CERTAINITY

Enterprise Phishing

Attack Surface Enumeration and Techniques

$ whoami

Yuri Gbur

- Senior Consultant | Offensive Security @ CERTAINITY
- Penetration Testing / Red Teaming
- MSc Computer Science @ TU Berlin
- OSCP, GCPN, CRTO, CARTP, CARTE

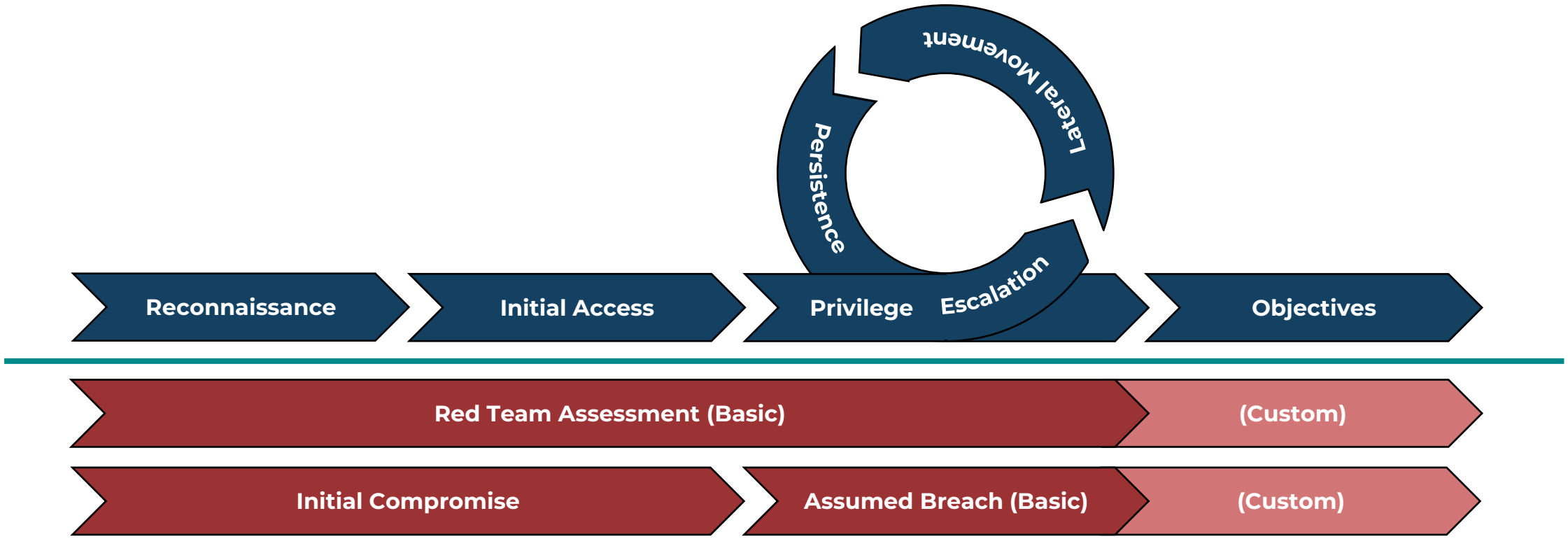
https://www.linkedin.com/in/yuri-gbur
https://infosec.exchange/@yukonsec
https://bsky.app/profile/yukonsec.bsky.social

Agenda

- OSINT / Reconnaissance
- "Clone" Phishing
- Multi-Factor Authentication (MFA)
- Reverse Proxy Phishing
- Phishing-Resistant MFA
- Phishing the Phishing-Resistant

Disclaimer:
Die Inhalte dieser Präsentation dienen ausschließlich Forschungszwecken. Die dargestellten (aktiven) Methoden dürfen nur nach vorheriger ausdrücklicher Genehmigung angewendet werden.

Angriffssimulationen



Phishing Landschaft – Wie wird gephished?

Phishing

- Emails
- Szenario kann generisch an große Gruppen gesendet werden.
- Geringer Angreiferaufwand
- Viele technische Abwehrmaßnahmen (Spam Score, Domain Reputation, Crawling ...)

Spear-Phishing / Whaling

- Emails
- Zielgerichtet auf kleine Gruppen oder Einzelpersonen, z.B. Führungspersonen ("Whaling").
- Hoher Reconnaissance Aufwand

Vishing

- Telefonanrufe (Voice Phishing)
- Hoher Angreiferaufwand, meist ebenfalls Zielgerichtet
- Kaum technische Abwehrmaßnahmen

Smishing (SMS Phishing), Quishing (QR-Code Phishing), ...

Phishing Landschaft – Was ist das Ziel?

Informationen

- Personenbezogene Daten
- Betriebsgeheimnisse
- Auch als aktive Reconnaissance

Credentials

- Benutzernamen / Passwörter
- Web-basierte / Öffentliche Zugänge (M365, DropBox, NextCloud, Webseiten, ...)

Remote Zugriff

- Malware Deployment
- Command & Control Zugriff
- Ransomware

Warum Credential Phishing?

- Weniger Technische Hürden
  - ➢ Kein AV, EDR, Credential Guard, ...
- Benutzerakzeptanz
  - ➢ Passwörter im Browser einzugeben ist unverdächtiger als Dateien aus dem Internet auszuführen.
- Passwortwiederverwendung
  - ➢ "Phish once, compromise many".
- Hoher Impakt
  - ➢ Kompromittierung von Cloud oder SaaS Accounts (z.B. M365).

TODO-Liste

- Angriffsziele
  - Domain
  - Emailadressen
- Szenario / Incentivierung
- Phishing-Link

CERTAINITY

OSINT / Reconnaissance

“If you know neither the enemy nor yourself, you will succumb in every battle.”

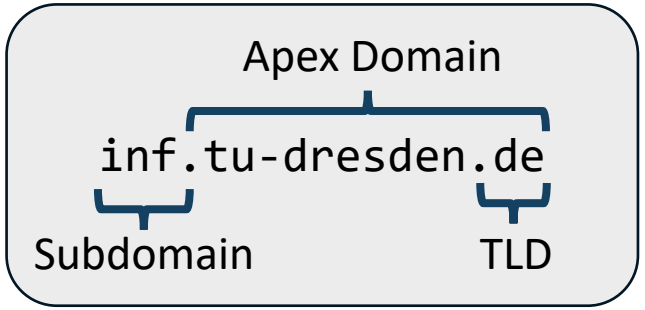
- Sun Tzu

From Zero to Hero

Social Media

Webseiten Scraping ⟷ Firmenname / Domain ⟷ Unternehmensdaten

Subdomain / Apex Domain Enumeration



https://osintframework.com/

Allgemeine Suchmaschinen

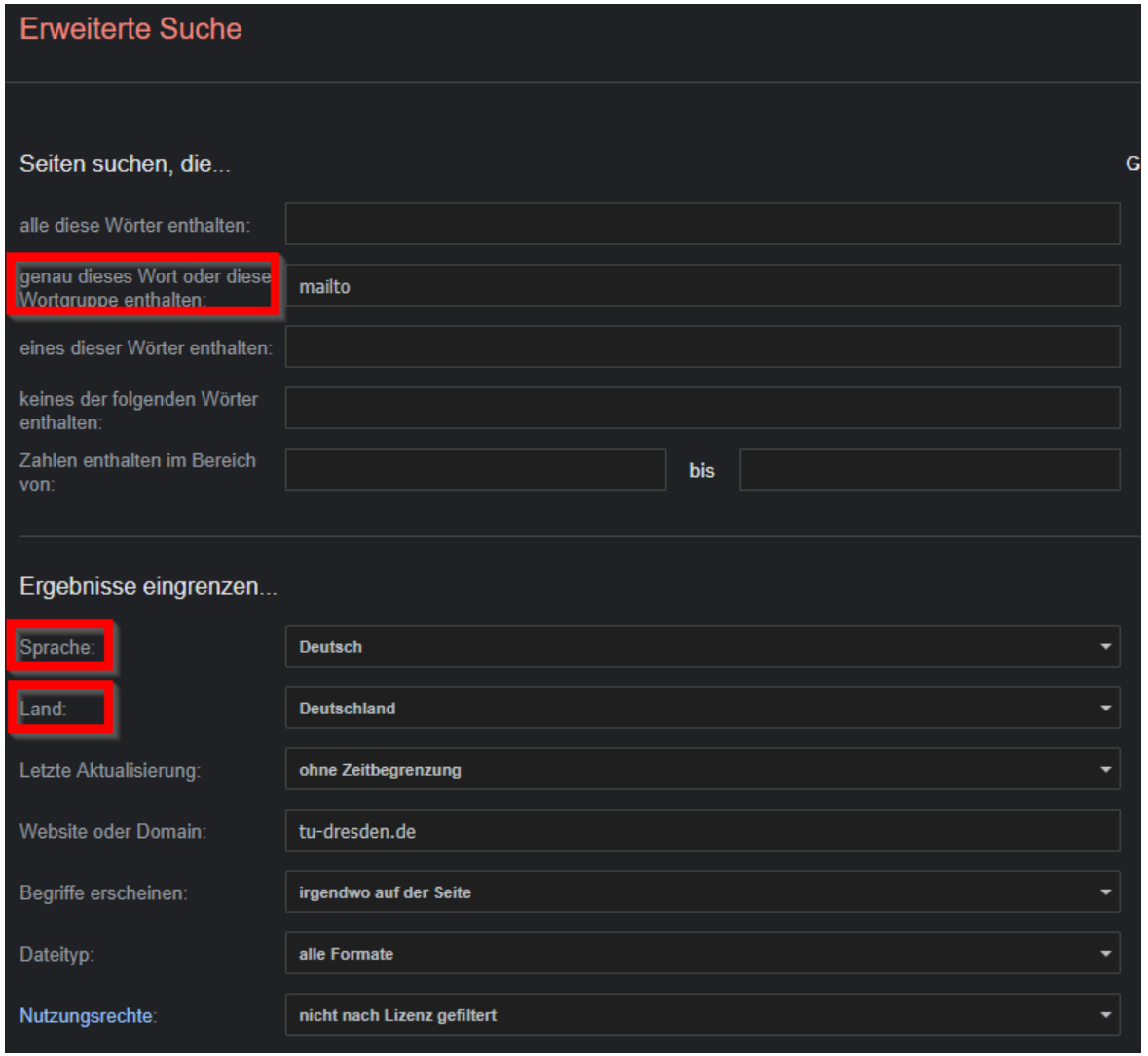
Google (https://google.com)

