



Adversary in the Middle – Notes from the field

Kenneth van Surksum & Erik Loef

DEMO 1 – Adversary in The Middle

- Login with demouserA
- MFA with number matching
- Copy session cookie to new browser

Kopiëren naar

Beantwoorden

Allen beantwoorden

Doorsturen

In-/uitzoomen

Afdrukken

...

Egbert van der Ven heeft Ingenieursbureau Multical BV Persoonlijk en vertrouwelijk - Bijlage.pdf met je gedeeld



Egbert van der Ven (via Dropbox) <no-reply@dropbox.com>

From: Bertjan
Sent on: Tuesday
To: Bertjan
Subject: Bertjan

Aan:



i Sommige inhoud in dit bericht is geblokkeerd omdat de afzender niet in de lijst met veilige afzenders voorkomt.

Afzender vertrouwen

Geblokkeerd

Sommige personen...

Egbert van der Ven (egbertvanderven@multical.nl)
heeft je uitgenodigd om het bestand
**Ingenieursbureau Multical BV Persoonlijk en
vertrouwelijk - Bijlage.pdf** te bekijken in
Dropbox.

Bestand openen

- Screenshots uit de phishing mail genomen:

nl - OneDrive

nl - OneDrive

Sign in to Outlook

https://associacaoindustportugues.nl

https://bqseh.venurconstructions.com/common/oauth2/authorize?client_id=00000002-0000-0ff1-ce00-000000000000&redirect_uri...

OneDrive

Download

Pedro Oliveira > nl

Name

HIER OPENEN OM DOCUMENT TE BEK

Microsoft

Sign in

to continue to Outlook

Email, phone, or Skype

No account? Create one!

Can't access your account?

Next

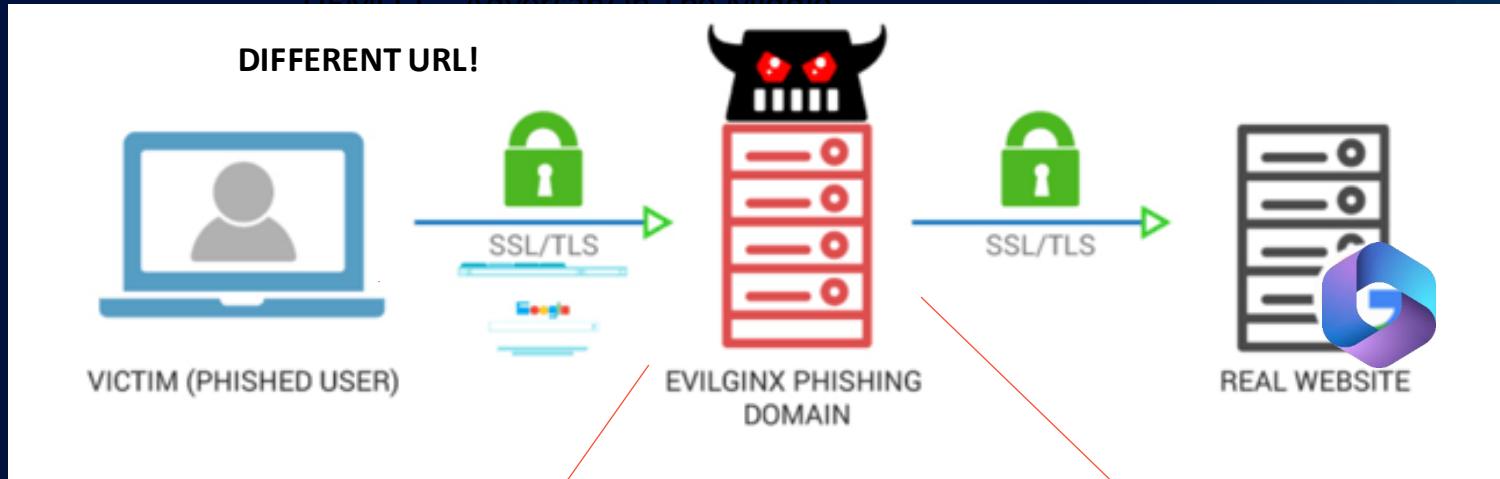
Sign-in options



MODERN
ENDPOINT
MANAGEMENT
SUMMIT
2025

Our setup

DEMO 1 - Adversary in The Middle



DIFFERENT DEVICE

**DIFFERENT IP
ADDRESS**



Meanwhile @ SOC

- DEMO 1 –
DIFFERENT URL
• Login w/
• MFA w/
• Copy se

A potentially malicious URL click was detected

High | Unknown | Resolved

Manage alert | View messages in Explorer | Link alert to another incident | Tune alert

Office 365

Generated on Aug 13, 2024 10:46:34 AM First activity Aug 13, 2024 10:42:08 AM

Last activity Aug 13, 2024 10:42:08 AM

Evidence

Entity Name	Remediation Status	Verdict
image480421.png		
Outlook-Microsoft.png		
Outlook-permission.png		
image.png		
https://app.pipefy.com/public/form/rsKgHx4		

