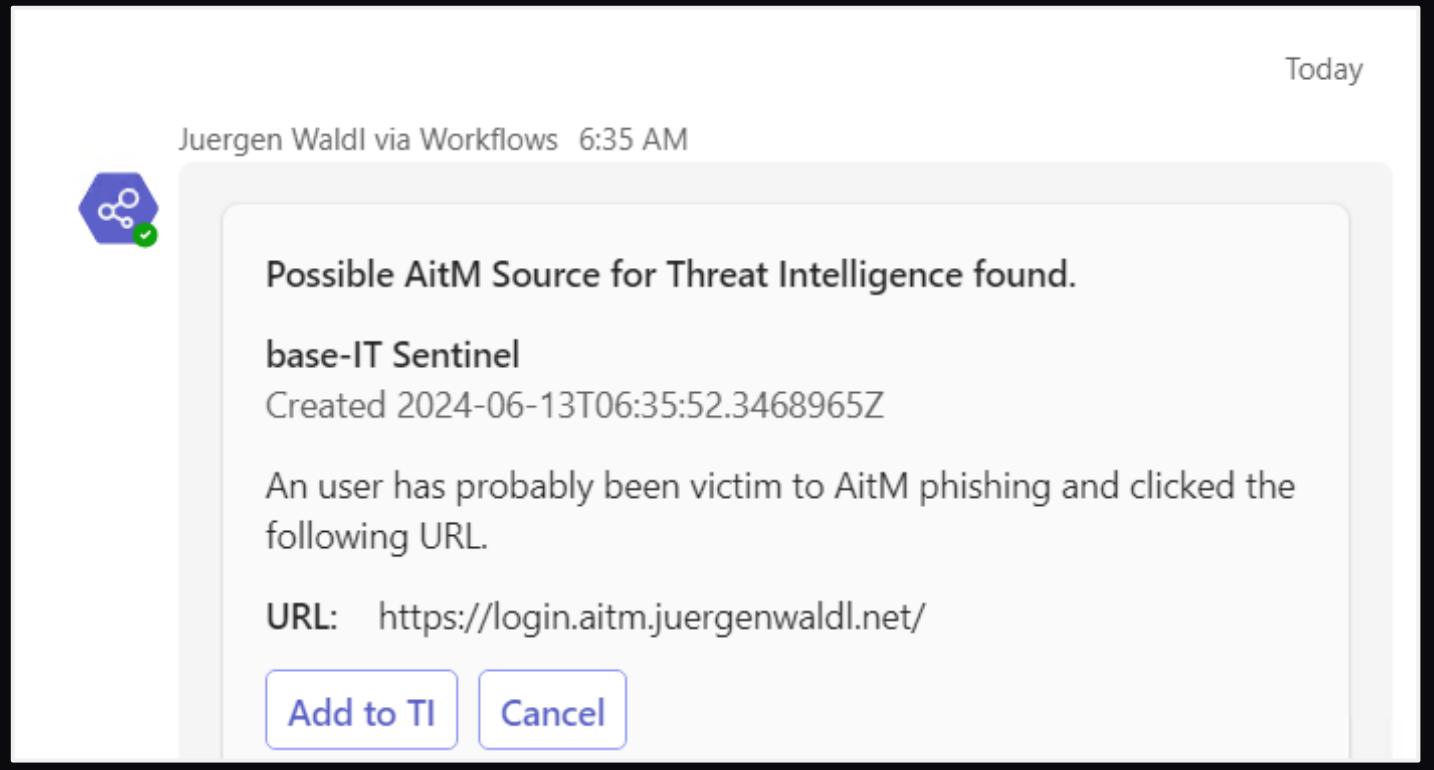
- jeder Aufruf der Anmeldeseite triggert eine Workflow (Logic App / Function App)
- Auswertung der eingehenden Anfrage in der Logic App
- Alarm bei falschem Referrer & Background Image ändert sich



SIEM Alert


Connection to AitM URL on device detected
Incident number 232
Refresh
Delete incident
Logs
Tasks
Activity log
This is the new, improved incident page - Now generally available. You can use the toggle to switch back.
High
Severity
New
Status
Unassigned
Owner
Workspace name
law-walju-test
Description
--
Alert product names
Microsoft Sentinel
Evidence
1
Events
1
Alerts
0
Bookmarks
Overview
Entities
Incident timeline
Search
Add filter
Jun 13
08:35:21
Connection to AitM URL on device de...
Hi...
Detected by Microsoft Senti...
Tactics...
Entities
Search
Type : All
login.aitm.juergenwaldl.net
URL
intunecc-win11-.intune.cc
Host
juergen.waldl
Account