"Dorking"

- **inurl**:tu-dresden
- **site**:tu-dresden.de
- **intitle**:"Technische Universität Dresden"
- **intext**:mailto **site**:tu-dresden.de

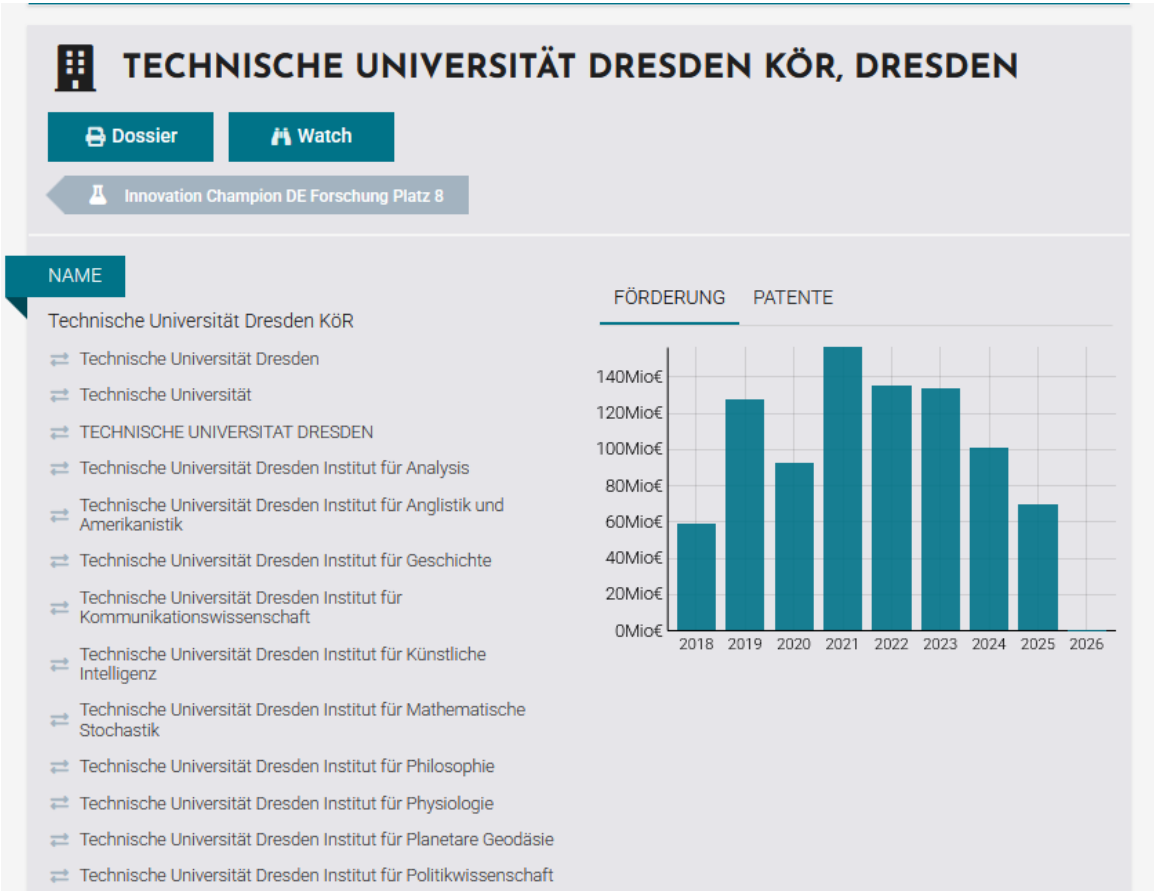
"Reverse Image Search"

Ähnliche Funktionalität in DuckDuckGo, Bing, Yandex, Baidu, ...

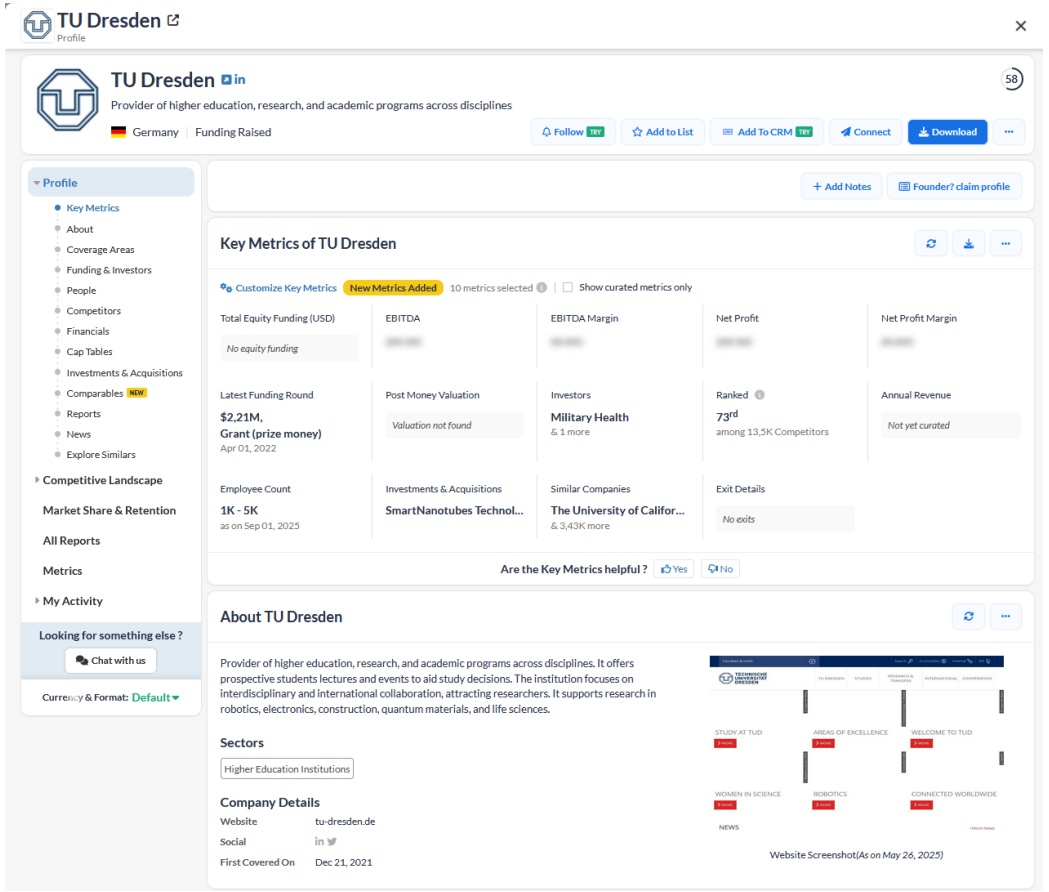


Firmeninformationen

Northdata (https://www.northdata.de)



Tracxn (https://tracxn.com)



ASN / IP Reverse Search

```
┌──(kali㉿kali)-(2026-01-20 (21:11:56))-[~]
└─$ dig +short tu-dresden.de
141.76.14.10
```

```
┌──(kali㉿kali)-(2026-01-20 (21:13:11))-[~]
└─$ whois 141.76.14.10 | grep AS
mnt-domains:    TUD-HOSTMASTER-MNT
% Information related to '141.76.0.0/16AS680'
origin:         AS680
```

2a13:dd80::/29	Route	Technische Universitaet Dresden
192.76.154.0/24	Route	Technische Universitaet Dresden
141.76.0.0/16	Route	Technische Universitaet Dresden
141.30.0.0/16	Route	Technische Universitaet Dresden

Achtung: Aktive Enumeration

```
┌──(kali㉿kali)-(2026-01-23 (17:57:04))-[~]
└─$ dig +short -x 141.76.14.10
www.tu-dresden.de.
```

```
┌──(kali㉿kali)-(2026-01-20 (21:32:02))-[~]
└─$ caduceus -i 192.76.154.0/24,141.76.0.0/16,141.30.0.0/16
endorse.hpr-smwk.sachsen.de
endorse.hpr-smwk.sachsen.de
smwkhprts1.hpr-smwk.sachsen.de
debian.inf.tu-dresden.de
debian.inf.tu-dresden.de
ftp.inf.tu-dresden.de
ftp.inf.tu-dresden.de
studenten.ihi-zittau.de
studenten.ihi-zittau.de
exway-e1.voip.tu-dresden.de
collab-edge.mailbox.tu-dresden.de
collab-edge.tu-dresden.de
collab-edge.voip.tu-dresden.de
exway-e1.voip.tu-dresden.de
idp.tu-dresden.de
idp.tu-dresden.de
idp2.htw-dresden.de
idp2.htw-dresden.de
tu-dresden.de
tu-dresden.de
dresden-uni.eu
www.tud.de
```

Was ist mit der Cloud?

