PSCONF.EU

PowerShell Conference Europe

Next Up:

Miriam Wiesner

MALMÖ 25

3

2

1


Tabs
Tabs
Tabs
PSCONF.EU
2020
RAZER

PSCONF.EU

PowerShell Conference Europe

I’m in your browser, eating your cookies (…and bypassing your MFA)

Miriam Wiesner

MALMÖ 25

Many thanks to our sponsors:

Jane Street

KNOWLEDGE FACTORY

SynEdgy

@miriamwiesner.bsky.social

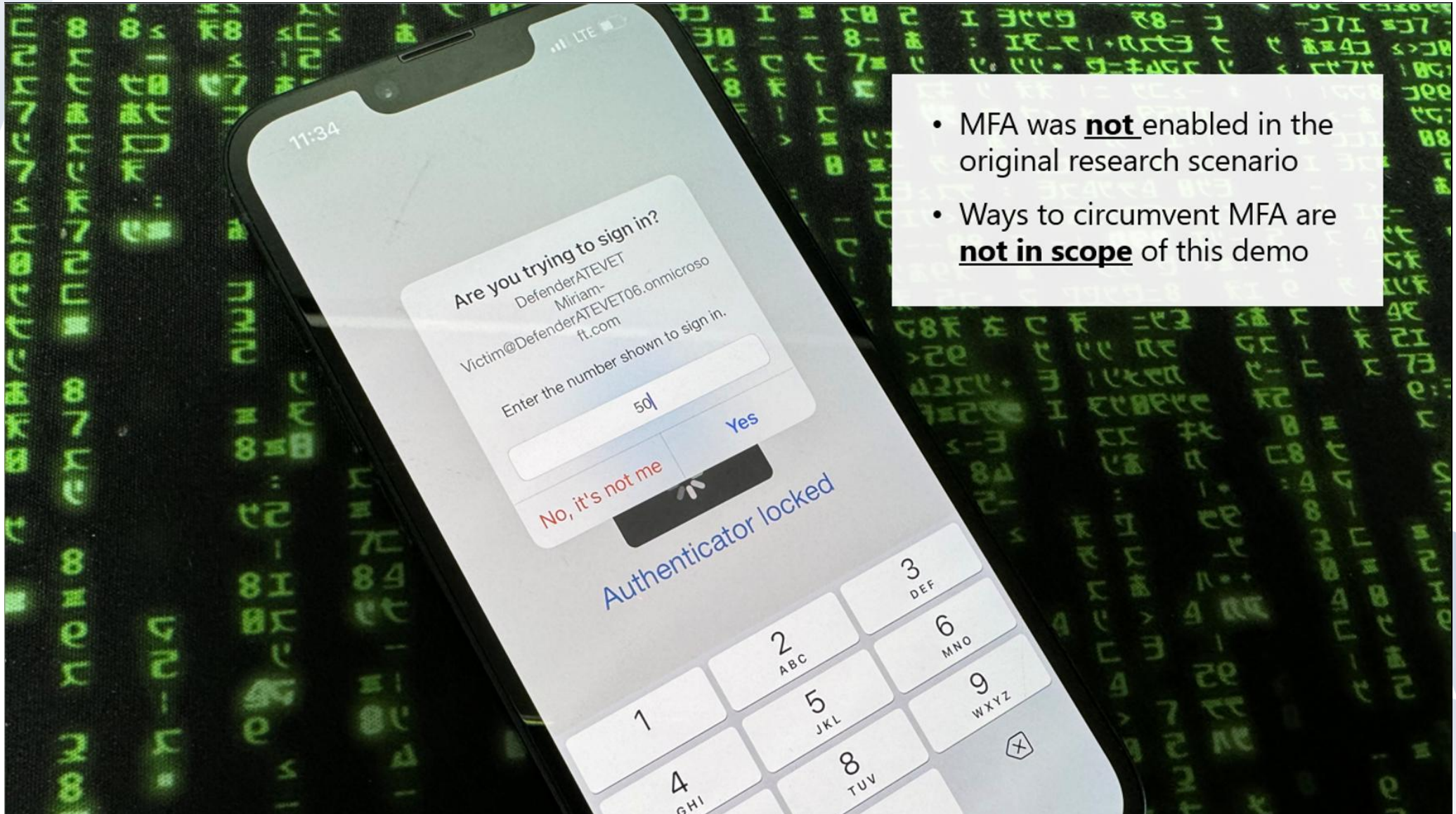
@miriamxyra

Miriam Wiesner

- Sr. Security Research Program Manager
  - Sentinel Research
  - https://github.com/miriamxyra
- Author of the book “PowerShell Automation and Scripting for Cybersecurity - Hacking and defense for red and blue teamers”
  - Amazon.com: https://aka.ms/mw-book
  - Packt: https://aka.ms/mw-book-packt

@miriamwiesner.bsky.social @miriamxyra

What happened before…



- MFA was **not** enabled in the original research scenario
- Ways to circumvent MFA are **not in scope** of this demo

Phishing

AitM

Social Engineering

XSS

How are attackers actually bypassing MFA?

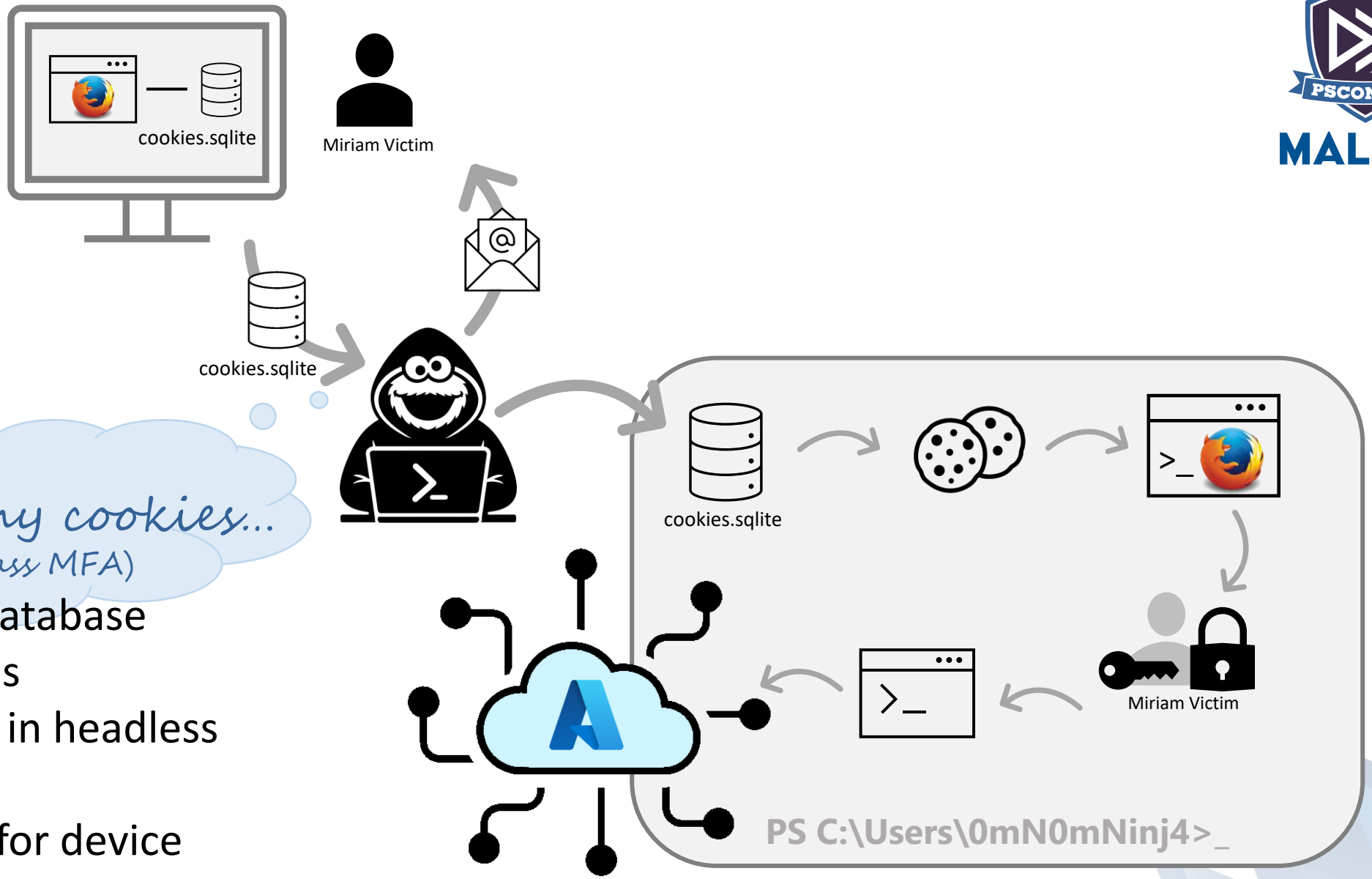
MFA Fatigue

Legacy Fallback Options

Cookie Replay

Session Hijacking

@miriamwiesner.bsky.social @miriamxyra



How to get my cookies...
(and bypass MFA)

- ✓ Steal cookie database
- ✓ Extract cookies
- ✓ Replay cookie in headless browser
- ✓ Reuse cookie for device authentication
- ✓ Profit

@miriamwiesner.bsky.social @miriamxyra

PSCONF.EU MALMÖ 25

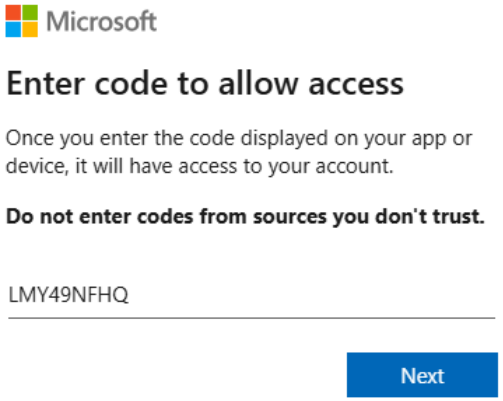
@miriamwiesner.bsky.social @miriamxyra

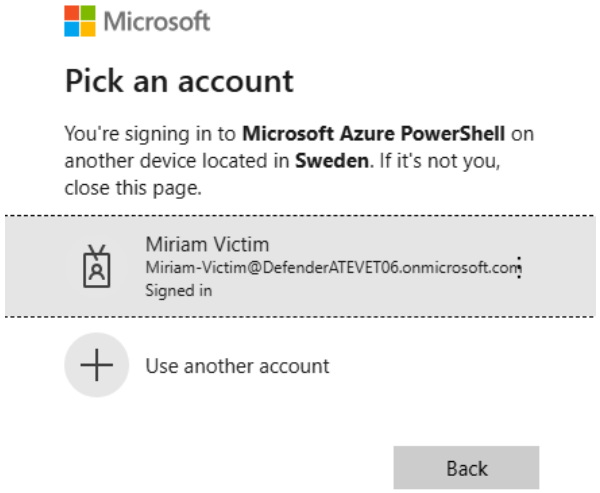
Access token and scopes

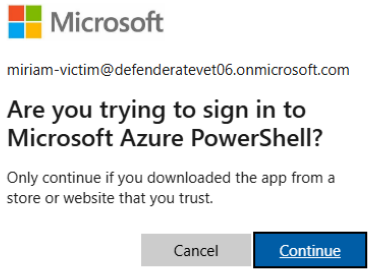
Token Type	Role
Access Token	Defines what resources and operations the token can access (authorization)
Refresh Token	Can be used to request new access tokens with the same or fewer scopes
Id Token	Defines who the user is (authentication)

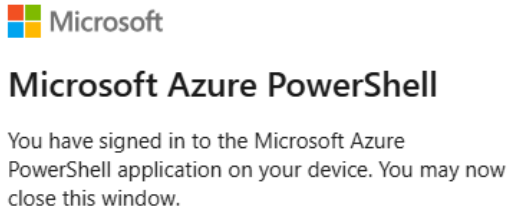
- The token can only be used to access the resources and operations **defined by those scopes**.
- When using a refresh token, the client can request a **subset** of the original scopes.
- Scopes:
  - ~~Azure Portal: c44b4083-3bb0-49c1-b47d-974e53cbdf3c~~
  - Microsoft Azure PowerShell: 1950a258-227b-4e31-a9cf-717495945fc2

Device Authentication – in a browser









@miriamwiesner.bsky.social @miriamxyra

PSCONF.EU MALMÖ 25

@miriamwiesner.bsky.social @miriamxyra

Protect your environment

- MFA is not a silver bullet – but still important
  - e.g. against password spraying or password breaches
- Additionally, to MFA: Enable conditional access, identity protection policies, and configure lockout policies
- Block legacy authentication & MFA mechanisms
- Educate your users
  - Don’t stay “always logged in”
  - Delete your cookies when your session closes

Monitor alerts in your XDR and/or SIEM solution

- For Example
  - Risky Users
  - Anomalous Tokens
  - Stolen session cookie was used

- Look for anomalies, e.g.
  - Suspicious Sign-In patterns (Different Location, User Agent, ISP, Tor,…)
  - Unusual MS Graph or mailbox activities
- Suspicious PowerShell activities
  - Headless browser usage where it’s not expected
  - Cookie or sessionStorage/localStorage Access and/or extraction

Look for suspicious Sign In Patterns

KQL Starter Snippet

Feel free to adjust and improve, depending on your environment...

```
SigninLogs
| where ResultType == 0  // successful sign-in
| where AuthenticationDetails has "MFA"  // MFA was used
| summarize
    Count = count(),
    DistinctIPs = dcount(IPAddress),
    DistinctUserAgents = dcount(UserAgent),
    FirstSeen = min(TimeGenerated),
    LastSeen = max(TimeGenerated)
    by UserPrincipalName, SessionId, AppDisplayName, AppId, ResourceDisplayName,
ResourceIdentity
| where DistinctIPs > 1 or DistinctUserAgents > 1
| order by LastSeen desc
```

Thank you!

Q&A

15 minutes

@miriamwiesner.bsky.social @miriamxyra