SOAR Response



Microsoft Custom CSS ist deprecated…

Datum	Was passiert
05.01.2026	Neue Tenants haben kein Custom CSS Feature
21.07.2026	Ältere Tenants ohne bestehende Nutzung können es nicht mehr aktivieren
Ende Okt. 2026	Globales Retirement der Layout- und CSS Positioning-Properties
2027	Vollständiges Retirement von Custom CSS

MC1458474 · Microsoft Learn

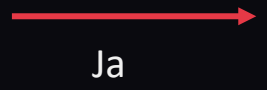
Evilginx - Filters

PHISHLET / YAML

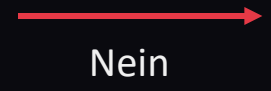
```
sub_filters:
  - {triggers_on: "login.microsoftonline.com",
     orig_sub: "login", domain: "microsoftonline.com",
     search: "ext-sign-in-box\\s*\\{[^}]*background-image[^}]*\\}",
     replace: "", mimes: ["text/html", "text/css"]}
```

How to reliably detect and block?

- Befinde ich mich auf einer Microsoft Entra Loginpage?



- Stimmt die URL mit den bekannten Microsoft SignIn Urls überein?



- Block SignIn

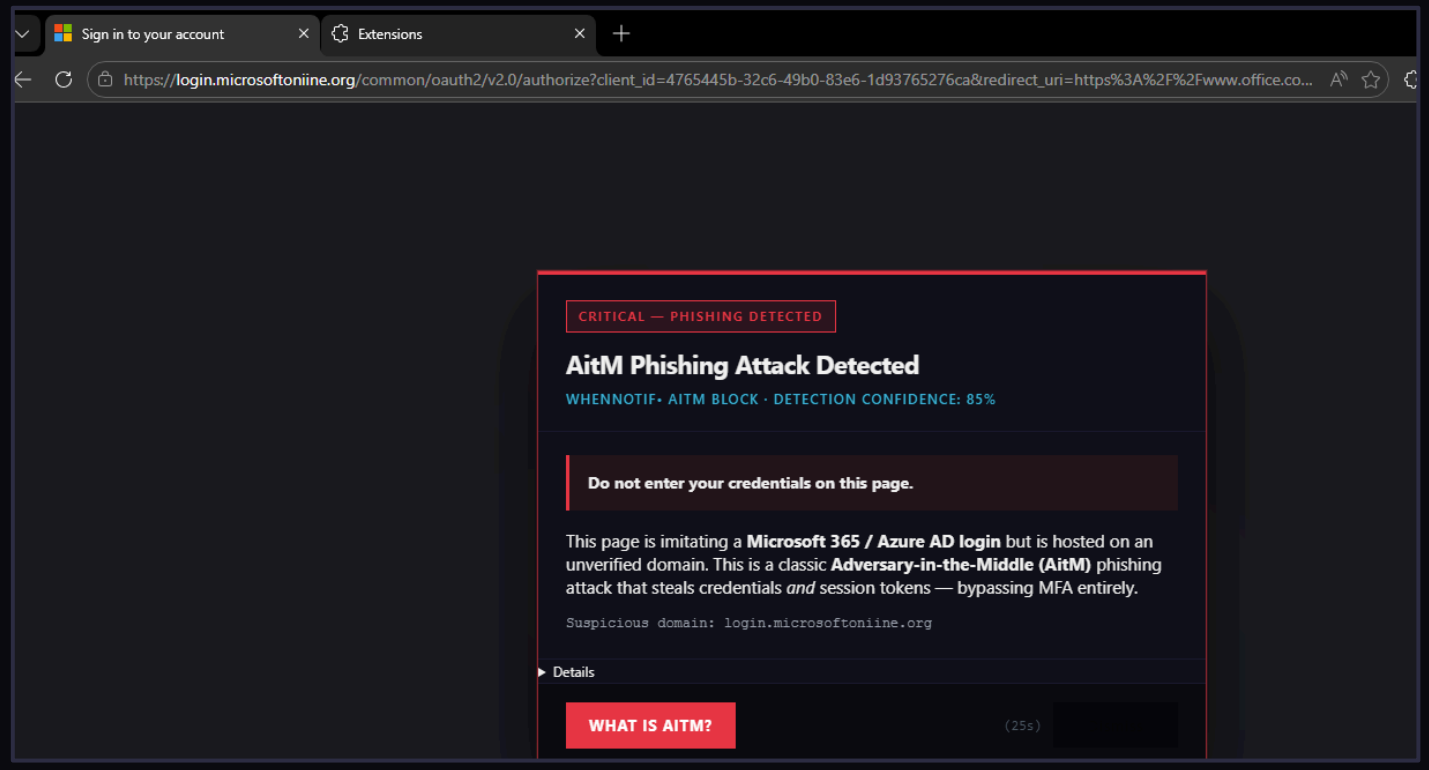
DOM Signal Detection & Scoring

Signal	Was wird geprüft?
Microsoft JS-Runtime	$Config / ServerData oder ≥3 Inline-Script-Marker
Tenant-Branding	TenantId, BannerLogo, UserIllustrationUrl im $Config
ConvergedSignIn PageID	meta name="PageID"
Microsoft CDN	Ressourcen von aadcdn.msftauth.net
… viele weitere	DOM-IDs, Body-Klassen, MS-Blau Farbcode,…

Detection im Browser

PhishGuard

- Lokal im Browser, keine Telemetrie, keine Cloud
- Community Edition frei auf GitHub, Pro Edition -> contact me!



PhishGuard Community Edition

> **Clientseitige Detection funktioniert, solange der Angreifer mit einem Reverse Proxy arbeitet.**

TAKEAWAY · AKT I

Drei Generationen - (k)eine Lösung?



✓ GEN 1 · Reverse Proxy

klassischer AitM Proxy.

AKT II

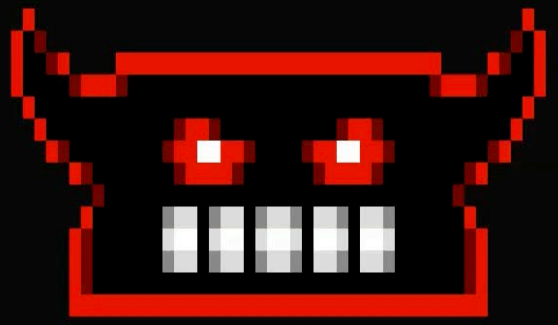
Defend

02

MFA Downgrade und die einzige Maßnahme, die uns serverseitig hilft…

GEN 2 · DEMO

MFA Downgrade, live



```
                 __ __                  __
 _______ _|__|  |    ____ |__| ____ ___  ___ ____________ ____
 _/ __ \\  \/ /  |  |   / ___\|  |/    \\  \/  / \____ \_  __ \/ _ \
 \  ___/\   /|  |  |__/ /_/  >  |   |  \>    <  |  |_> >  | \(  <_> )
  \___  >\_/ |__|____/\___  /|__|___|  /__/\_ \ |   __/|__|  \____/
      \/                 /_____/     \/      \/ |__|
```

by Kuba Gretzky (@mrgretzky) version 4.2.0

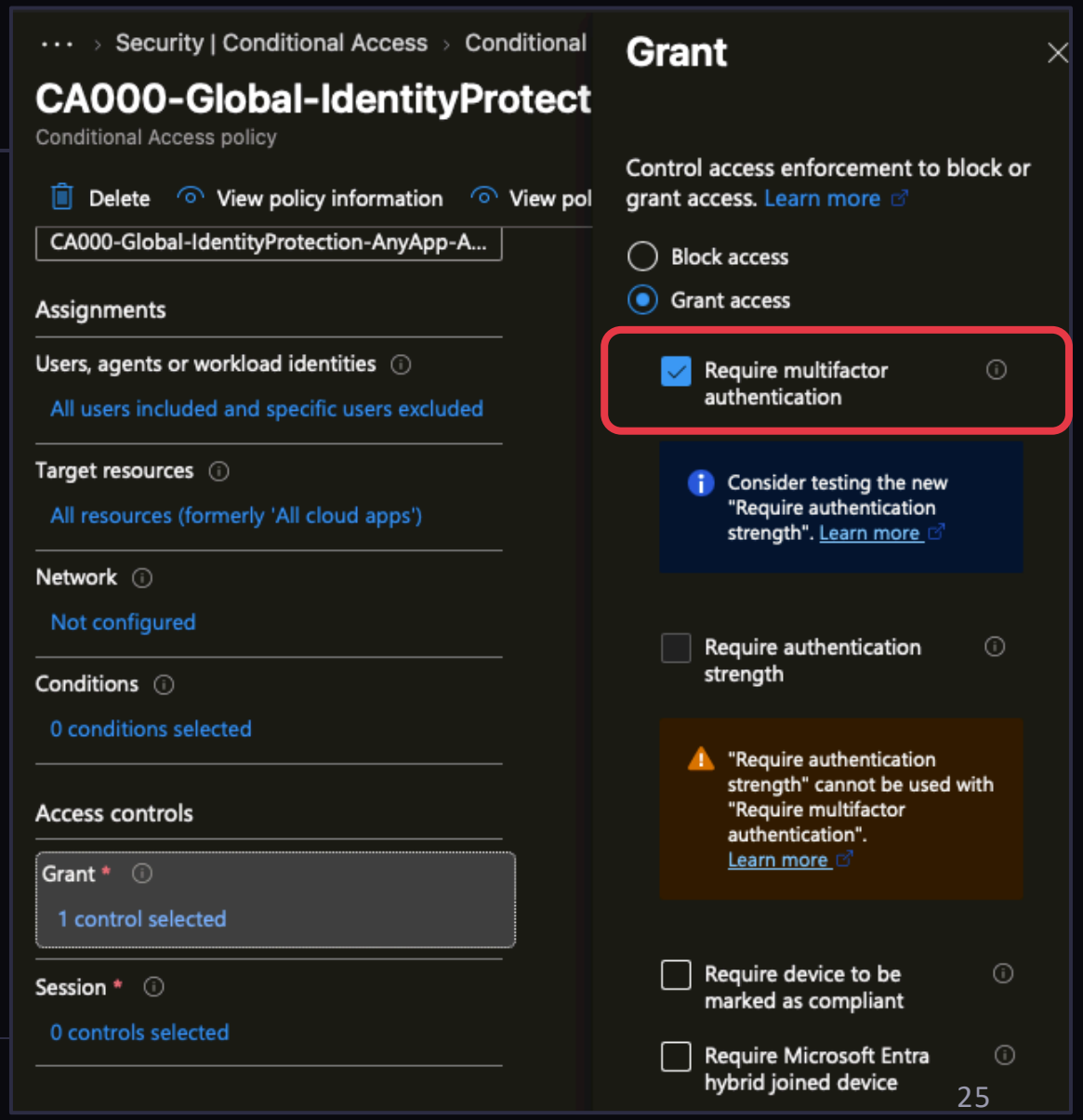
how much is the phish?

```
 > servers connect local
[11:37:43] [inf] connecting to server: local (127.0.0.1:443) [9c2afee3a5105f0b.evilginx]
[11:37:43] [inf] connected to server
[11:37:43] [inf] <kuba@breakdev.org> user connected
 local >
```

Misconfiguration…

WAS PRÜFT CA?

- Wurde _irgendeine_ Form von MFA abgeschlossen?
- Ja
- Token / Session Cookie wird ausgestellt

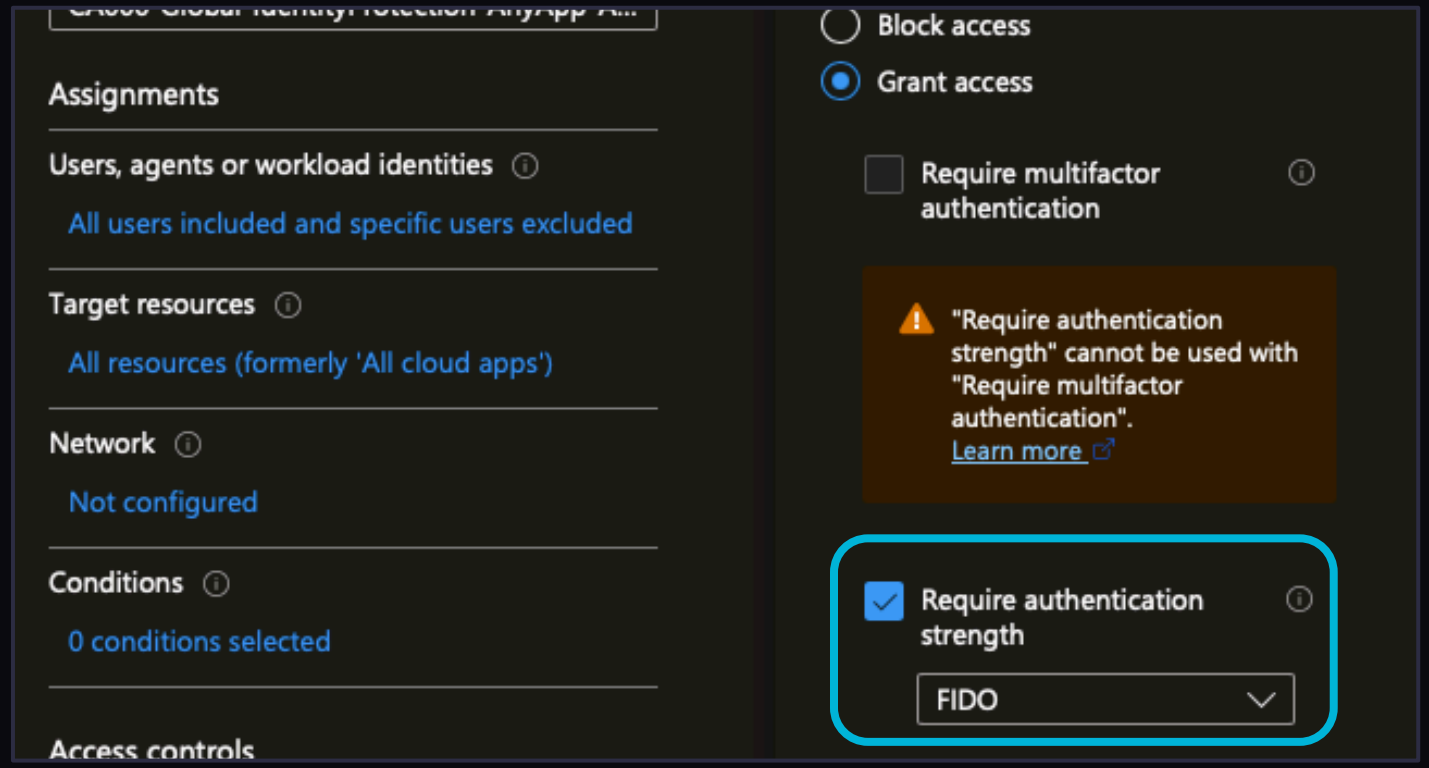


Entra – Conditional Access

Nicht ob MFA. Welche MFA.

Authentication Strength

- Grant-Control: “Authentication Strength“ forcieren
- Nur „sichere“ Methoden: FIDO2, Passkeys, WHfB, CBA



Grant-Control der CA-Policy: Authentication Strength

“Nicht „Require MFA“, sondern Authentication Strength!

TAKEAWAY · AKT II

Drei Generationen - (k)eine Lösung?



✓ GEN 1 · Reverse Proxy

klassischer AitM Proxy.



✓ GEN 2 · MFA Downgrade

AitM Proxy “with a twist“.

AKT III

Disrupt

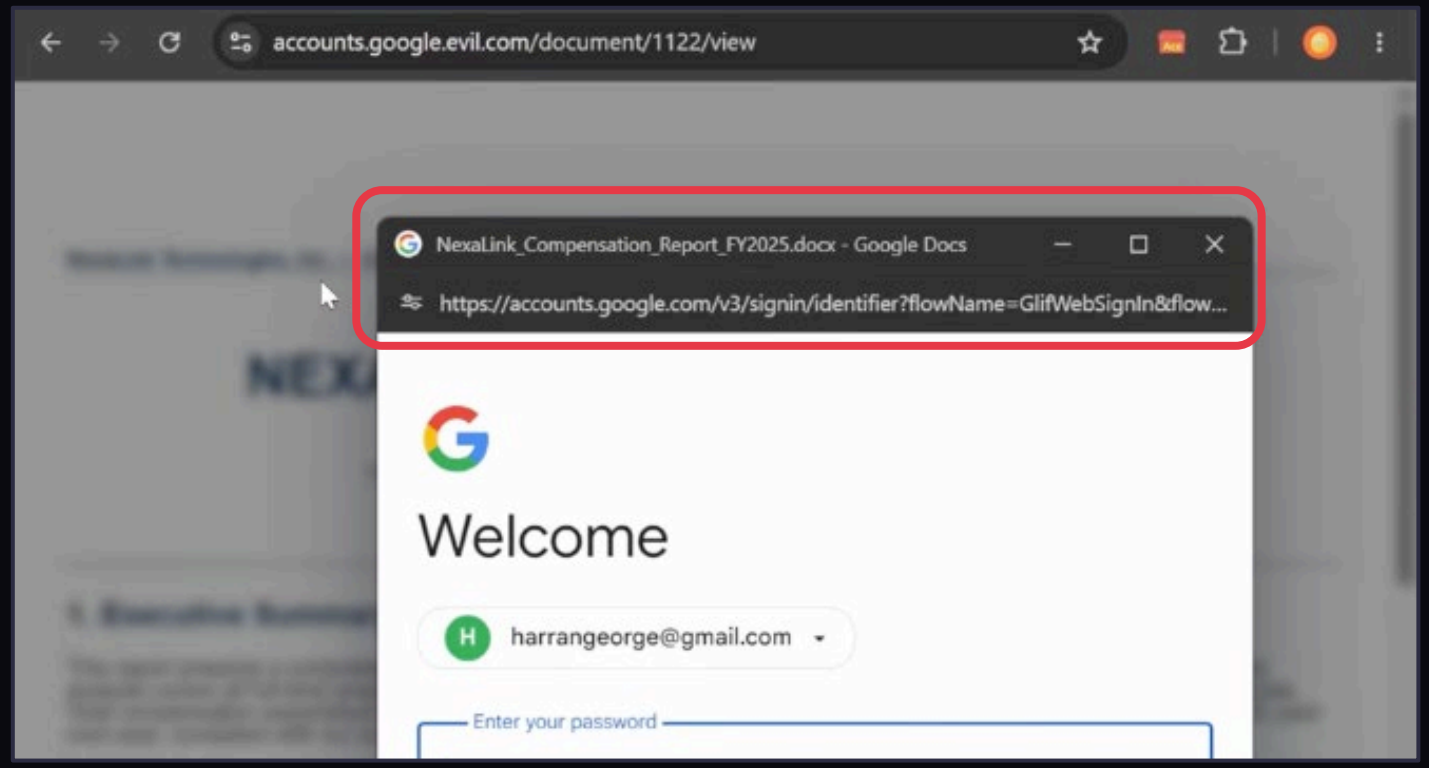
03

Credential Relay Phishing - wenn unsere Detection nicht mehr greift…

Back to the roots: kein Proxy mehr

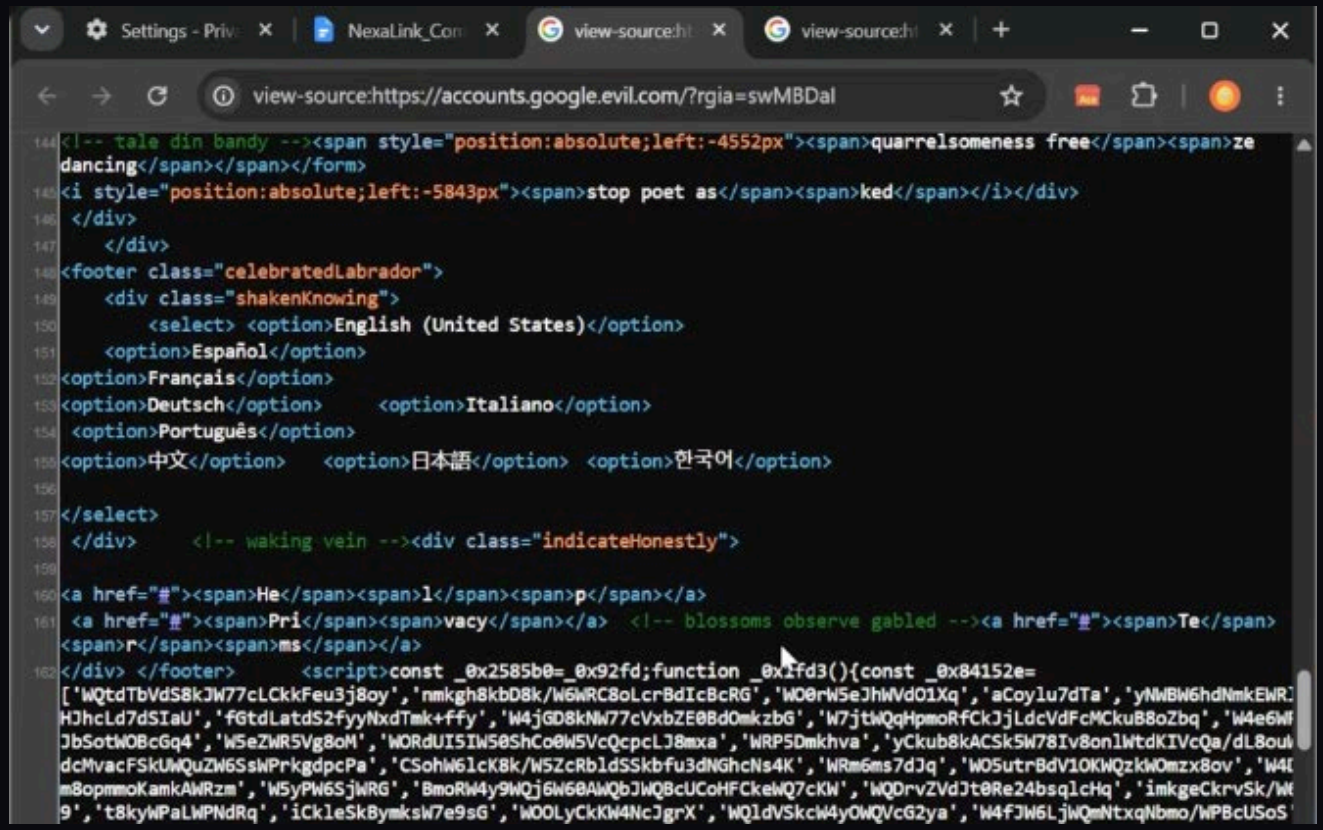
Browser-in-the-Browser

- Selbst gehostete, statische Fälschung
- Fake-Titelleiste und Fake-URL: reines HTML/JS
- Nativ in Evilginx Pro 5.0



aus „Credential Relay Phishing“, Kuba Gretzky (YouTube)

Und hier scheitert jede „browser-based“ Detection



Obfuskation: randomisierte Namen, zerstückelter Text,…

> **Wir spielen solange Katz- und Maus bis phishing-resistant MFA zur Pflicht wird…**

TAKEAWAY · AKT III

Drei Generationen - (k)eine Lösung?



✓ GEN 1 · Reverse Proxy

Der Angreifer leitet die echte Seite durch und schneidet den Token mit.



✓ GEN 2 · MFA Downgrade

Der Angreifer blendet die starken Methoden aus, bevor der User wählt.



✓ GEN 3 · Credential Relay

Der Angreifer braucht die echte Seite gar nicht mehr.

AKT IV (?)

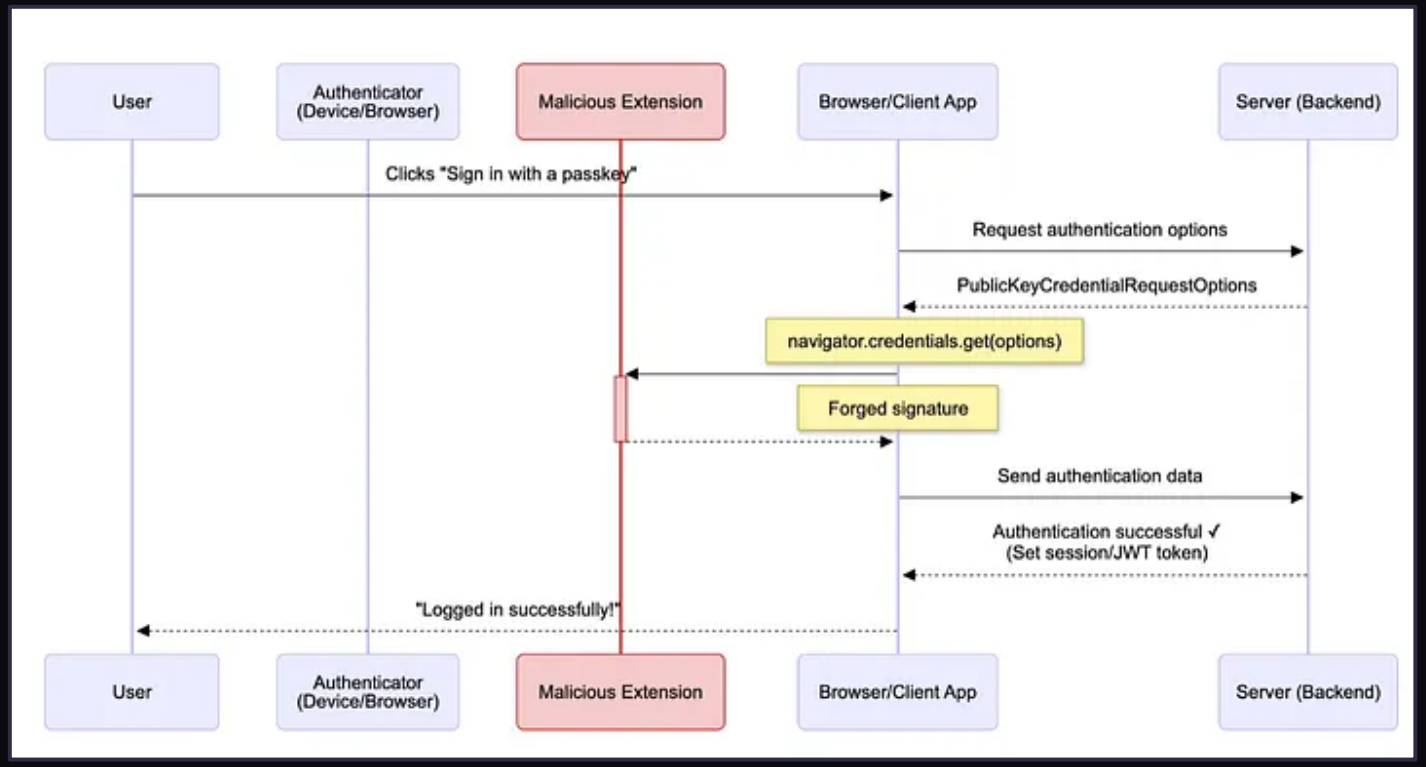
A glimpse into future

04

The ”new kid” on the block?

Passkey Registration Phishing

- Was wenn bereits die Registrierung des Passkeys gephisht wurde?



* https://labs.sqrx.com/passkeys-pwned-0dbddb7ade1a

Call to action - Prevention



1 · Conditional Access

auf „Authentication Strength“ konfigurieren



2 · Authentication Methods

Phishbare Methoden (TOTP, SMS/Phone Call, etc.) abschalten, nicht nur Auth Strength erzwingen.



3 · Registrierung

dieselbe MFA Stärke auch für die Registrierung von MFA Methoden verlangen



4 · Response

„Session Revoke“-Funktion nutzen anstatt „Passwort zurücksetzen“.

Und bei der Detection?

DETECT

- SIEM Use Cases:
  - Sign-in-Logs auf “weak“ Methods bei Accounts mit „phishing-resistent MFA“-Pflicht prüfen
  - Untypische SignIn Properties (Location, User Agent, etc.)

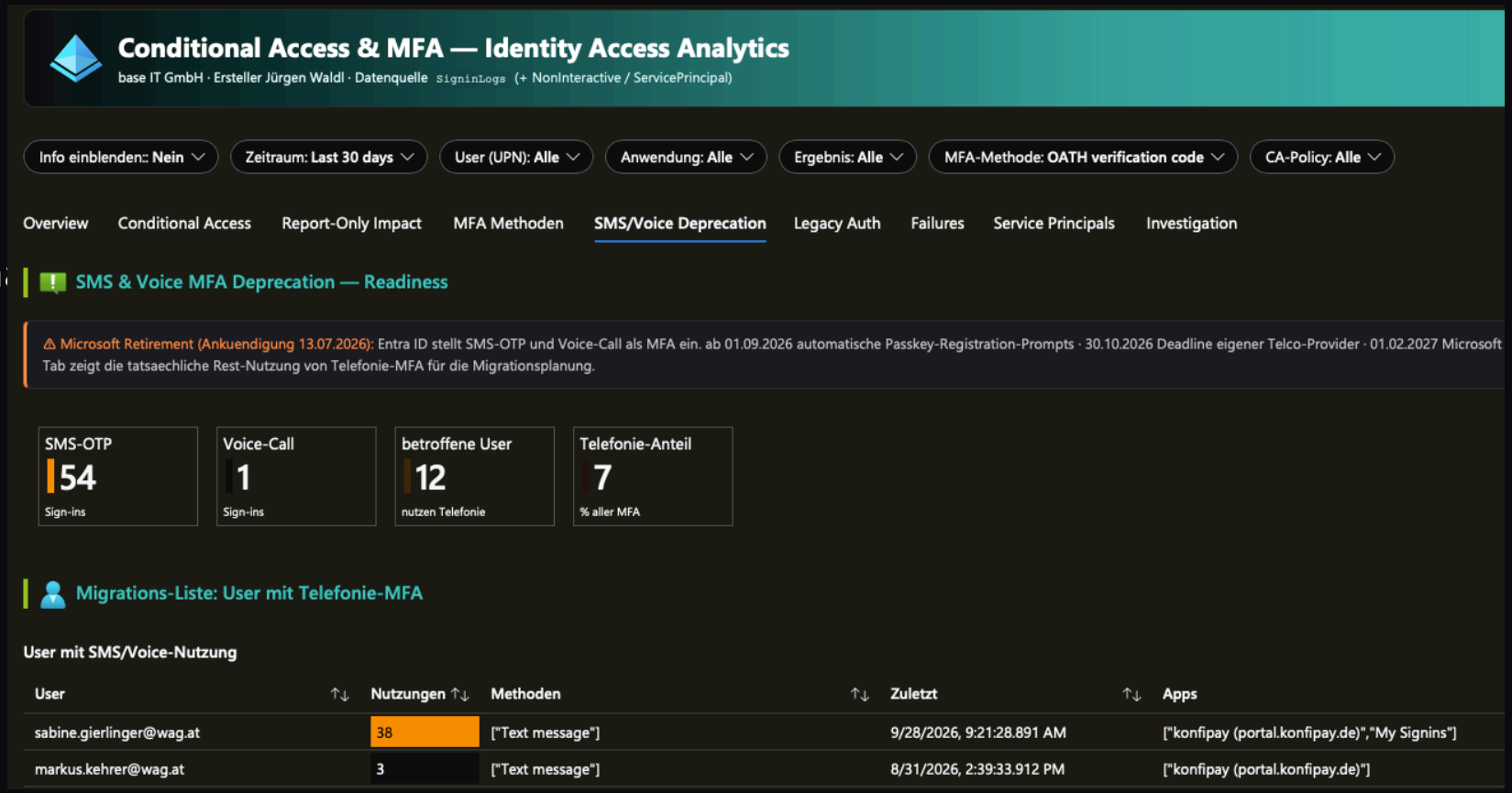
FRÜHWARNUNG

- PhishGuard als zusätzliche Schicht im Browser
- Ein User-Report-Kanal, der tatsächlich gelesen wird

Und bei der Detection?

DETECT

- Workbooks zur visuellen Anom
  Analyse



Und bei der Detection?

DETECT

- SIEM Use Cases:
  - Sign-in-Logs auf “weak“ Methods bei Accounts mit „phishing-resistent MFA“-Pflicht prüfen
  - Untypische SignIn Properties (Location, User Agent, etc.)
- Workbooks zur visuellen Anomalieerkennung & Analyse

FRÜHWARNUNG

- PhishGuard als zusätzliche Schicht im Browser
- Ein User-Report-Kanal, der tatsächlich gelesen wird

whennotif

The end of this talk.

Phishing to be continued…

Jürgen Waldl · base-IT GmbH

whennotif.io

- PhishGuard Community Edition:
  github.com/waljue/phishguard-community