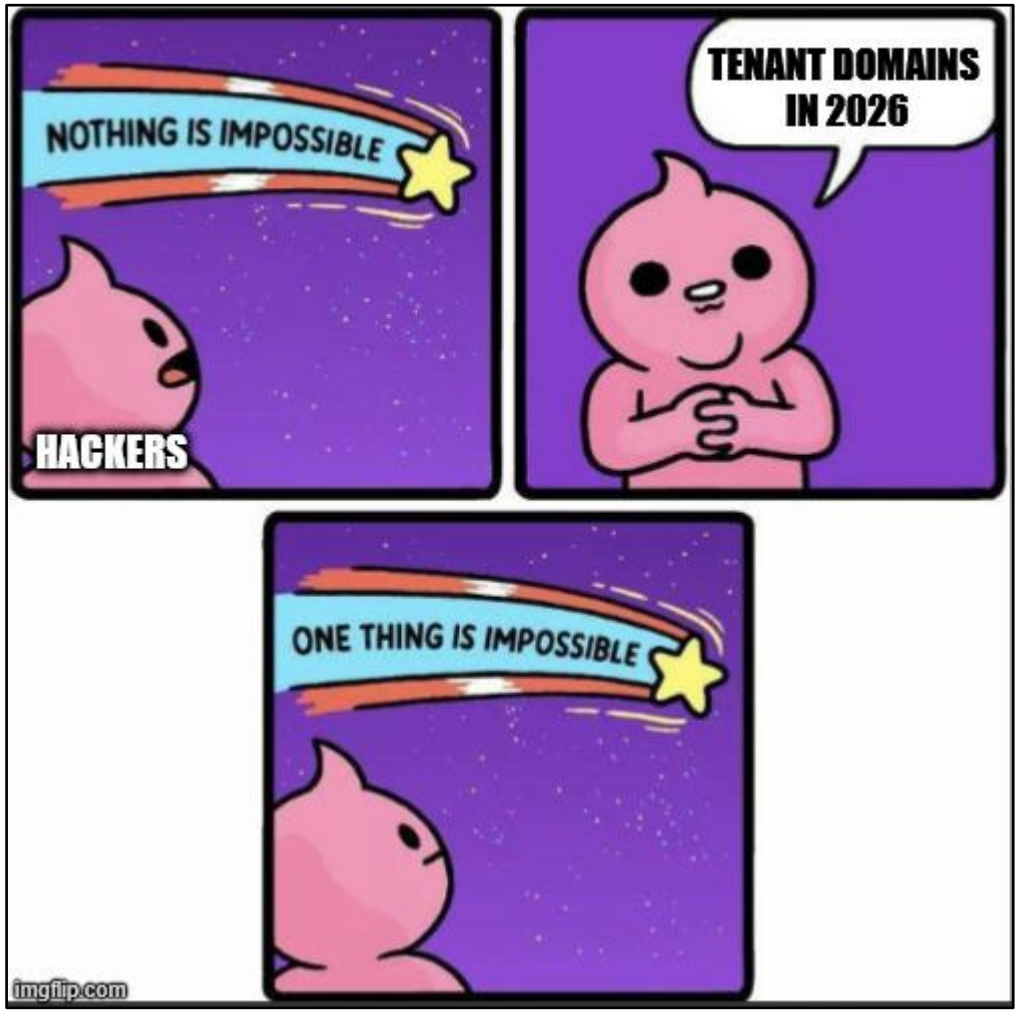
- Scan der gesamten IP-Ranges der Cloud Provider auf Port 443
  - Mapping der Domains auf bekannte Apex Domains
  - Mapping der Zertifikatsinformation auf bekannte Firmennamen
- Sammlung der IP-Ranges: https://github.com/lord-alfred/ipranges
- Laufzeit ~3 Tage
- Aktives Scanning, aber Pattern kaum für das Ziel erkennbar.

Google Cloud

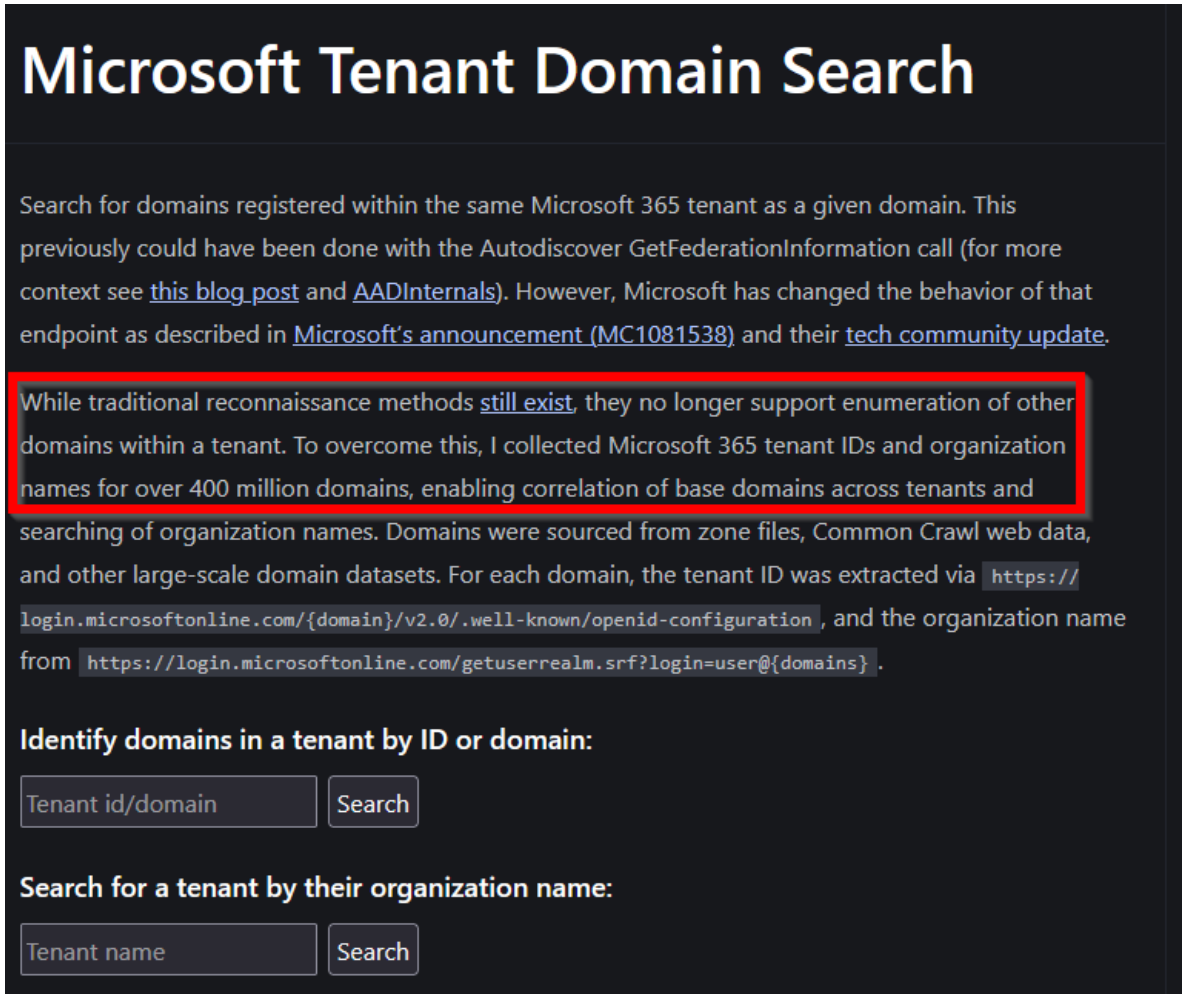
DigitalOcean

Entra ID Tenant Domains


```
https://autodiscover-
s.outlook.com/autodiscover/
autodiscover.svc
```



Entra ID "Vorratsdatenspeicherung"



Original API

https://micahvandeusen.com/tools/tenant-domains/

Tooling

https://github.com/TheArqsz/tenant-domains

```
┌──(kali㉿kali)-(2026-01-20 (22:18:08))-[~/Tools/Enumeration/
└─$ ./tenant-domains.sh -d microsoft.com

[*] Searching for domain: microsoft.com
2hatsecurity.com
acompli.com
adxstudio.com
affirmednetworks.com
ageofempires.com
ageofempiresonline.com
aka.ms
ally.io
altspacevr.com
altvr.com
appcenter.ms
arg-int.core.windows.net
averesystems.com
azmosa.io
azure.com
```

It's always DNS – Even for Reconnaissance

```
┌──(kali㉿kali)-(2026-01-20 (22:23:48))-[~]
└─$ for t in A AAAA MX TXT NS SOA SRV CAA CNAME; do
  dig tu-dresden.de $t +short
done
141.76.14.10
10 b3011.mx.srv.dfn.de.
10 a3011.mx.srv.dfn.de.
10 c3011.mx.srv.dfn.de.
"v=spf1 include:_spf.zih.tu-dresden.de include:_spf.o301.mx.srv.dfn.de include:_spf.bps-system.de includ
e:cemsc.net include:_spf.zimpel.de ~all"
"adobe-idp-site-verification=6e2dfc8c175f7d874197fdee6fd92985d1f52f826a486a6e9b9586de11b345a3"
"MS=D5C91E3A539F983C73A5FCFA8FCF7195ADAD6D7E"
"lnk_sndcpt_00fca03d274327a135473e33e07996dd"
"ZOOM_verify_BknoIvsqjs9bXO0MErTgyw"
"google-site-verification=DGZkuR23xCSStevwpTamkYn6UhvzY8i_KmG3AnopG5Y"
"cisco-ci-domain-verification=7e112bd4572ac03fd65505b65a3f9f47ec659032c03cbb12548b3231964e81d8"
adns1.zih.tu-dresden.de.
dns-1.dfn.de.
adns2.zih.tu-dresden.de.
dns-3.dfn.de.
pdns1.zih.tu-dresden.de. hostmaster.tu-dresden.de. 2026011601 14400 1800 2764800 1800
0 issue "pki.dfn.de"
0 issue "harica.gr"
0 issue "letsencrypt.org"
0 iodef "mailto:ca@tu-dresden.de"
0 issuewild ";"
0 issue "sectigo.com"
```

```
┌──(kali㉿kali)-(2026-01-20 (22:28:28))-[~]
└─$ dig +short _dmarc.tu-dresden.de TXT
"v=DMARC1; p=none; rua=mailto:dmarcreports@zih.tu-dresden.de"
```

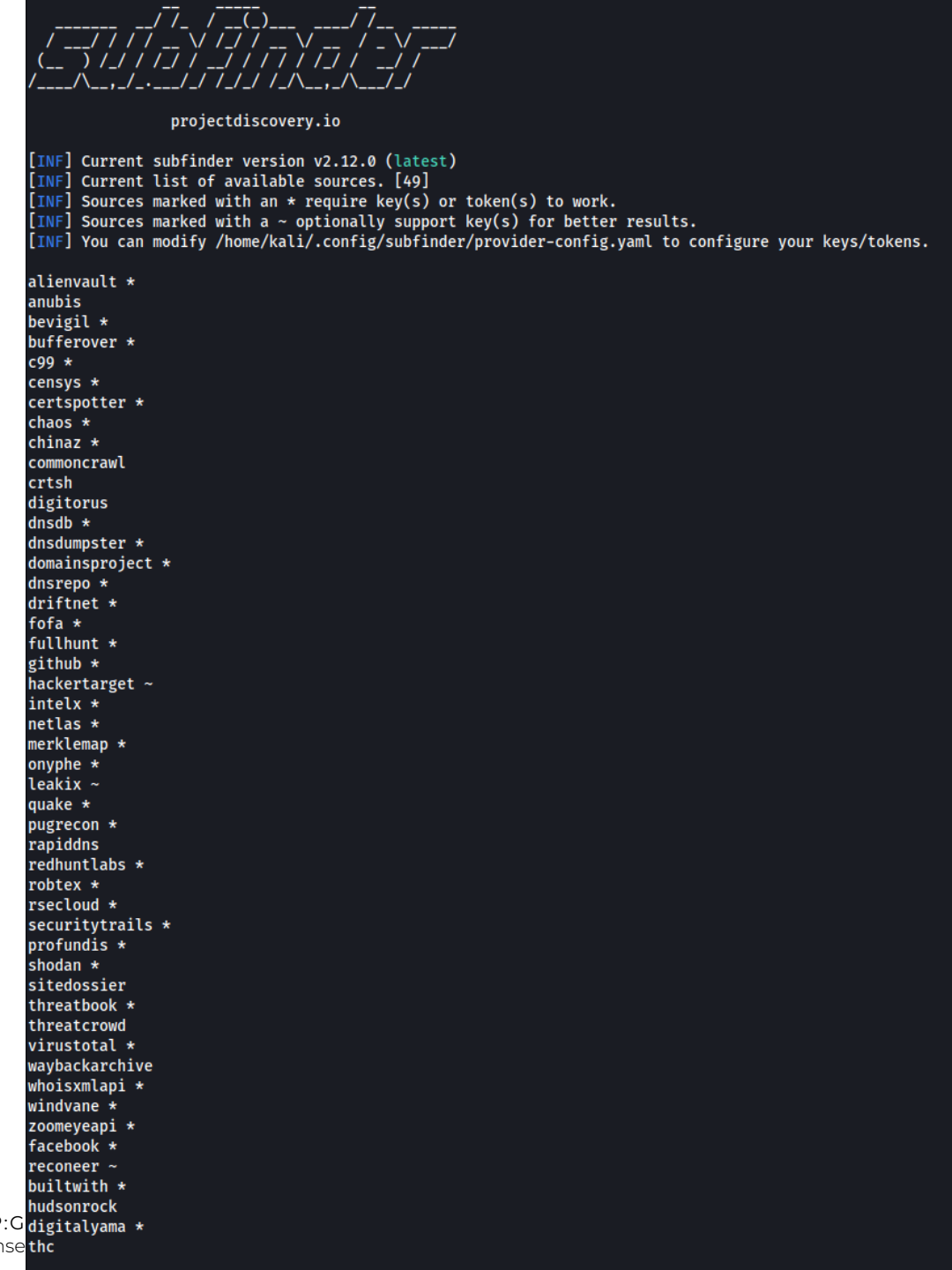
Passive Enumeration

```
┌──(kali㉿kali)-(2026-01-20 (22:31:43))-[~]
└─$ subfinder -d tu-dresden.de -all -o tu-dresden.de_subfinder.txt


                     __    _____                  __
   _______  __/ /_  / __(_)___  ____/ /__  _____
  / ___/ / / / __ \/ /_/ / __ \/ __  / _ \/ ___/
 (__  ) /_/ / /_/ / __/ / / / / /_/ /  __/ /
/____/\__,_/_.___/_/ /_/_/ /_/\__,_/\___/_/

                projectdiscovery.io

[INF] Current subfinder version v2.12.0 (latest)
[INF] Loading provider config from /home/kali/.config/subfinder/provider-config.yaml
[INF] Enumerating subdomains for tu-dresden.de
x8d1ee12e.agdsn.tu-dresden.de
hhb03.wasser.tu-dresden.de
hw-manage.zih.tu-dresden.de
siox4.zih.tu-dresden.de
we0649.dip.tu-dresden.de
we1013.dip.tu-dresden.de
wg0455.dip.tu-dresden.de
[INF] Found 49069 subdomains for tu-dresden.de in 1 minute 18 seconds
```

Subdomain Datenquellen

- Certificate Information (https://crt.sh/)
- Internet Intelligence Services
  - Censys (https://www.censys.com/)
  - Project Chaos (https://chaos.projectdiscovery.io/)
  - Shodan (https://www.shodan.io/)
  - IntelX (https://intelx.io/)
- Repositories (https://github.com/)
- Subdomain Services (https://subdomainfinder.c99.nl/)
- ...

- Viele Services benötigen bezahlte Lizenzen / API Keys



Active Subdomain Brute-Force

- Liste mit häufig verwendeten Subdomains
- DNS-Anfragen iterativ über alle Kombinationen

Herausforderungen

- Oft leicht erkennbar in DNS-Logs
- DNS-Rate-Limiting
  - Proxies / mehrere Resolver / Bulk Lookups

In der Realität oft kaum einzigartige Ergebnisse im Vergleich zu (großteils) passiven Methoden und deutlich langsamer.

Email-Addressen Sammeln

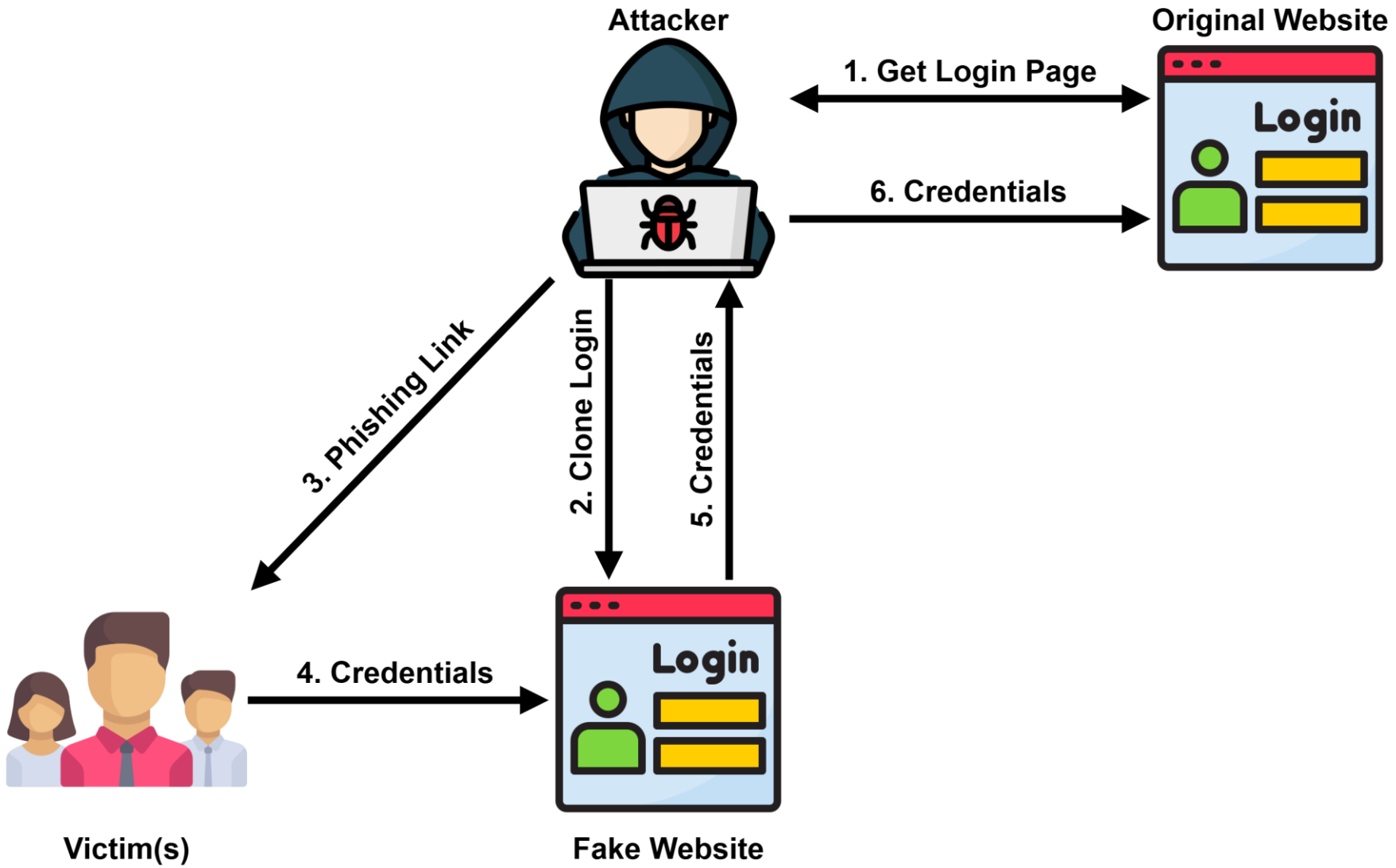
- Webseiten - Herausfinden von Mustern (z.B. <vorname>.<nachname>@tu-dresden.de)
- LinkedIn Scraping - Namen auf Muster übertragen
- Benutzernamen Enumeration - z.B. M365 Login

```
┌──(kali㉿kali)-(2026-01-23 (17:40:28))-[~/Tools/Enumeration/CredMaster]
└─$ python3 -W ignore::DeprecationWarning credmaster.py --profile_name fireprox --plugin o365enum -u test.html --r
egion eu-central-1 --threads 1 --color
[2026-01-23 16:41:18.063] Execution started at: 2026-01-23 16:41:18.063279
[2026-01-23 16:41:18.063] Creating 1 API Gateways for https://login.microsoftonline.com
[2026-01-23 16:41:19.051] Created API - Region: eu-central-1 ID: (pp1mh4f807) - https://pp1mh4f807.execute-api.eu-
central-1.amazonaws.com/fireprox/ => https://login.microsoftonline.com
[2026-01-23 16:41:19.355] Testconnect: Connection success, continuing
[2026-01-23 16:41:19.355] Total Regions Available: 15
[2026-01-23 16:41:19.355] Total API Gateways: 1
[2026-01-23 16:41:19.355] Starting Spray...
[2026-01-23 16:41:19.355] Loading users and useragents
[2026-01-23 16:41:19.618] eu-central-1: [!] VALID_USERNAME: yuri.gbur@certainity.com
[2026-01-23 16:41:19.772] eu-central-1: [-] UNKNOWN_USERNAME: max.mustermann@certainity.com
[2026-01-23 16:41:19.772] Completed userenum at 2026-01-23 16:41:19.772795
[2026-01-23 16:41:19.906] Destroying API (pp1mh4f807) in region eu-central-1
[2026-01-23 16:41:20.478] End Time: 2026-01-23 16:41:20.478523
[2026-01-23 16:41:20.478] Total Execution: 2.415244 seconds
[2026-01-23 16:41:20.478] Valid credentials identified: 0
```

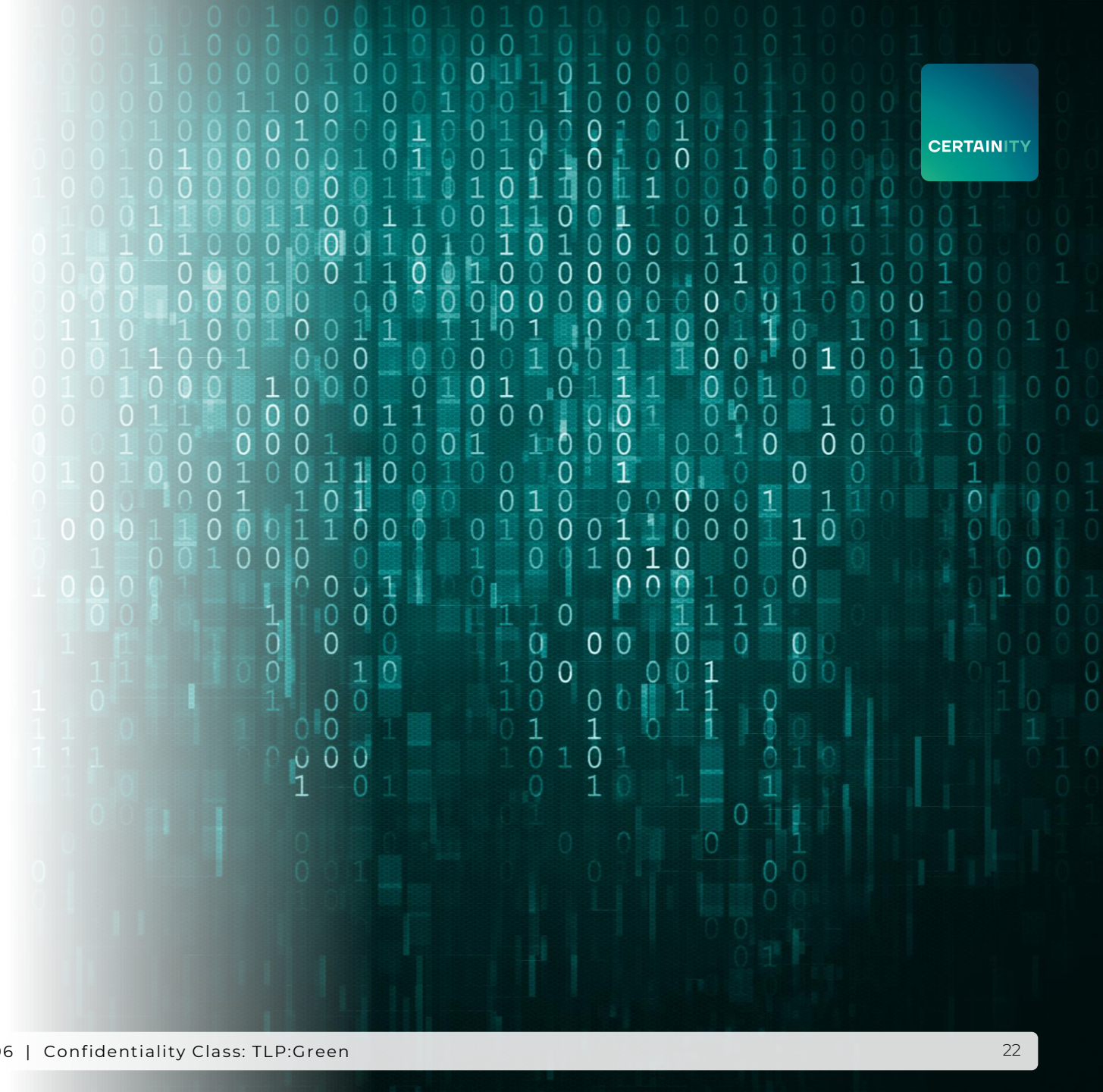
"Clone" Phishing

“Men in general judge more from appearances than from reality.”
- Niccolo Machiavelli

"Clone" Phishing



Gophish Demo / Hands-on



CERTAINITY

Multi-Factor Authentication (MFA)

“No plan survives first contact with the enemy.”
- Helmuth von Moltke

Multi-Factor Authentication (MFA)

- Etwas das ich weiß (z.B. Passwort)
- Etwas das ich besitze (z.B. Mobiltelefon)
- Etwas das ich bin (z.B. Fingerabdruck)
- Wo ich bin (IP-Location) / Wann logge ich mich ein (Uhrzeit)

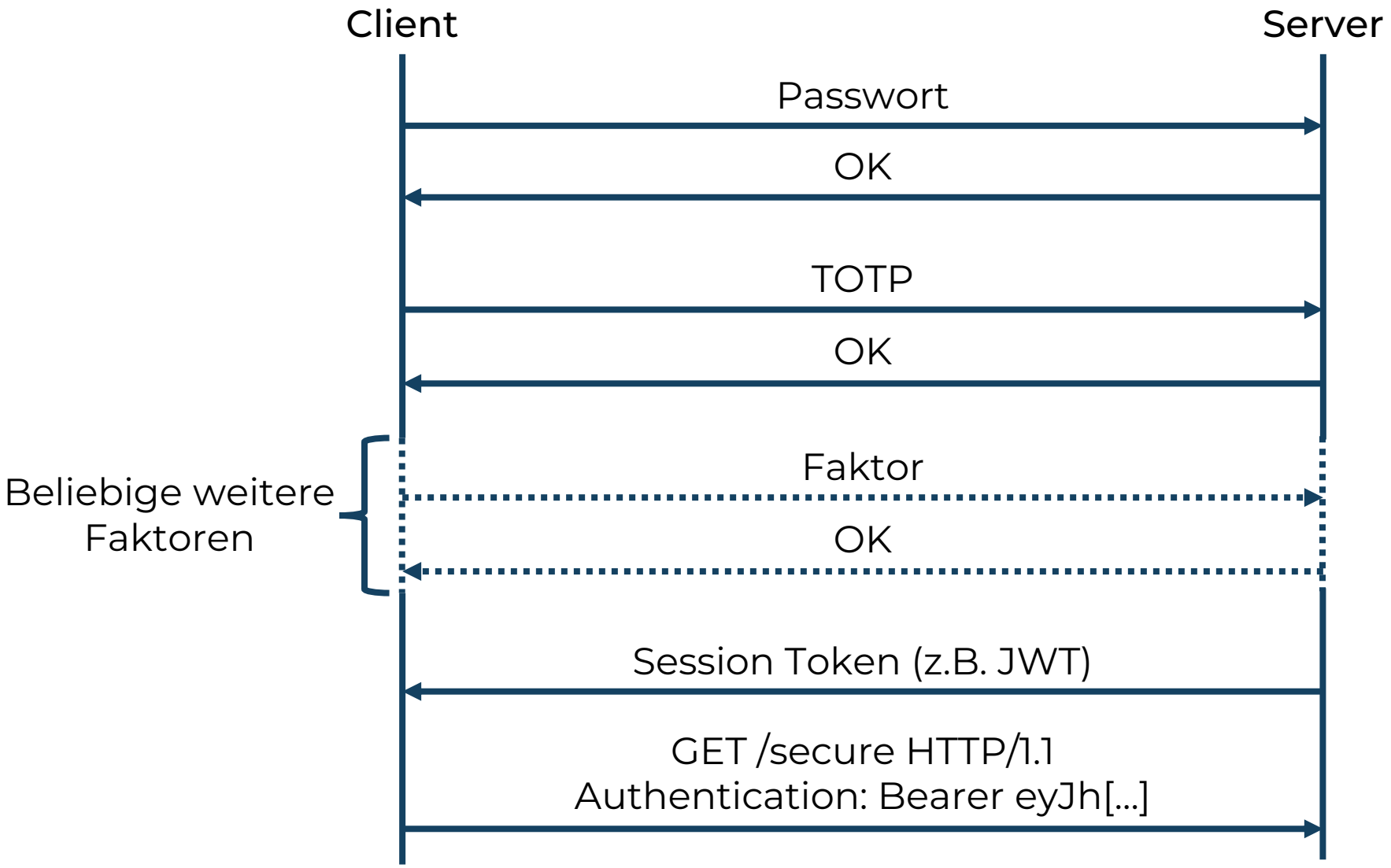
Klassisch

- Passwort
- TOTP

Enterprise

- Passwort
- Gerätebindung
  - Yubikey / Smartcard
  - Compliant Device (z.B. Intunes)
- + Risikoevaluierung
  - Ort
  - Zeit

Modern Web Authentication

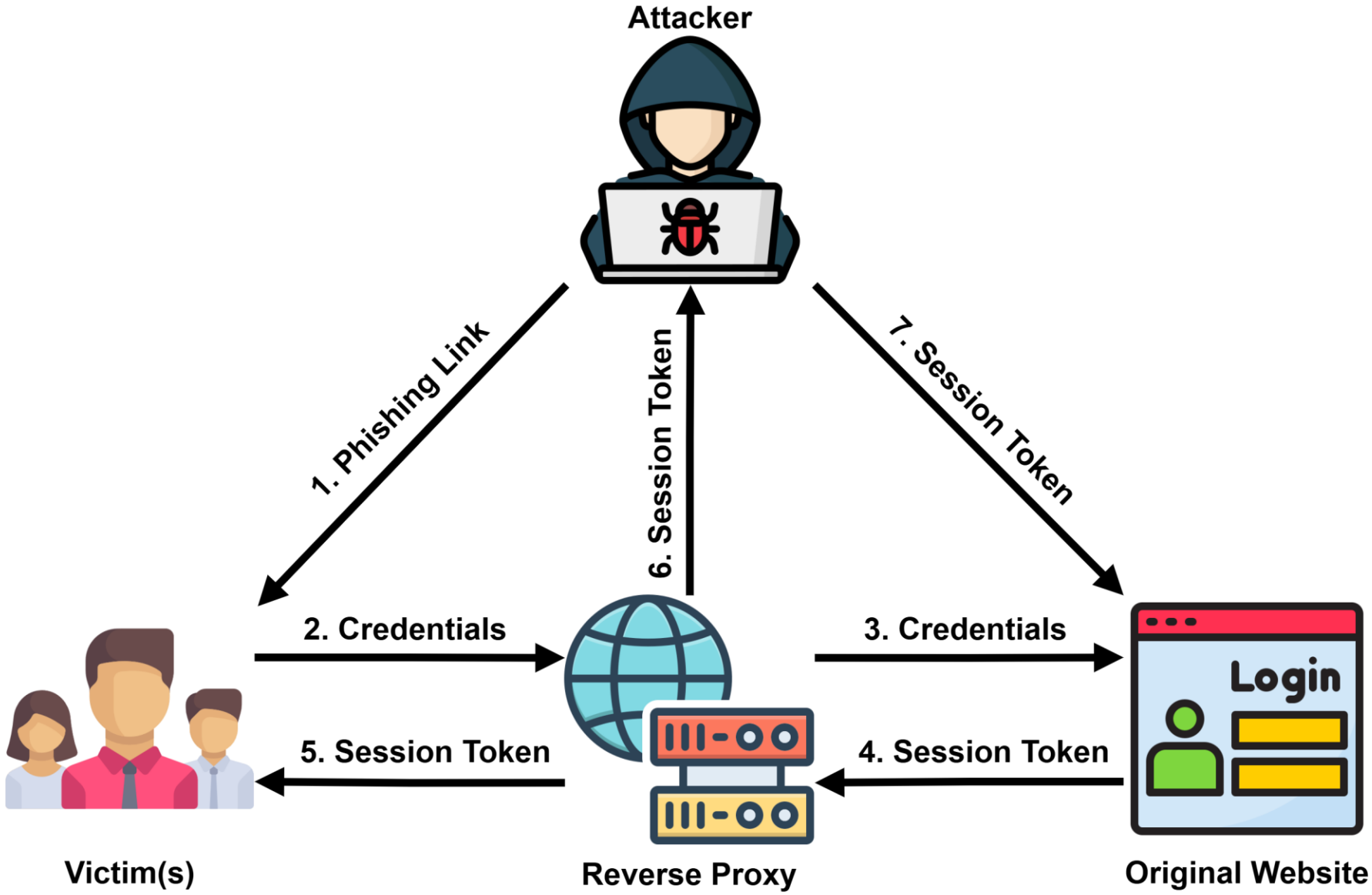


CERTAINITY

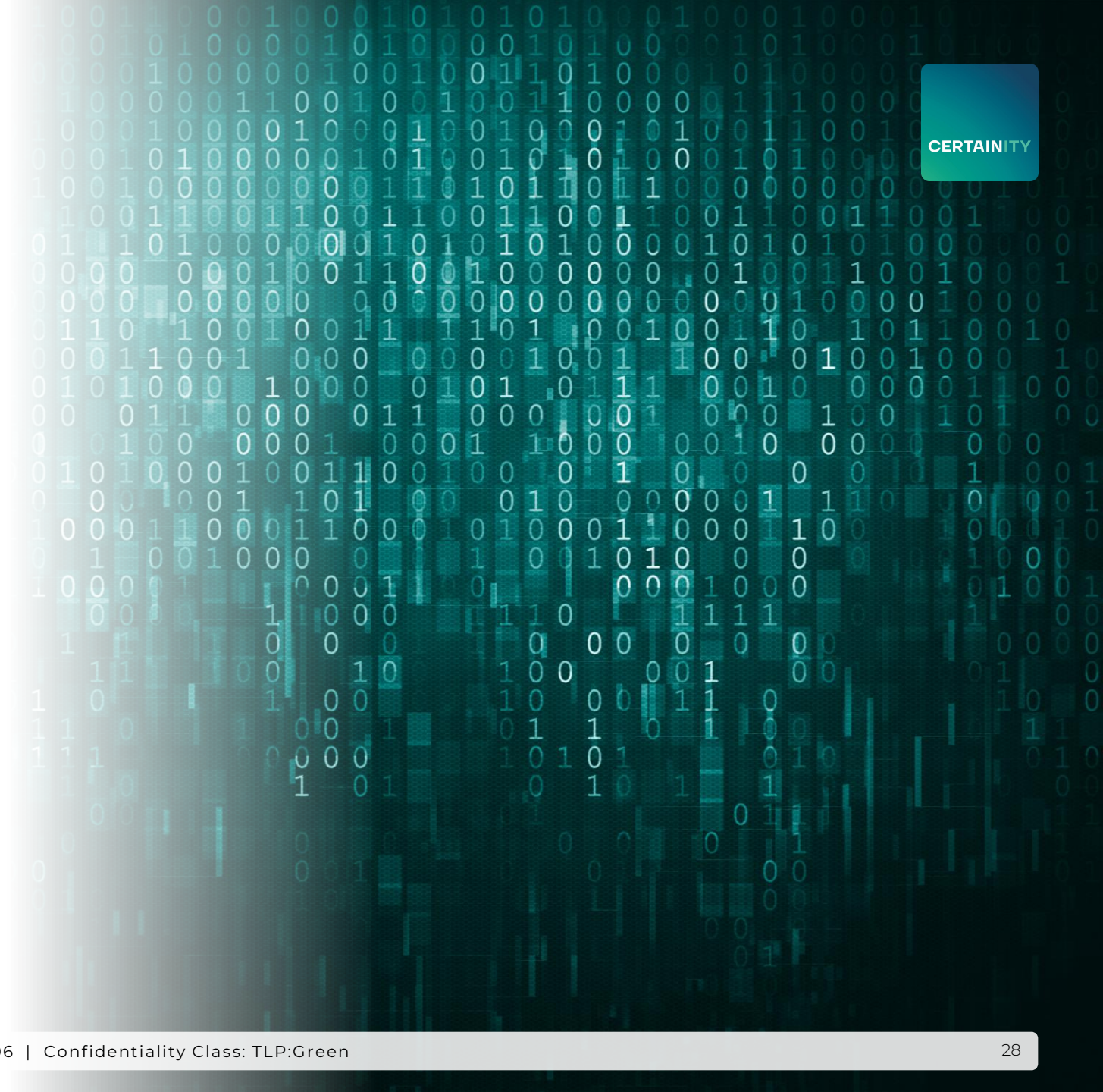
Reverse Proxy Phishing

“He who defends everything defends nothing.”
- Friedrich der Große

Reverse Proxy Phishing



Evilginx Demo / Hands-on



CERTAINITY

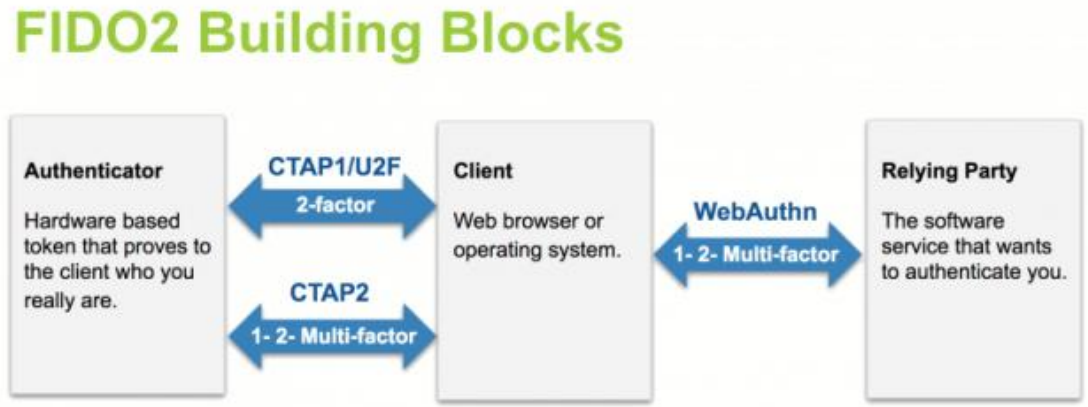
Phishing-Resistant MFA

“Security depends not on trusting the enemy’s intentions, but on controlling their capabilities.”

- Thomas C. Schelling

Gegenmaßnahmen & Phishing-Resistant MFA

- Besonders gesicherte Aktionen erfordern MFA-Neueingabe (z.B. Passwortwechsel)
  - Nur limitiert Effektiv
- Domain-Binding (Software): Client-seitige Validierung der Domain (JavaScript)
  - Ausgeliefertes JavaScript / Kommunikation ist Angreifer-kontrolliert
  - Browser-Emulation im Reverse-Proxy
- Domain-Binding (Hardware):
  Authentication-Gerät (z.B. Yubikey / Passkeys) speichert Domain mit ab.
  - Nicht Manipulierbar durch Angreifer
  - Emulation nicht möglich, da Authentication-Gerät direkt mit dem lokalen Browser kommuniziert.

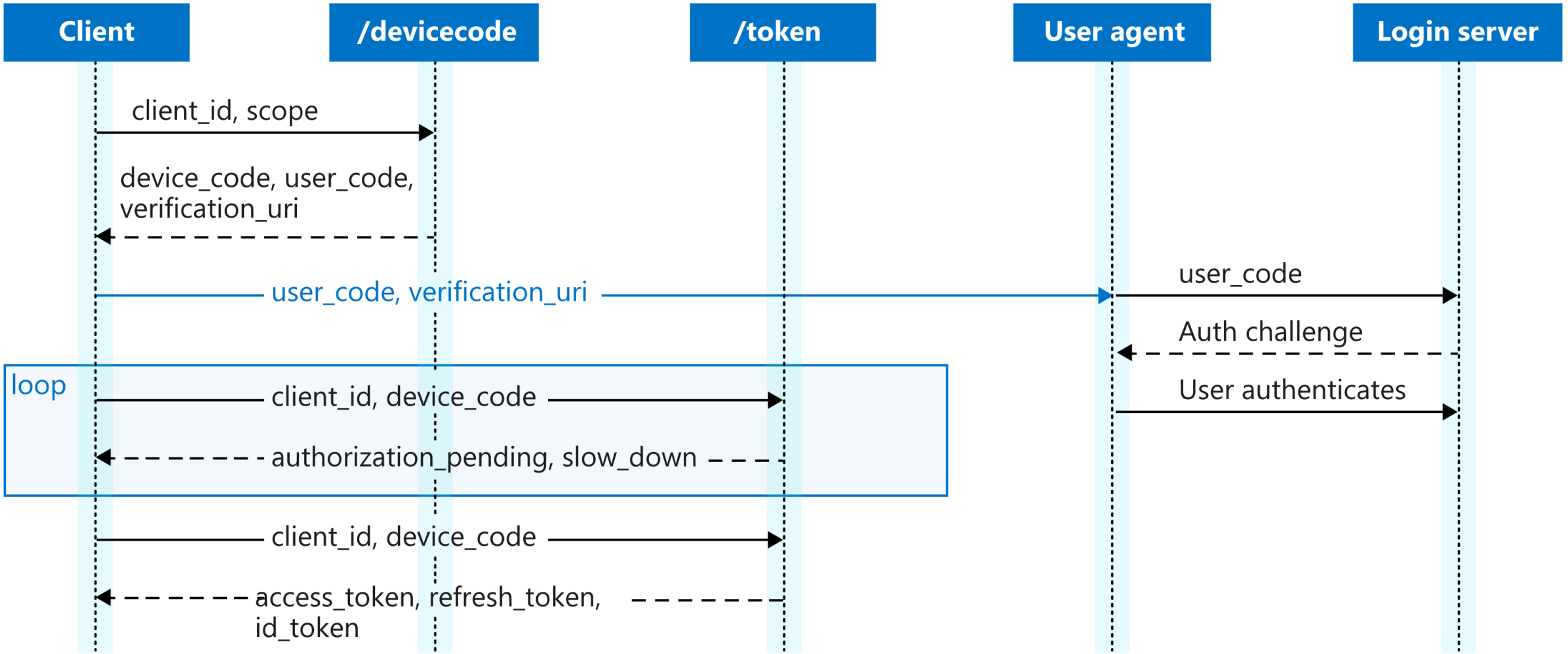


CERTAINITY

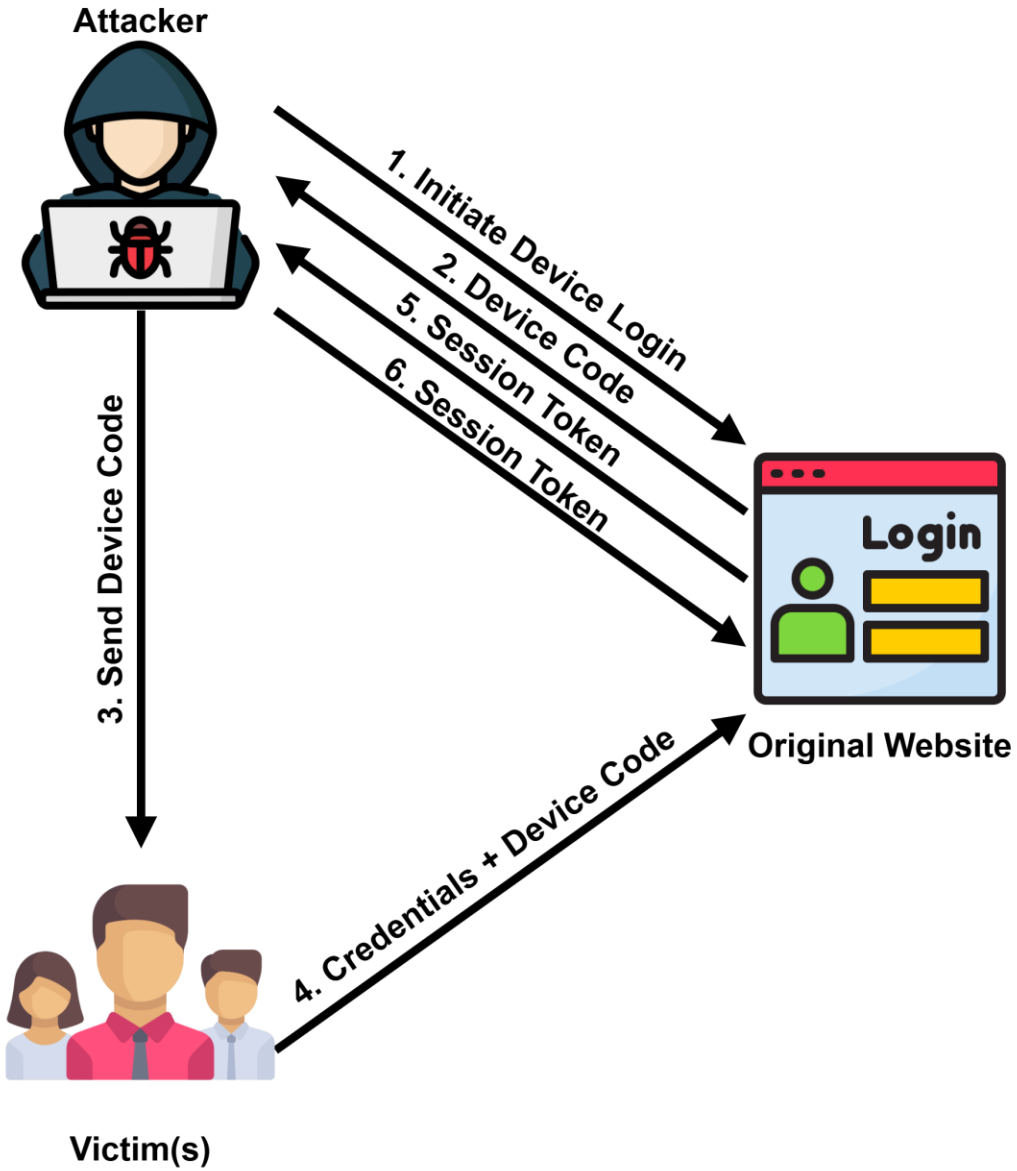
Phishing the Phishing-Resistant

“Avoid what is strong and strike at what is weak.”
- Sun Tzu

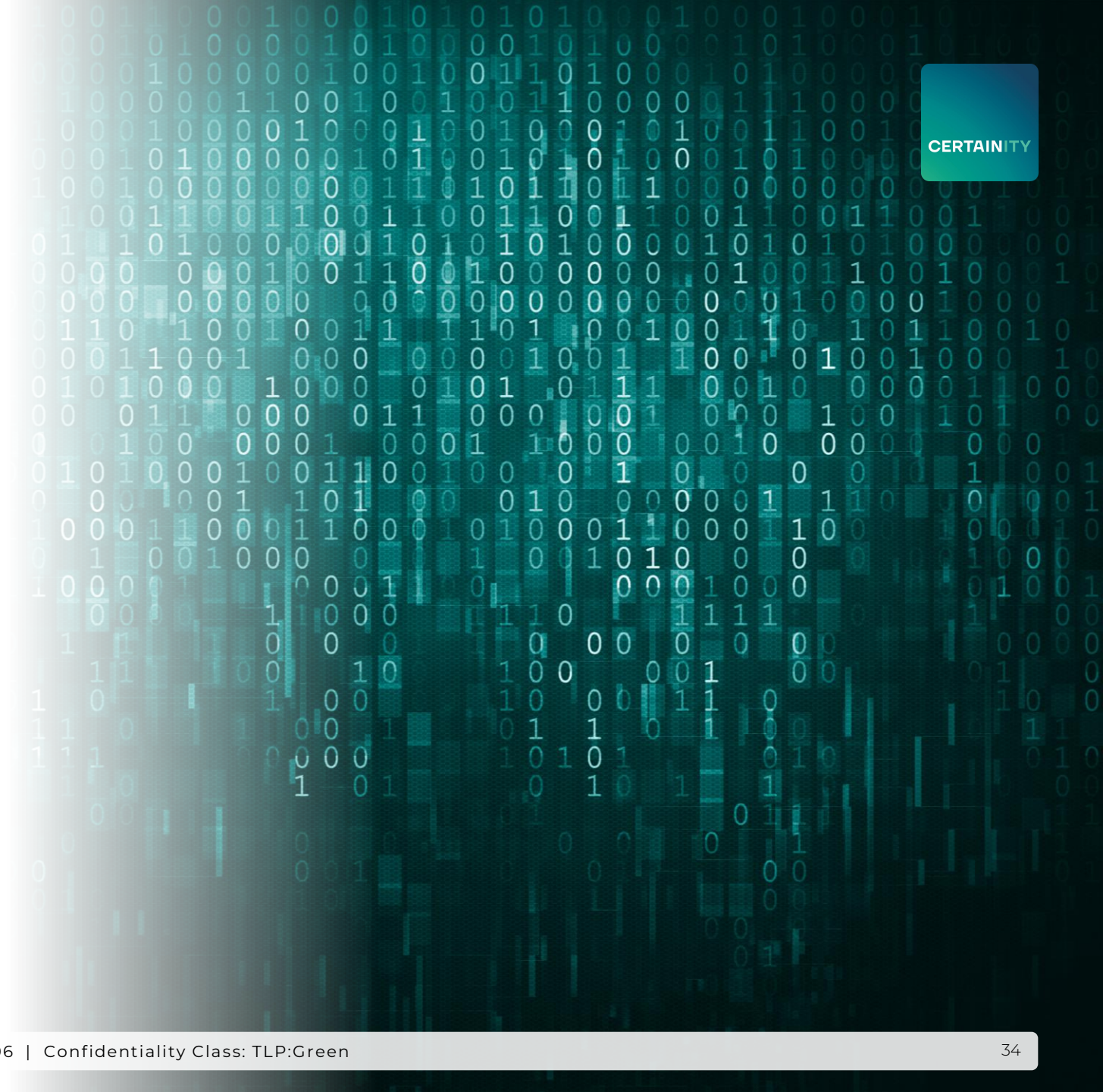
Device Code Authentication



Device Code Phishing



Device Code Phishing Demo



Passkeys: Usability VS Security

- Problem 1: Passkeys sind Gerätgebunden
  - Viele Benutzer wollen keine Extrageräte (z.B. Yubikey)
- Lösung: OS / Plattform-Authenticators speichern die Keys

- Problem 2: Viele Benutzer wollen Logins auf vielen Geräten
- Lösung 2: Passkeys können Synchronisiert werden

Wie wird der Sync Abgesichert?

- Login des Plattformanbieters (Google, Microsoft, Apple)

Was wenn diese Logins "klassisch" Abgesichert sind?

- Angreifer können potenziell Passkeys auf ihre Geräte synchronisieren.

Danke fürs Zuhören!

Yuri Gbur
yuri.gbur@certainity.com

LinkedIn

CERTAINITY

CERTAINITY GmbH

reliable. trustworthy. bespoke.

ELMARGASSE 2-4 | A – 1190 VIENNA
HG WIEN, FN 262176 D

office@certainity.com

certainity.com

linkedin.com/company/certainity