[View All](#)

Alert description

We have detected that one of your users has recently clicked on a link that was found to be malicious. - V1.0.0.5

Real Life Example



Microsoft Sentinel 16-1 19:03

Risky User [REDACTED] found

Severity: Medium

Workspace: stra1-proxsys-sentinel

Description: Risky User [REDACTED] Risklevel hidden

Please check if the user is compromised

Alerts:

Displayname	Description
Risky User [REDACTED] found	Risky User [REDACTED] Risklevel hidden Please check if the user is compromised

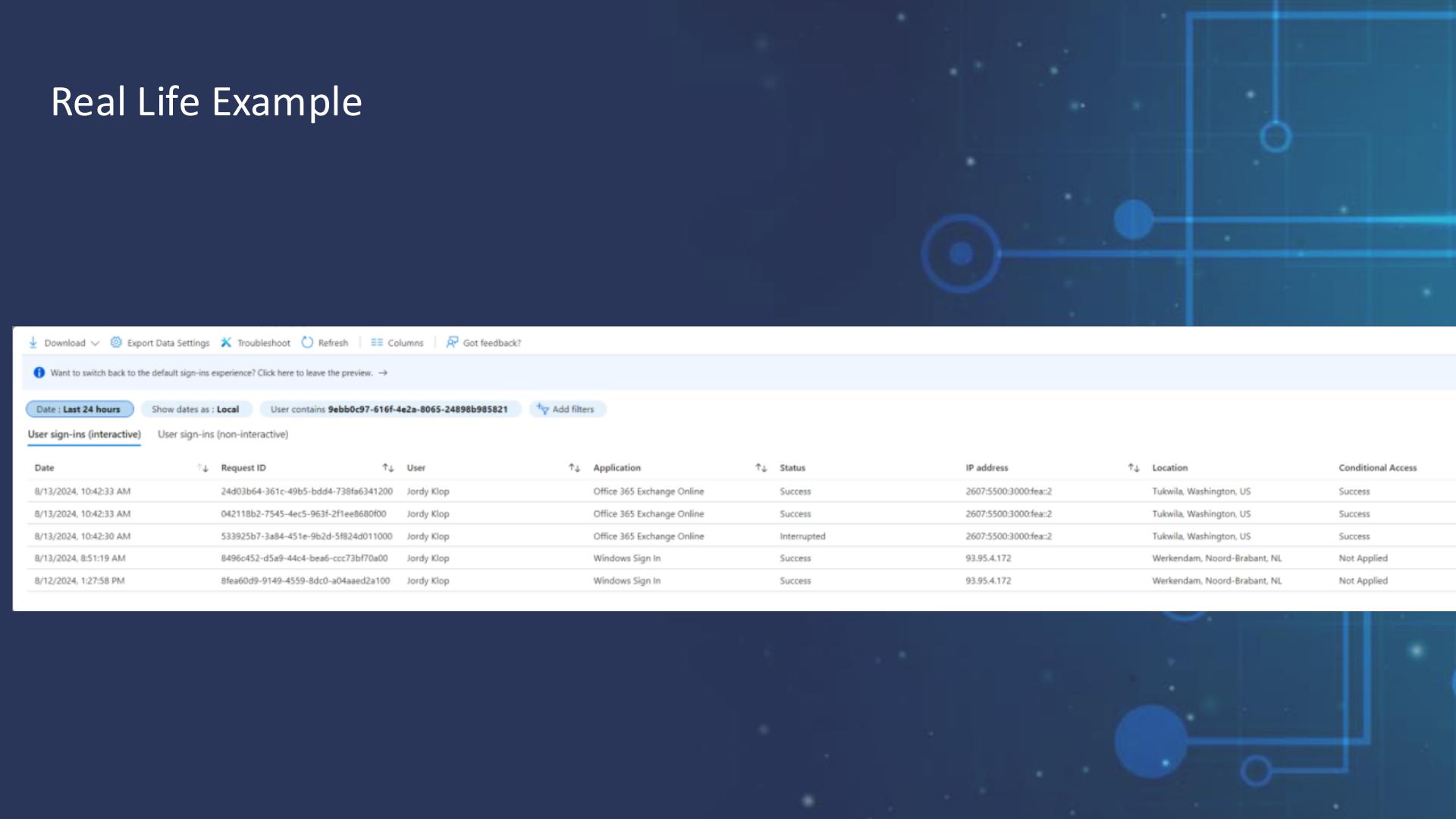
Related Entities:

Type	Entity
Account	[REDACTED]

Recent Example 17-01-2025

1/17/2025, 5:53:25 AM	87d8d544-ff8e-4ecd-bf79-f7ba9a4c1500		Office 365 Exchange Online	Failure	154.117.184.142	Auckland Park, Gauteng.
1/17/2025, 5:53:23 AM	8590fe6a-3103-4776-902a-a6f27996a000		Office 365 Exchange Online	Interrupted	154.117.184.142	Auckland Park, Gauteng.
1/17/2025, 5:53:23 AM	9dd1a0a9-d6ca-46a2-abd9-048744742d00		OfficeHome	Failure	154.117.184.142	Auckland Park, Gauteng.
1/17/2025, 5:53:23 AM	2e4cc499-1344-45b1-8bcc-346972b11d00		OfficeHome	Failure	154.117.184.142	Auckland Park, Gauteng.
1/17/2025, 5:53:22 AM	e3371929-d45e-44ad-9c88-6fd85aeac200		OfficeHome	Failure	154.117.184.142	Auckland Park, Gauteng.
1/17/2025, 5:53:21 AM	9dd1a0a9-d6ca-46a2-abd9-048715742d00		OfficeHome	Failure	154.117.184.142	Auckland Park, Gauteng.
1/17/2025, 5:53:20 AM	0a62f004-be5f-4f1a-9be1-49cf2869100		OfficeHome	Failure	154.117.184.142	Auckland Park, Gauteng.
1/17/2025, 5:53:20 AM	2997ed7b-6476-4545-8407-7089ab617600		OfficeHome	Failure	154.117.184.142	Auckland Park, Gauteng.
1/17/2025, 5:51:18 AM	8590fe6a-3103-4776-902a-a6f23a96a000		OfficeHome	Failure	154.117.184.142	Auckland Park, Gauteng.
1/17/2025, 5:53:16 AM	f55d559a-378c-488e-92e6-3725e3b34d00		OfficeHome	Interrupted	154.117.184.142	Auckland Park, Gauteng.
1/16/2025, 7:05:11 PM	783e0a2d-6d49-40d6-adc8-a8fcf3c47c00		Office 365 Exchange Online	Failure	154.117.184.142	Auckland Park, Gauteng.
1/16/2025, 7:05:09 PM	fcee2140-b396-405f-bec5-a2e7951d7700		Office 365 Exchange Online	Interrupted	154.117.184.142	Auckland Park, Gauteng.
1/16/2025, 6:50:12 PM	8dc80775-cacf-49c7-8ad0-39a60cbf5100		Office 365 Exchange Online	Success	154.117.184.142	Auckland Park, Gauteng.
1/16/2025, 6:50:11 PM	8dc80775-cacf-49c7-8ad0-39a6f3be5100		Office 365 Exchange Online	Interrupted	154.117.184.142	Auckland Park, Gauteng.
1/16/2025, 6:49:59 PM	b1910d74-be48-4b10-ad07-8666858c7600		OfficeHome	Success	154.117.184.142	Auckland Park, Gauteng.
1/16/2025, 6:49:58 PM	c36179ee-3767-4f99-98f3-65dc98a78800		OfficeHome	Interrupted	154.117.184.142	Auckland Park, Gauteng.
1/16/2025, 6:49:12 PM	0e73393c-3909-45e1-a1ed-87339047a600		OfficeHome	Interrupted	154.117.184.142	Auckland Park, Gauteng.
1/16/2025, 6:49:10 PM	bad21405-f117-42dc-8f05-a50a39666c00		OfficeHome	Interrupted	154.117.184.142	Auckland Park, Gauteng.
1/16/2025, 1:01:33 PM	fc3c14fe-19fa-4368-bbd8-e441c3437b00		Windows Sign In	Success	93.95.4.19	Gorinchem, Zuid-Holland
1/16/2025, 10:54:10 AM	c9e220f6-03cc-41c3-ad7d-4d8a071a0d00		Office 365	Success	217.147.18.83	Moskva, Moskva, RU
1/16/2025, 10:54:09 AM	6b7e4102-e226-412a-bd01-48bd1a0721500		Office 365	Interrupted	217.147.18.82	Moskva, Moskva, RU

Real Life Example



Download Export Data Settings Troubleshoot Refresh Columns Got feedback?

Want to switch back to the default sign-ins experience? Click here to leave the preview. →

Date : Last 24 hours Show dates as : Local User contains 9ebb0c97-616f-4e2a-8065-24898b985821 Add filters

User sign-ins (interactive) User sign-ins (non-interactive)

Date	Request ID	User	Application	Status	IP address	Location	Conditional Access
8/13/2024, 10:42:33 AM	24d03b64-361c-49b5-bdd4-738fa6341200	Jordy Klop	Office 365 Exchange Online	Success	2607:5500:3000:fea:2	Tukwila, Washington, US	Success
8/13/2024, 10:42:33 AM	042118b2-7545-4ec5-963f-2f1ee8680f00	Jordy Klop	Office 365 Exchange Online	Success	2607:5500:3000:fea:2	Tukwila, Washington, US	Success
8/13/2024, 10:42:30 AM	533925b7-3a84-451e-9b2d-5f824d011000	Jordy Klop	Office 365 Exchange Online	Interrupted	2607:5500:3000:fea:2	Tukwila, Washington, US	Success
8/13/2024, 8:51:19 AM	8496c452-d5a9-44c4-bea6-ccc73bf70a00	Jordy Klop	Windows Sign In	Success	93.95.4.172	Werkendam, Noord-Brabant, NL	Not Applied
8/12/2024, 1:27:58 PM	8fea60d9-9149-4559-8dc0-a04aaed2a100	Jordy Klop	Windows Sign In	Success	93.95.4.172	Werkendam, Noord-Brabant, NL	Not Applied

Example

User sign-ins (interactive)

A	Date	address	↑↓ Location
O	8/13/2024, 10:42:33 AM	07:5500:3000:fea::2	Tukwila, Washington
O	8/13/2024, 10:42:33 AM	07:5500:3000:fea::2	Tukwila, Washington
O	8/13/2024, 10:42:33 AM	07:5500:3000:fea::2	Tukwila, Washington
w	8/13/2024, 10:42:30 AM	95.4.172	Werkendam, Noord
w	8/13/2024, 10:41:19 AM	95.4.172	Werkendam, Noord
	8/12/2024, 1:27:58 PM		

One year of fighting adversary-in-the-middle, notes from the field



Erik Loef
@erikloef



Kenneth van Surksum
@kennethvs

MFA Methods

Bad: Password

123456

qwerty

password

iloveyou

Password1

Good: Password and...



SMS



Voice

Better: Password and...



Authenticator
(Push Notifications)



Software
Tokens OTP



Hardware Tokens OTP
(Preview)

Best: Passwordless



Authenticator
(Phone Sign-in)



Windows
Hello



FIDO2 security key



Certificates

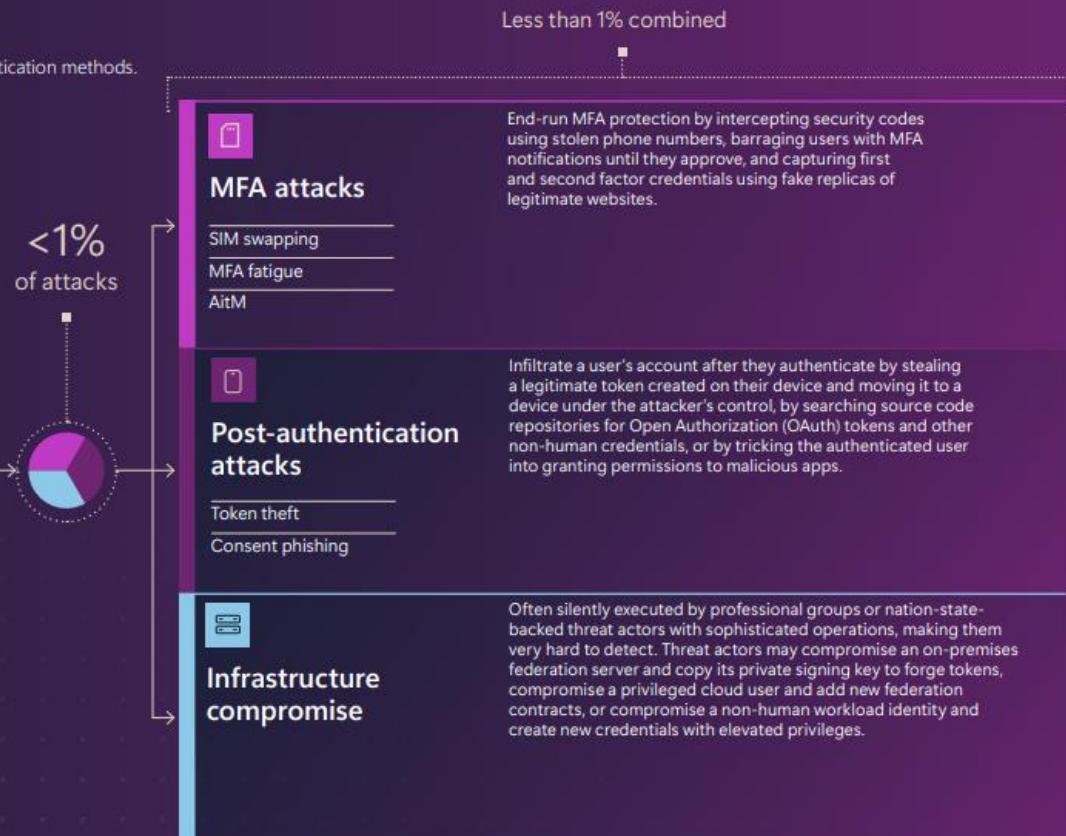
Phishing Resistant MFA Methods

Bad: Password	Good: Password and...	Better: Password and...	Best: Passwordless
123456 qwerty password iloveyou Password1	 SMS  Voice	 Authenticator (Push Notifications)  Software Tokens OTP  Hardware Tokens OTP (Preview)	 Authenticator (Phone Sign-in)  Authenticator (Passkey)  Windows Hello  FIDO2 security key  Certificates

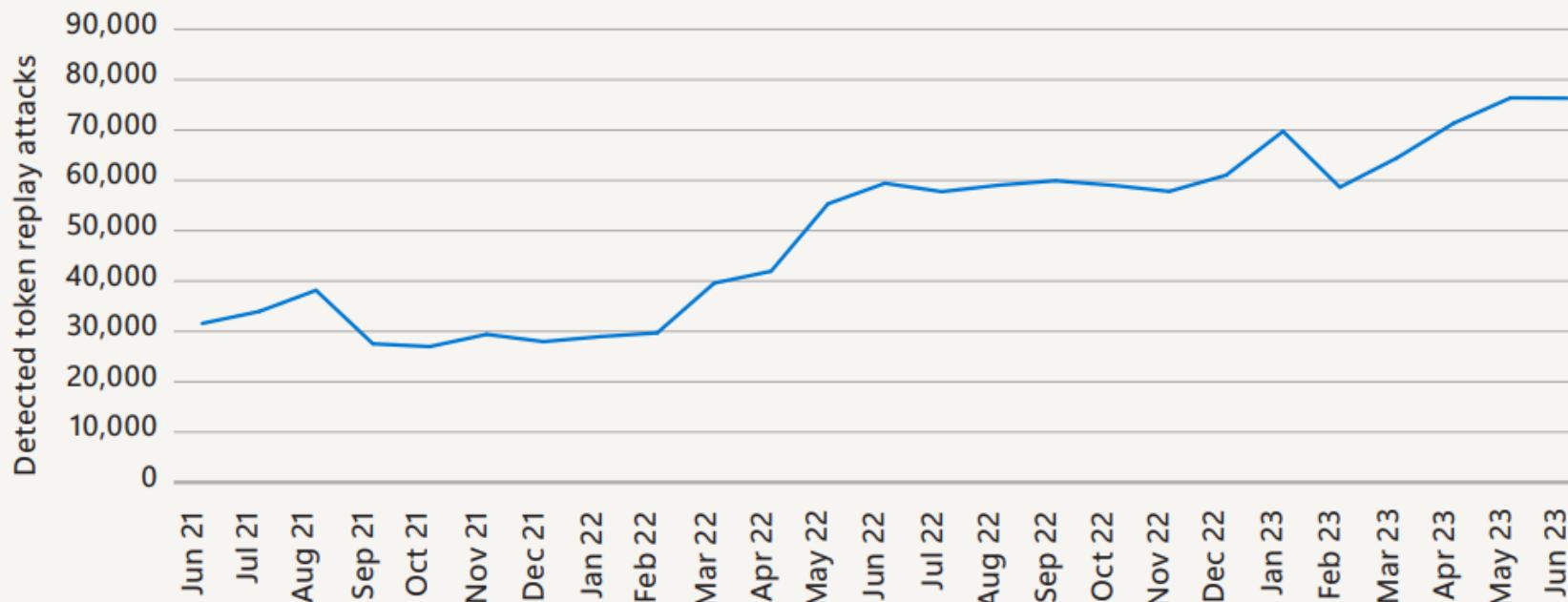
Phishing
Resistant

Identity attacks in perspective

Password-based attacks continue to dominate, but can be thwarted by using strong authentication methods.



Token replay attacks consistently growing since early 2022



Source: Azure Active Directory Identity Protection data

Data from 2 weeks

Ticket Search

Search Filters

+ New Export

	Ticket Number	Title	Description	Contract	Queue	Resources	Role	Status	Priority	Created	Due
<input type="checkbox"/>	T20240913.0024	Verdachte aanmelding door [REDACTED]	Gebruiker: [REDACTED] UserId: ed26bedd-1dfc-440d-9984-377b7c013439 Voer de stappen in de checklist uit:	Support	Security			In progress	P2: High	13/09/2024 09:09	14/09/2024 05:09
<input type="checkbox"/>	T20240912.0035	Verdachte aanmelding door [REDACTED]	Gebruiker: [REDACTED] UserId: 390d3bcf-e117-4ed9-a27d-255ca594c813 Voer de stappen in de checklist uit:	Support	Security			Ready for close	P2: High	12/09/2024 09:05	13/09/2024 05:05
<input type="checkbox"/>	T20240910.0201	Verdachte aanmelding door [REDACTED]	Gebruiker: [REDACTED] UserId: f5c88d7cb-82ae-46e1-bac7b26608b44dc8 Voer de stappen in de checklist uit:	Support	Security			Complete	P2: High	10/09/2024 15:15	11/09/2024 11:15
<input type="checkbox"/>	T20240910.0163	Verdachte aanmelding door [REDACTED]	Gebruiker: [REDACTED] UserId: fd5c2ea5-afac-4c56-8371-e51aa979a996 Voer de stappen in de checklist uit:	Support	Security			Complete	P2: High	10/09/2024 13:35	11/09/2024 09:35
<input type="checkbox"/>	T20240910.0120	Verdachte aanmelding door [REDACTED]	Gebruiker: [REDACTED] UserId: 563c67fc-633f-477f-8ff2-f1a2605b1f55 Voer de stappen in de checklist uit:	Support	Security			Complete	P2: High	10/09/2024 11:51	11/09/2024 07:51
<input type="checkbox"/>	T20240909.0120	Verdachte aanmelding door [REDACTED]	Gebruiker: automation@woordendaal.nl UserId: a6cb4fd4-a94d-4293-eb-a436d127b9a5 Voer de stappen in de checklist uit:	Support	Security			Complete	P2: High	09/09/2024 12:31	10/09/2024 08:31
<input type="checkbox"/>	T20240906.0002	Verdachte aanmelding door [REDACTED]	Gebruiker: [REDACTED] UserId: c03a4f1b-c9e8-4136-a968-70c45ff18416 Voer de stappen in de checklist uit: Er is ingelogd van Santa Venera, Central, MT vanaf een onbekend apparaat, voor de volgende sessie.	Strippenkaart	Support	van de [REDACTED], Keurmerk	SDA/ Maintain	Waiting IT contact	P2: High	06/09/2024 02:31	06/09/2024 22:31
<input type="checkbox"/>	T20240905.0003	Verdachte aanmelding door [REDACTED]	Gebruiker: peter.muyll@ydje.com UserId: 8bdc469b-7cb0-4dd8-96ed57e5fd122 Voer de stappen in de checklist uit:	Support	Security			Complete	P2: High	05/09/2024 02:30	05/09/2024 22:30
<input type="checkbox"/>	T20240905.0001	Verdachte aanmelding door [REDACTED]	Gebruiker: [REDACTED] UserId: a5586255-6099-4178-ac59-378f16ce0b7 Voer de stappen in de checklist uit:	Wijzigingstichting [REDACTED]	Support	(primary)		Complete	P2: High	05/09/2024 00:50	05/09/2024 20:50
<input type="checkbox"/>	T20240904.0070	Verdachte aanmelding door [REDACTED]	Gebruiker: [REDACTED] UserId: cfb08e3b-f596-439b-87c3-7ddc45272ade Melding: Possible Storm-0536 activity detected Severity: High Workspace: emr-01_poc-sentinel Description: Storm-0536 is	Support	Security			Complete	P2: High	04/09/2024 10:28	05/09/2024 06:28
<input type="checkbox"/>	T20240903.0038	Verdachte aanmelding door [REDACTED]	Gebruiker: [REDACTED] UserId: 9d05f054-9c0e-4518-be83-91815663e377 Voer de stappen in de checklist uit:	Support	Support			Complete	P2: High	03/09/2024 09:05	04/09/2024 05:05
<input type="checkbox"/>	T20240902.0075	Verdachte aanmelding door [REDACTED]	Gebruiker: [REDACTED] UserId: 5bd0e2c3-025e-428a-994c-915cf61bdd9c Voer de stappen in de checklist uit:	Strippenkaart	Security			Complete	P2: High	02/09/2024 09:35	03/09/2024 05:35
<input type="checkbox"/>	T20240828.0081	Verdachte aanmelding door [REDACTED]	Gebruiker: [REDACTED] UserId: 356985d6-219f-4fcf-a408-85fe40074611 Voer de stappen in de checklist uit:	Support	Security	[REDACTED] (primary)	SDA/ Maintain	Complete	P2: High	28/08/2024 10:52	29/08/2024 06:52
<input type="checkbox"/>	T20240827.0172	Verdachte aanmelding door [REDACTED]	Gebruiker: [REDACTED] UserId: d0042397-32de-4148-a157-73ba0018a200 Voer de stappen in de checklist uit:	Support	Security			Complete	P2: High	27/08/2024 15:47	28/08/2024 11:47
<input type="checkbox"/>	T20240821.0181	Verdachte aanmelding door [REDACTED]	Gebruiker: [REDACTED] UserId: a5ee893-805c-4d5e-8188-d6aef2aa2186f Voer de stappen in de checklist uit:	Support	Support	[REDACTED] (primary)	SDA/ Maintain	Complete	P2: High	21/08/2024 23:19	22/08/2024 19:19
<input type="checkbox"/>	T20240820.0166	Verdachte aanmelding door [REDACTED]	Gebruiker: [REDACTED] UserId: 0011768d-fa8e-4b10-b28c-27a81d4fa81 Voer de stappen in de checklist uit:	Support	Support	[REDACTED] (primary)	SDA/ Maintain	Complete	P2: High	20/08/2024 14:08	21/08/2024 17:08

1 - 100 of 162 (0 selected)

< 1 2 > 100 rows per page

Sentinel Fusion



Microsoft Sentinel Gisteren 22:07

Preview: Possible multistage attack activities detected by Fusion

Severity: High

Workspace: soli1-proxsys-sentinel

Description: This Fusion incident triggered by our machine learning model correlates anomalous signals and suspicious activities that are potentially associated with multistage attacks on User: ed26bedd-1dfc-440d-9984-377b7c013439 and on IP: 67.182.70.129. We recommend that you investigate all alerts and/or anomalies included in this incident to understand the full chain of attack and take immediate actions to remediate.

For more information about this detection, please visit <https://aka.ms/SentinelFusion>



What is Microsoft advising?

The image shows a screenshot of a Microsoft Security blog post. At the top left is the Microsoft logo and navigation links for Microsoft Security, Solutions, Products, Services, Partners, Resources, and More. On the right are links for All Microsoft, Search, Light/Dark mode, and a search bar labeled "Search the blog". Below the header is a photograph of two men in an office setting, one looking at a laptop screen. The main content area has a blue header with the title "Detecting and mitigating a multi-stage AiTM phishing and BEC campaign" and a subtitle "By Microsoft Threat Intelligence". The text below the title discusses a multi-stage adversary-in-the-middle (AiTM) phishing and business email compromise (BEC) attack against banking and financial services organizations. It mentions the attack originated from a compromised trusted vendor and transitioned into a series of AiTM attacks and follow-on BEC activity spanning multiple organizations. The text highlights the complexity of AiTM and BEC threats, which abuse trusted relationships between vendors, suppliers, and other partner organizations with the intent of financial fraud. At the bottom left, there are social sharing icons for Facebook, Twitter, and LinkedIn, along with links for Microsoft Defender for Cloud Apps, Microsoft Defender for Endpoint, and Microsoft Defender for Office 365. A "more" link is also present. The bottom right corner features a blue decorative graphic with a grid pattern.

June 8, 2023

[f](#) [X](#) [in](#)

Microsoft Defender for Cloud Apps

Microsoft Defender for Endpoint

Microsoft Defender for Office 365

[more](#)

Microsoft Defender Experts uncovered a multi-stage adversary-in-the-middle (AiTM) phishing and business email compromise (BEC) attack against banking and financial services organizations. The attack originated from a compromised trusted vendor and transitioned into a series of AiTM attacks and follow-on BEC activity spanning multiple organizations. This attack shows the complexity of AiTM and BEC threats, which abuse trusted relationships between vendors, suppliers, and other partner organizations with the intent of financial fraud.

[Detecting and mitigating a multi-stage AiTM phishing and BEC campaign | Microsoft Security Blog](#)

WHAT is NCSC saying?



Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

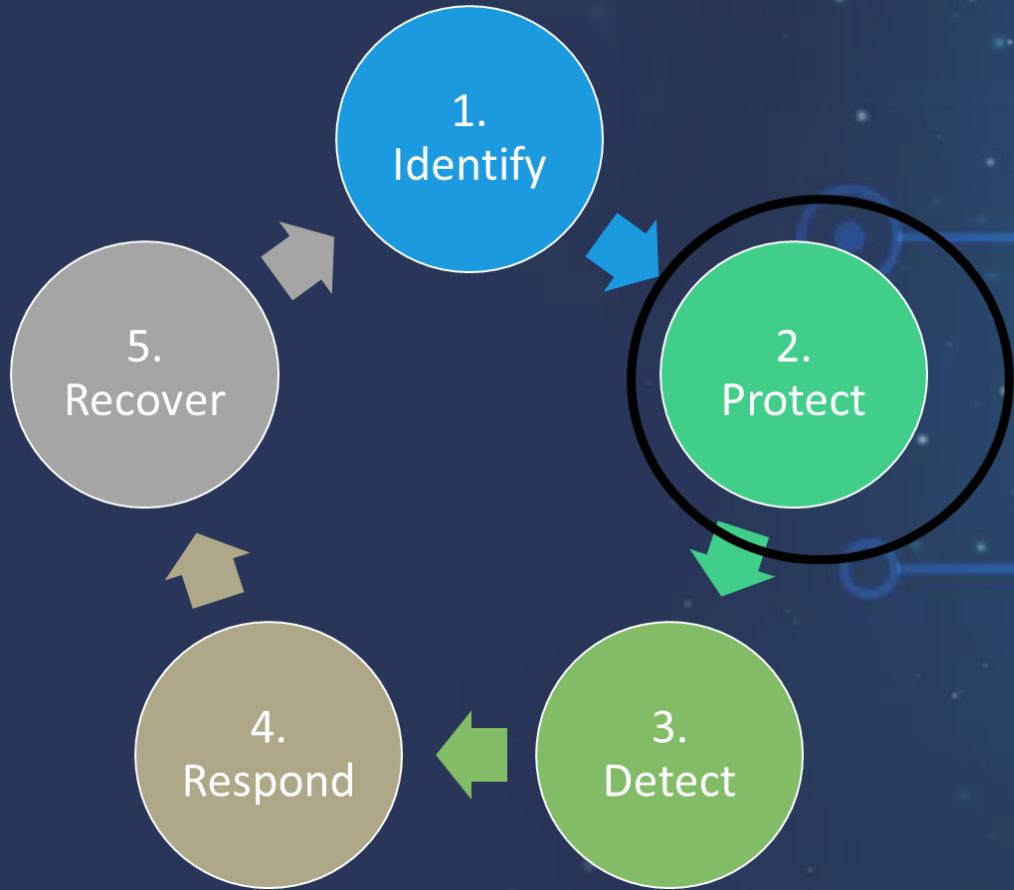
NCSC CTI-Report

Waargenomen Adversary-in-the-Middle-
phishingaanvallen op Nederlandse organisaties

Publicatiedatum: 30-1-2025



In het najaar van 2024 heeft het NCSC meerdere meldingen van phishing-e-mails ontvangen waarbij een Adversary-in-the-Middle-techniek (AiTM) wordt toegepast. Deze techniek is gericht op het bemachtigen van inloggegevens en sessiecookies waarmee kwaadwillenden toegang tot gebruikersaccounts verkrijgen. De verkregen toegang kan vervolgens worden misbruikt voor het verkrijgen van gevoelige bedrijfsinformatie of het uitvoeren van verdere aanvallen.



Protect – phishing resistant MFA

- Certificate Based Authentication
- Passkeys/FIDO security key
- Windows Hello or Business/macOS Platform SSO

Demo 2: Adversary in the Middle



With hardened Identity, AiTM is mitigated

Demo with Fido Security key

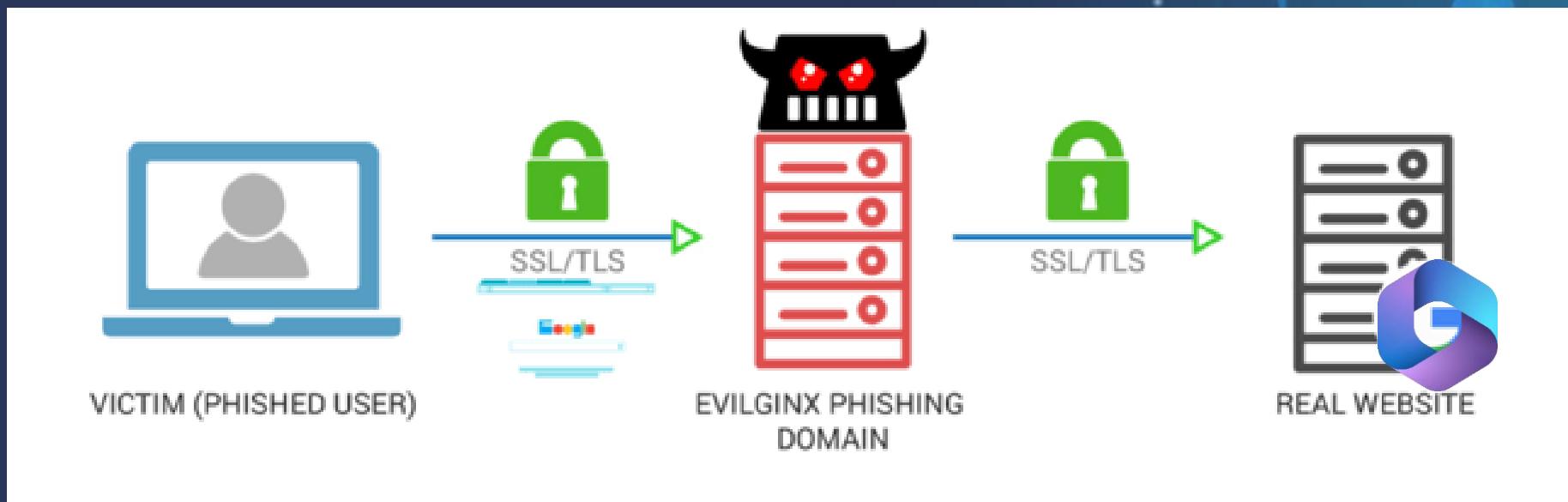
Pro/Cons

- Certificate Based Authentication
 - Issue on mobile especially BYOD scenarios
- Passkeys/FIDO security key
 - Passkeys (now GA)
 - FIDO key support for mobile
 - Complex process onboarding/offboarding and lost
- Windows Hello or Business
 - Windows only
 - Platform SSO (macOS)



Protect – CA options

- Allow only managed devices
- Allow only public IPs from your country
- Use Microsoft Entra Global Secure Access (GSA)/Compliant Networks



Demo 3



Part 1:

Block and allow specific IP ranges

Part 2:

Allow only managed devices

Pro/Cons

- During holiday season many changes
- Not working for 4G/5G internet (roam home)
- BYOD isn't possible anymore

Protect – CA options with P2

- