KPMG

MFAngler – automated M365 phishing framework

IT-SECX 2025

—

03.10.2025

KPMG

Agenda

01 Teach a man to phish…

02 MFA Enters the Chat

03 Introducing MFAngler

04 Demos: Initial Access & Automated Persistence

05 Field test

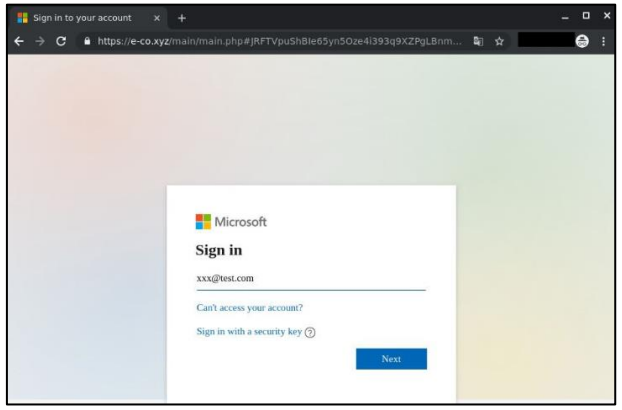
06 Limitations & Conclusion

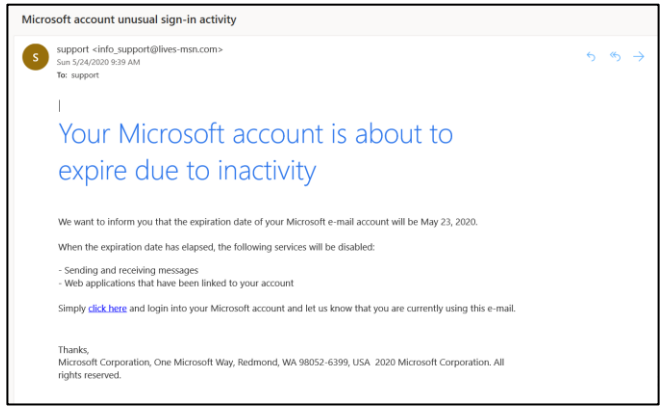
Teach a man to Phish …

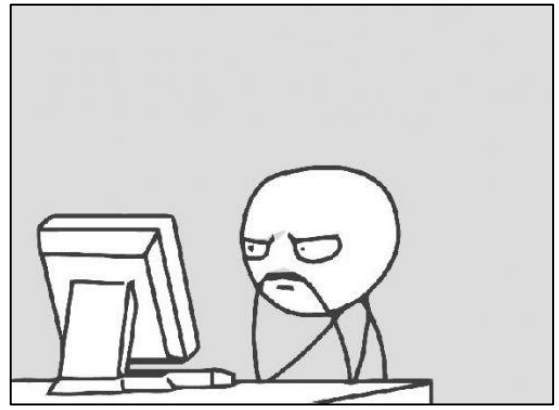
1: Copy Target Site

2: Send out Phishing Mails

3: Wait…







Teach a man to Phish …

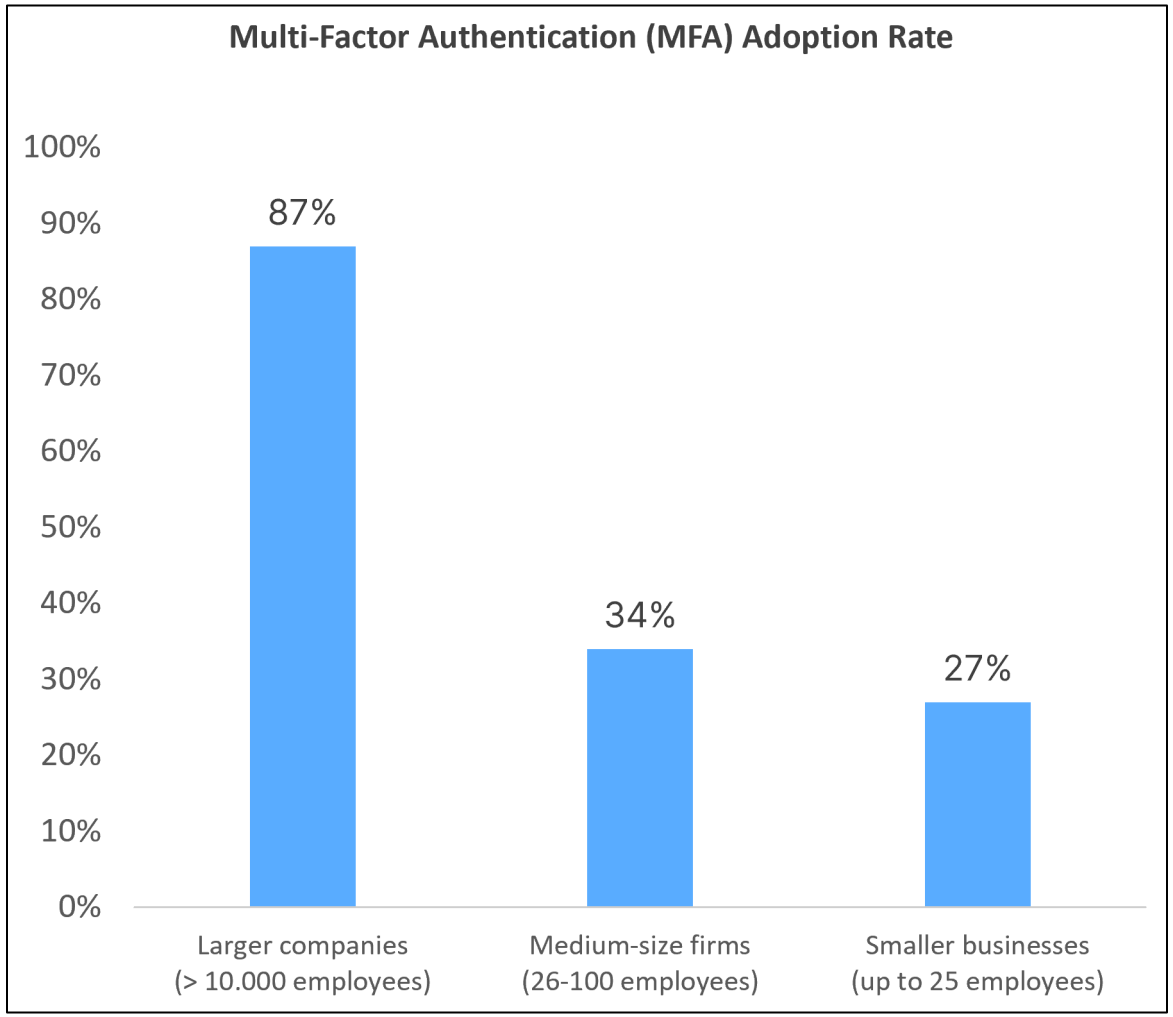
We use phishing in a number of assessments, mainly

- dedicated Social Engineering assessments
- Initial Access Assessments
- Red Team Projects

Teach a man to Phish …

We run into certain problems with that approach in more recent time …

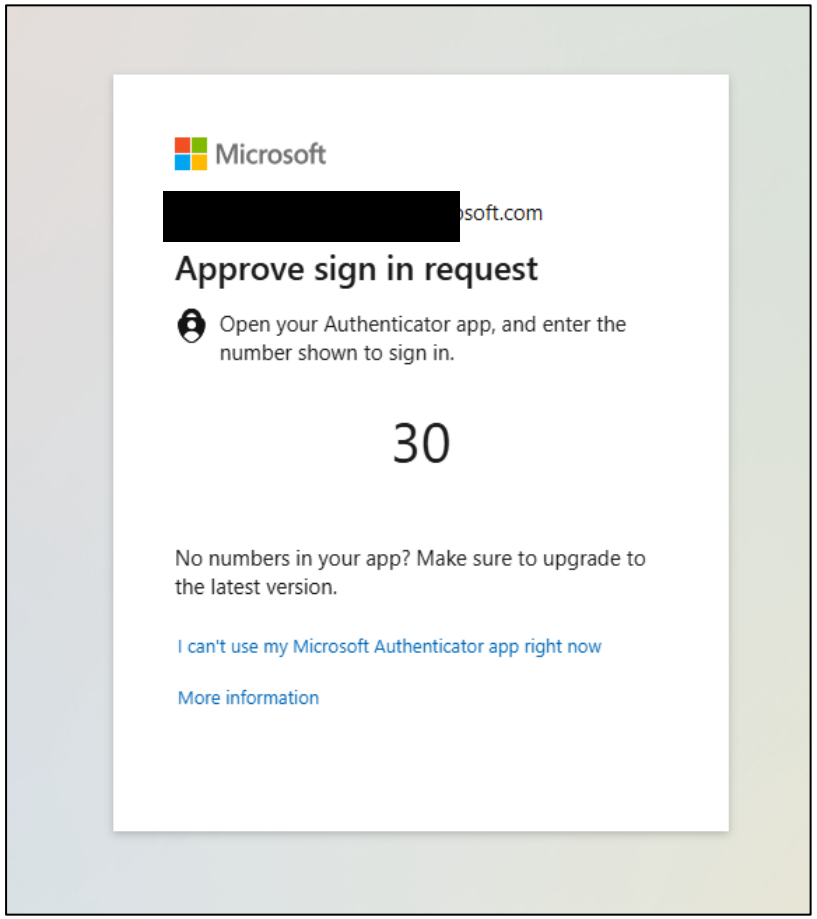
MFA Enters the Chat



Source: https://jumpcloud.com/blog/multi-factor-authentication-statistics

MFA Enters the Chat

- Username and Password alone not sufficient anymore
- More interaction by the user needed
- Additional persistence techniques required
- Simple phishing-templates don‘t work anymore



...and immediately overdoes it

- **SMS/Call**
- **TOTP**
- **Azure MFA (proprietary)**
- ***Passkey****
- Other third party (DUO/PingID)
- Hardware Second Factor

What did that mean for us?

We needed a solution for assessments that

- Can handle MFA during phishing campaigns
- Does not (immediatelly) trigger defense mechanisms
- Can handle a large number of logins at the same time/in short time
- Is (somewhat) autonomous
- Can be reused
- Allows us to keep logging in (Persistence)
- … has a cool (AI generated) name

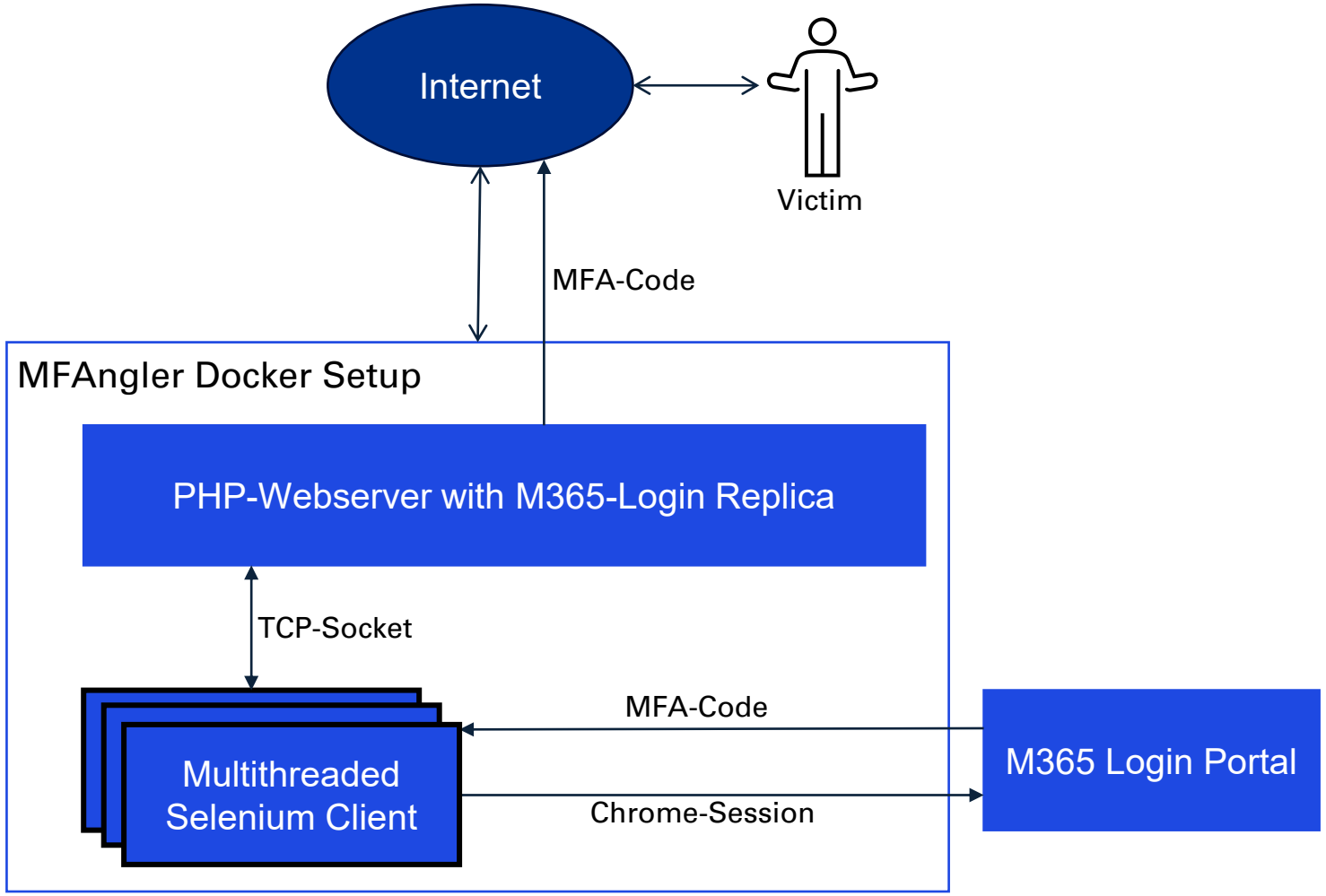
Introducing MFAngler

MFA Phishing-Toolkit for Microsoft Azure Login Workflow

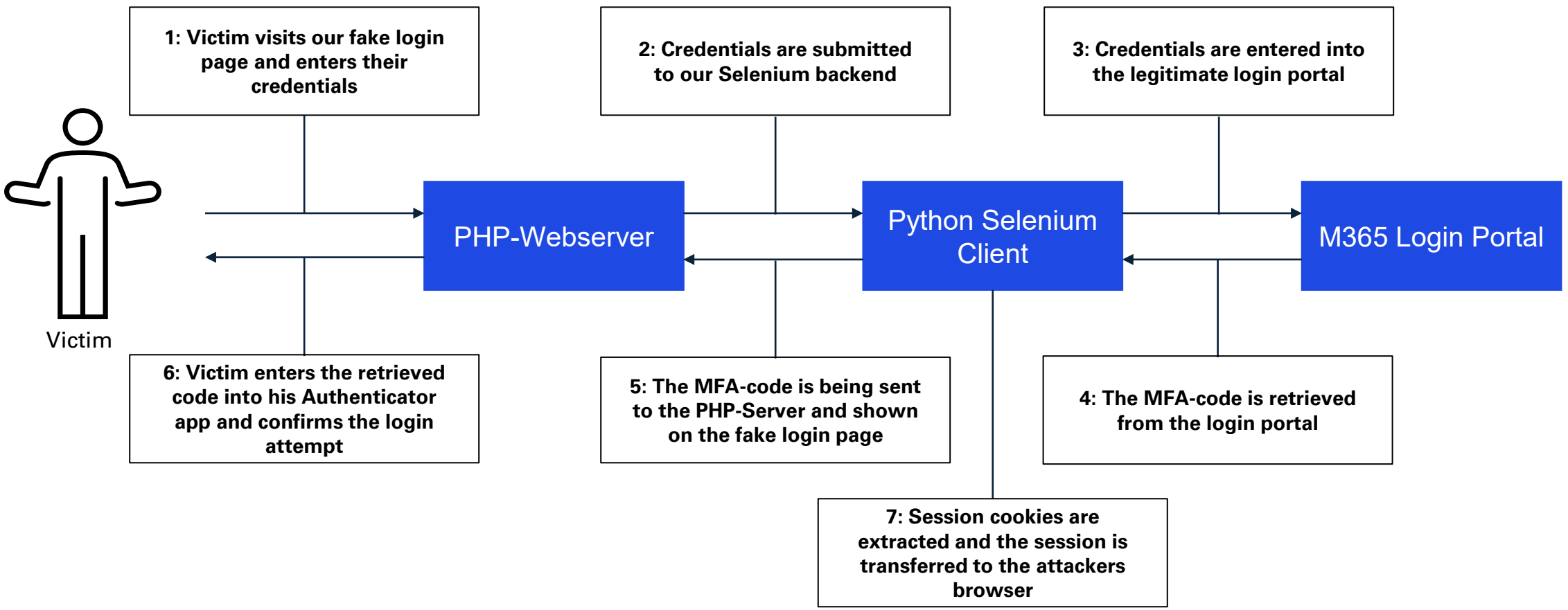
Features:

- Multi-Threaded browser emulation through Selenium
- Automated setup parameterized to customize behaviour and design
- Multiple MFA options for login
- Dockerized

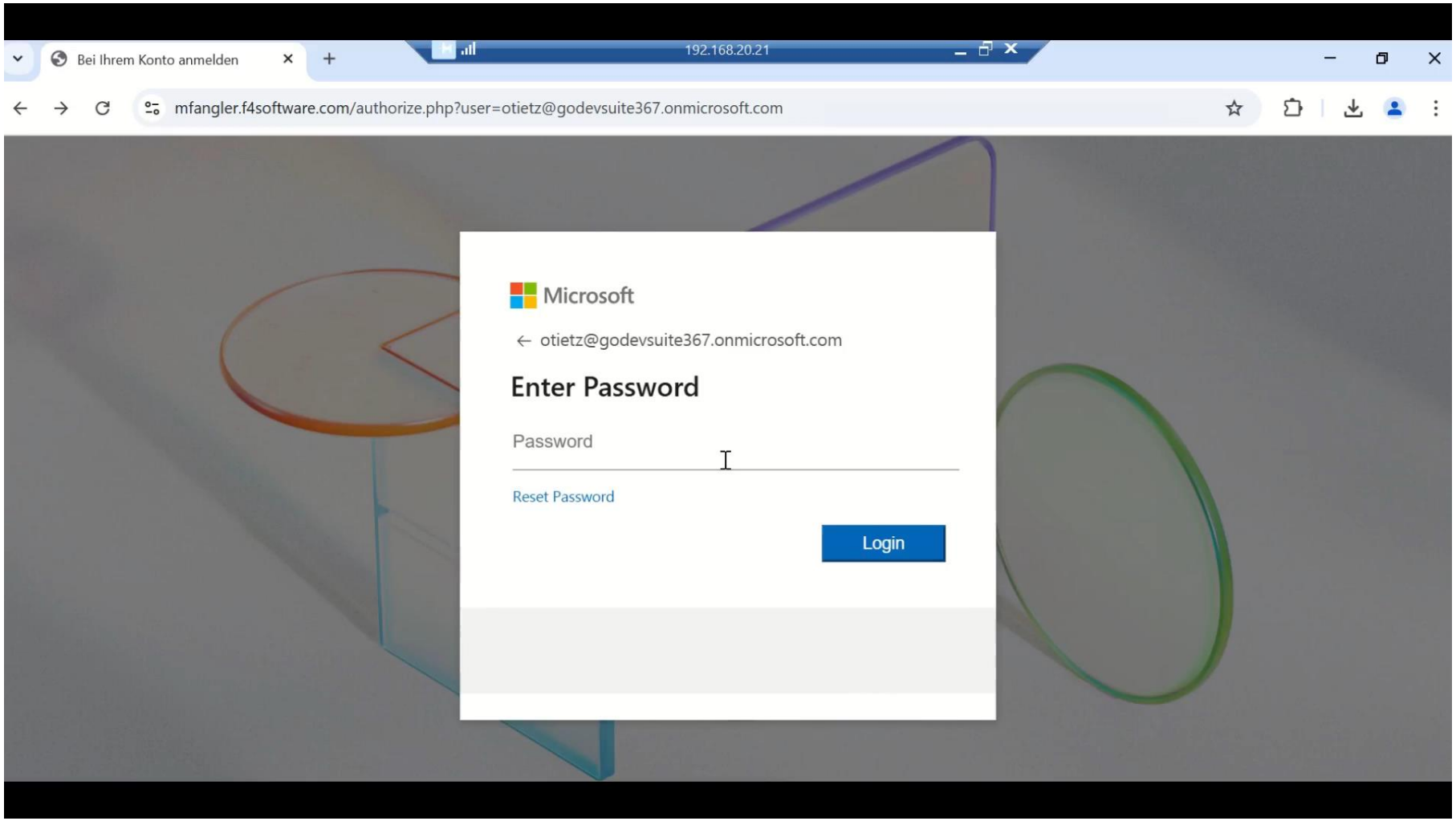
MFAngler Architecture



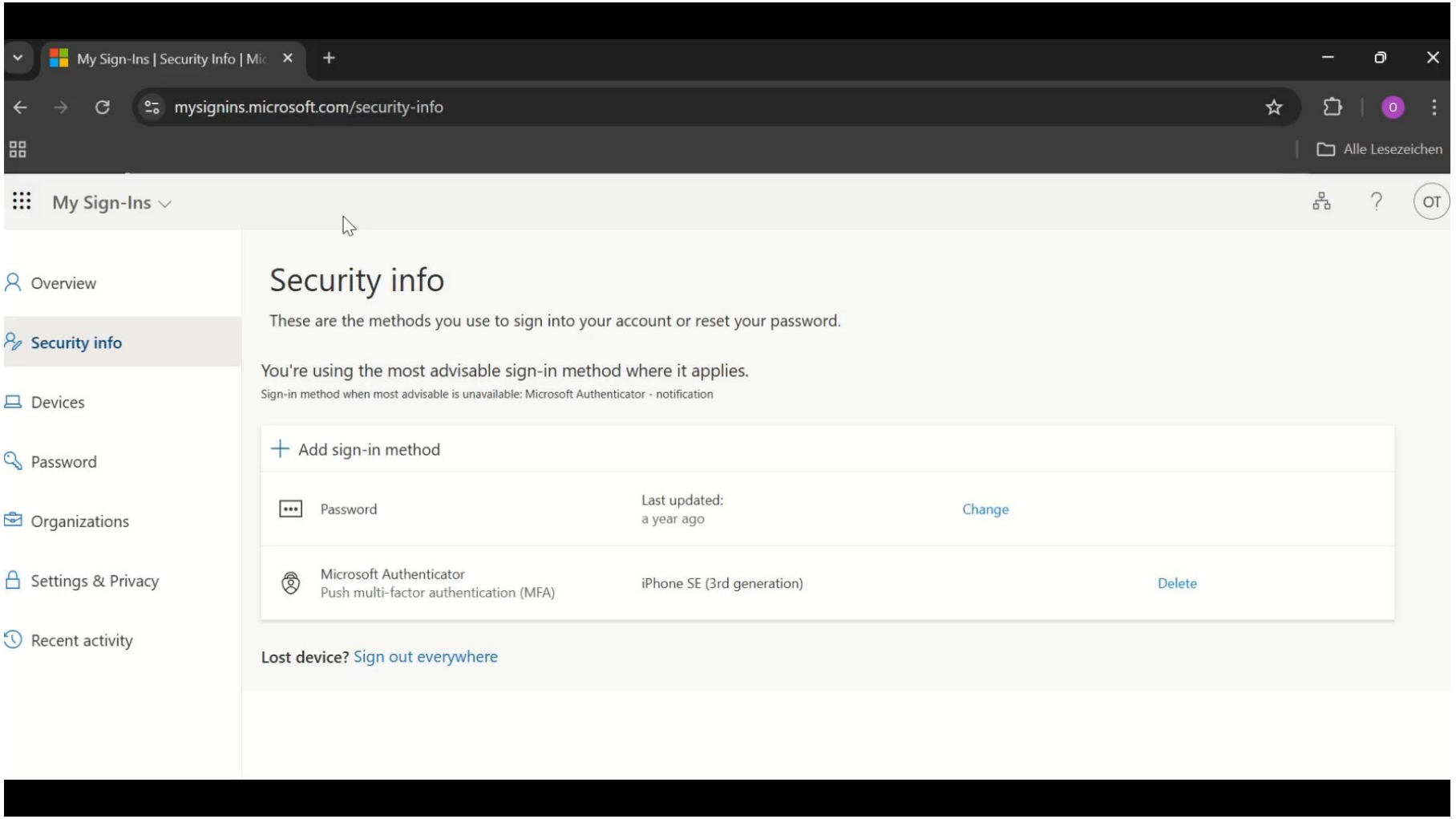
Initial Access



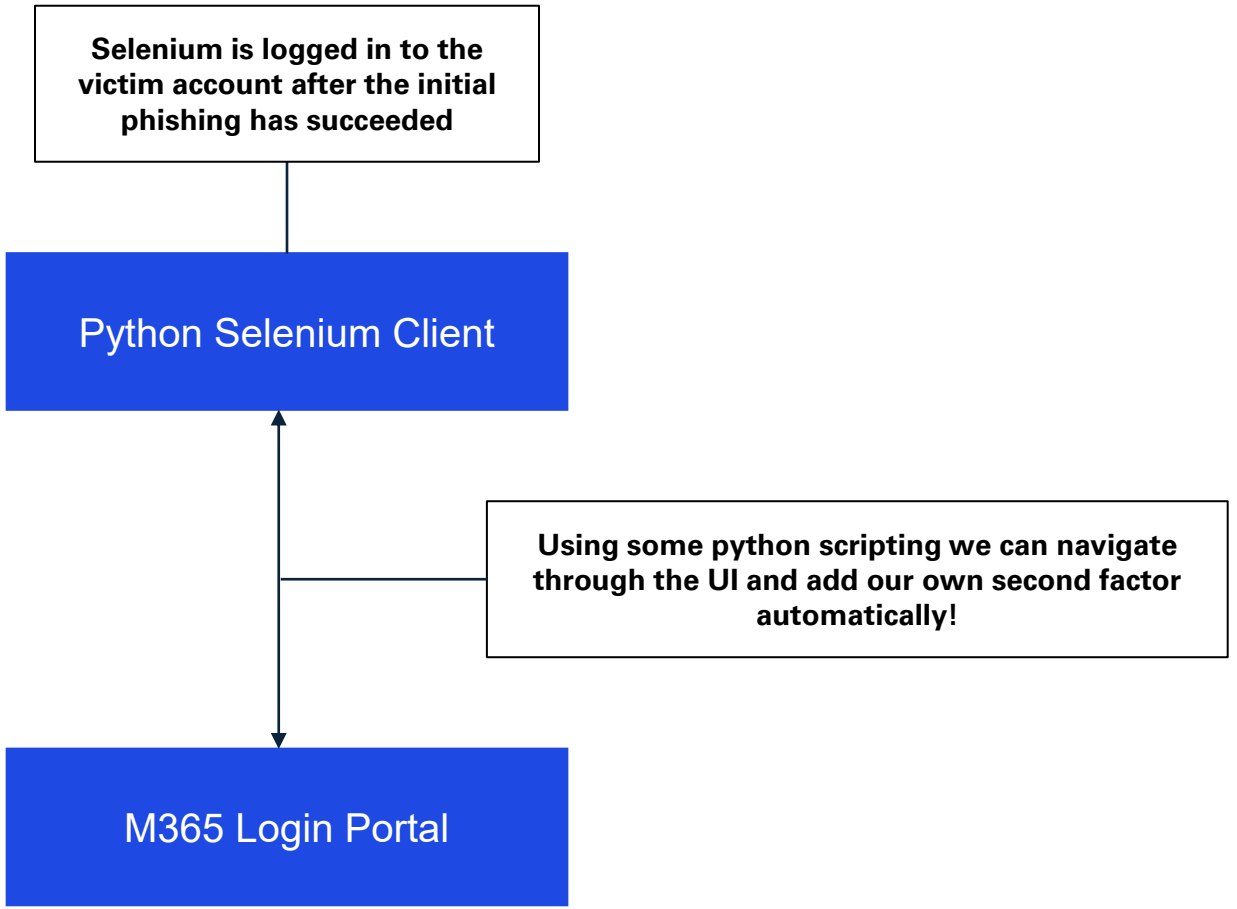
DEMO: Using MFAngler to gain access to an M365 Portal



But wait, there is more...



But wait, there is more...



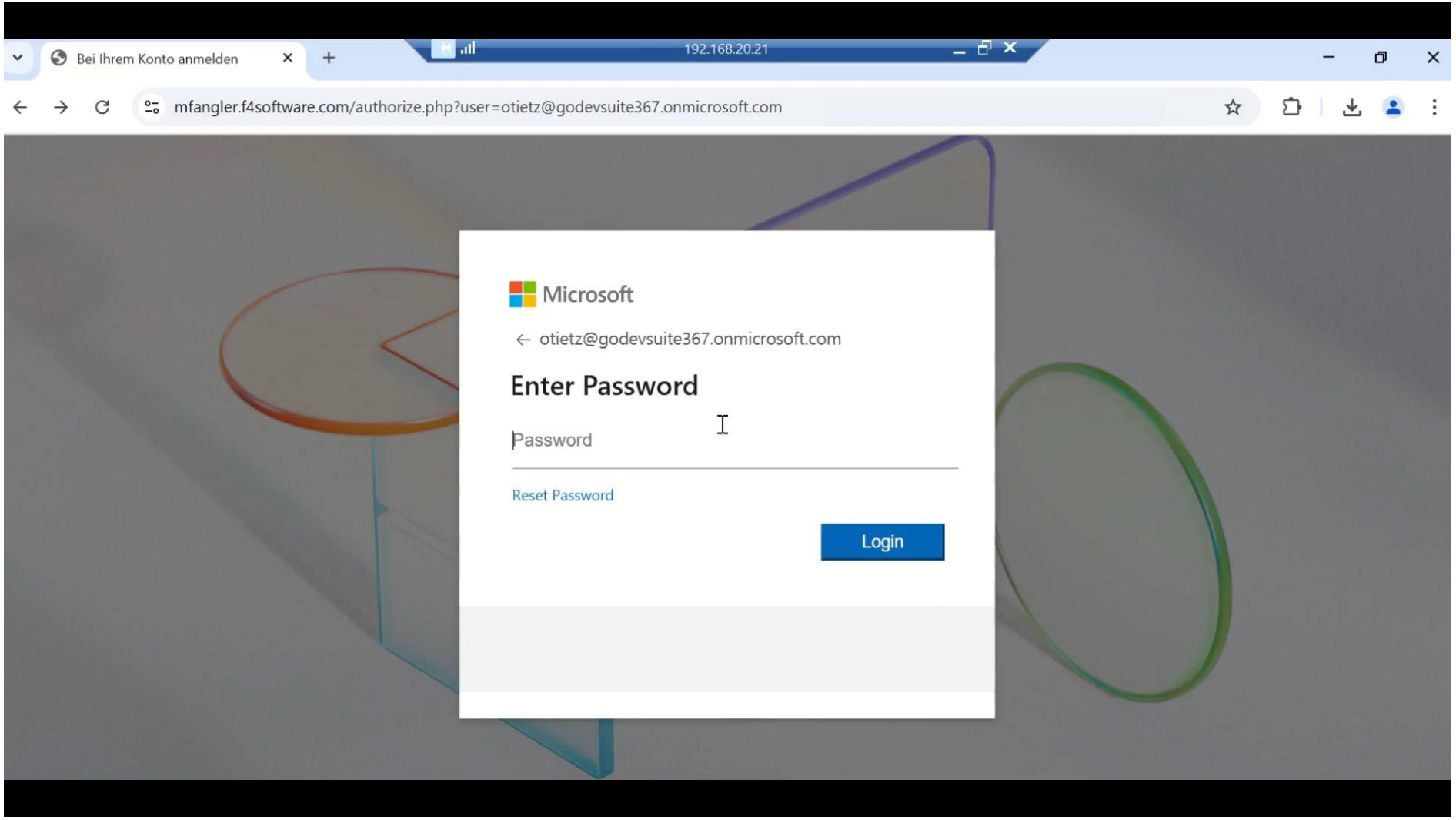
Introducing MFAngler

MFA Phishing-Toolkit for Microsoft Azure Login Workflow

Features:

- Multi-Threaded browser emulation through Selenium
- Automated setup parameterized to customize behaviour and design
- Multiple MFA options for login **and for persistence**
- Dockerized
- **Persistence through adding MFA to account**

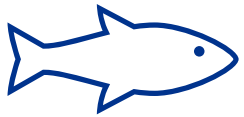
DEMO: Automated Persistence with MFAngler



Field test

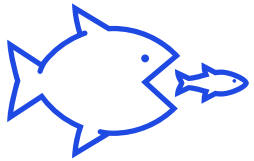
The timeline:

- 1 minute after sending, the first account was fully compromised
- 15 minutes later we saw reaction: E-Mails withdrawn from inboxes, URL and IPs blocked



75%

of people who input passwords had additional MFA added



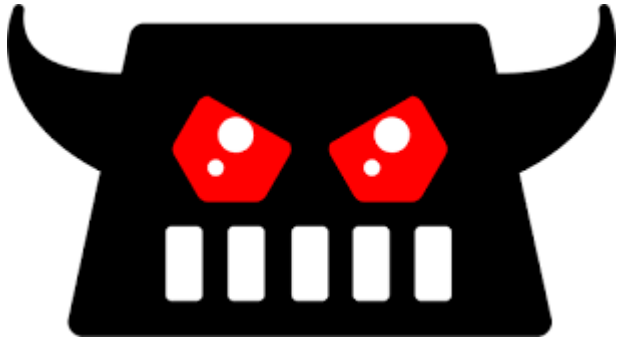
10%

changed password

0%

removed the added MFA

But wait...



Evilginx exists???

- a proxy between victim and legitimate login site
- taking requests and forwarding them directly to the login sites
- has it‘s own problems with detections (i.e. check window.location)

Comparison

- Proxy vs. Emulation
- Redirect vs. Cloning

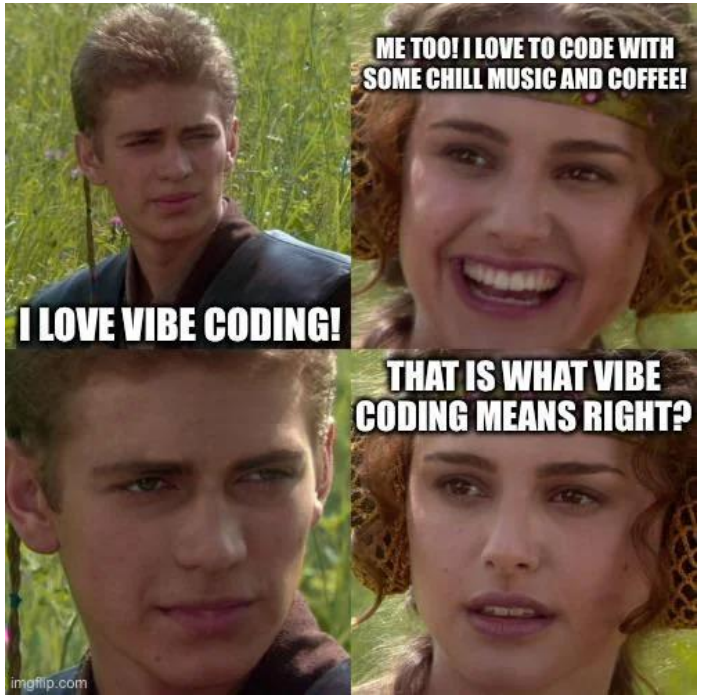
Source: https://evilginx.com/

Limitations

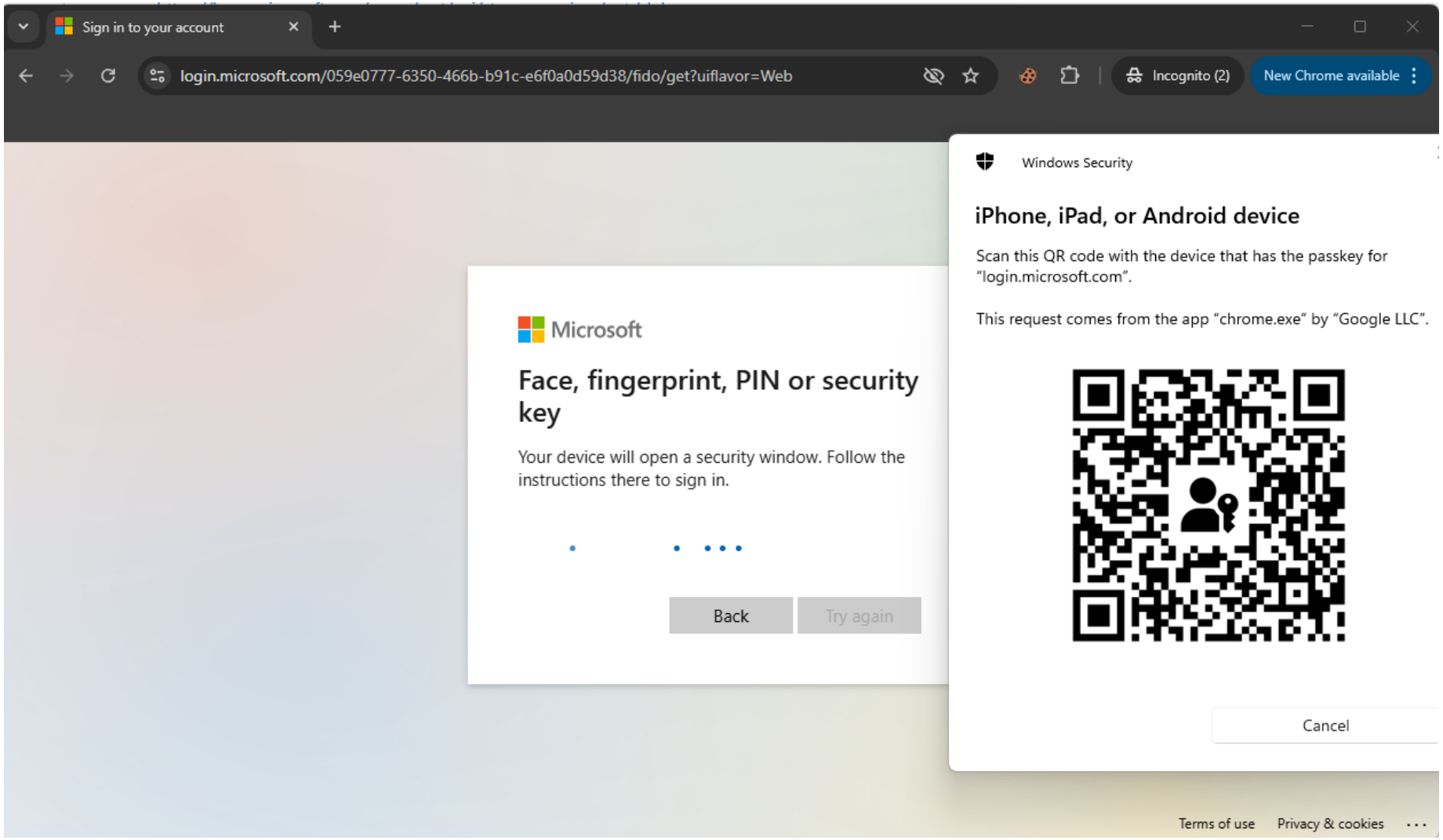
- ***Only for Microsoft Azure Login Portal***
- Only applicable for M365 native login workflow (non federated)
- Updates in the UI flow by Microsoft -> Manual adjustment needed
- Device-based Conditional Access
- Hardware Tokens

Future Development

- Include Passkey Authentication
- Decouple emulation code and phishing frontend further
- Refactor emulation code **#vibecoding**



Future Development - Passkeys

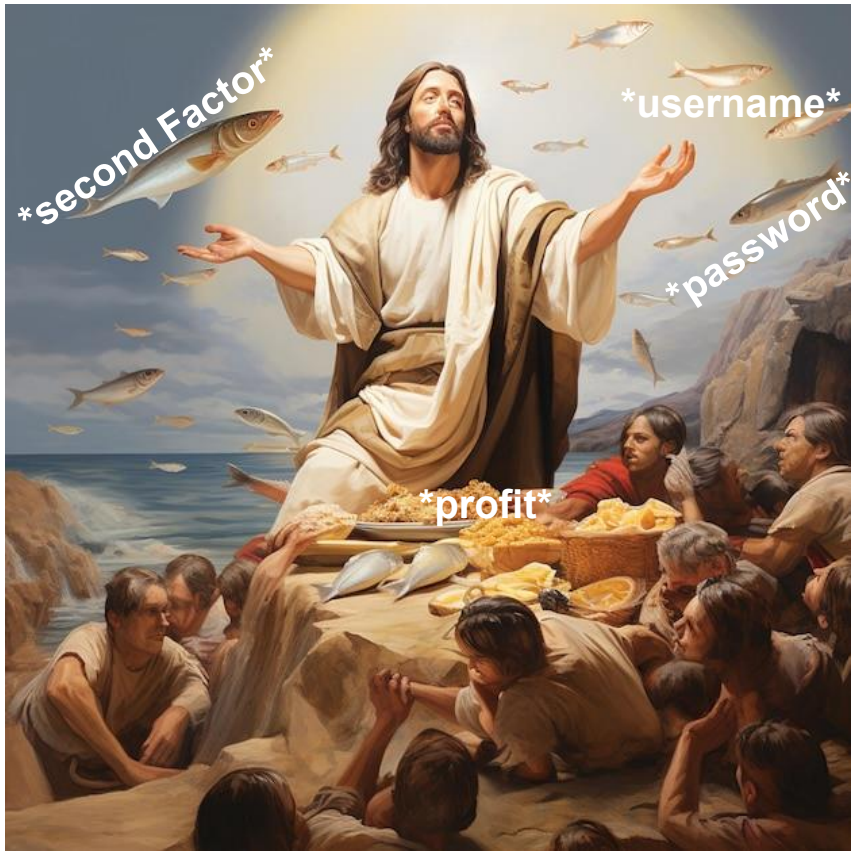


Conclusion

- Used MFAngler successfully in multiple engagements since last year
- Worked with several different Microsoft tenants across multiple countries within the KPMG network
- No additional detection evasion needed

- Not every “phishing resistant MFA” is safe from every form of phishing attack
- Phishing is dead, long live phishing!

Teach a man to *MFA* Phish ...



kpmg.at

MS Authentication Types

Authentication method combination	MFA strength	Passwordless MFA strength	Phishing-resistant MFA strength
FIDO2 security key	✅	✅	✅
Windows Hello for Business	✅	✅	✅
Certificate-based authentication (Multi-Factor)	✅	✅	✅
Microsoft Authenticator (Phone Sign-in)	✅	✅	
Temporary Access Pass (One-time use AND Multi-use)	✅		
Password + something you have[1]	✅		
Federated single-factor + something you have[1]	✅		
Federated Multi-Factor	✅		
Certificate-based authentication (single-factor)			
SMS sign-in			
Password			
Federated single-factor			

Source: https://learn.microsoft.com/en-us/entra/identity/authentication/concept-authentication-strengths?source=recommendations

Password Manager Passkey Support

Password Manager Landscape: Passkey Support							
Password Manager	Windows	macOS	Linux (out of scope)	iOS	iPadOS	Android	Browser Extensions
1Password	✓	✓ Mac >=14	✗	✓ >=17		✓ >=14	✓
Bitwarden	✓	✓	✗	✓		✓	✓
DASHLANE	✓	✓ Mac >=14	✗	✓ >=17		✓ >=14	✓
Samsung Pass	✗	✗	✗	✗	✗	✓ >=7 (Samsung Devices)	✗ (Not Needed)
Google Password Manager	✓ (via chrome) requires TPM >= 129	✓ (via chrome) >= 129	✗ / ✓ (via chrome)	✓ (via chrome) >= 17 >= Chrome 132	✓ (via chrome) >= 17 >= Chrome 132	✓ (default on Android)	✗ (Chrome only unless used as Native Store)
NordPass	✓	✓	✗	✓ >=17		✓ >=14	✓
KEEPER	✓	✓	✗	✓ >=17		✓ >=14	✓
Enpass	✓	✓	✗	✓ >=17		✓ >=14	✓
Proton	✓ (Web)	✓ (Web)	✗	✓ >=17		✓ >=14	✓
KeePassXC	✓	✓	✗	✗ (3rd-Party Apps)	✗	✗ (3rd-Party Apps)	✗ Safari (3rd-Party)

https://www.corbado.com/blog/passkey-implementation-password-managers#3-the-password-manager-landscape-for-passkeys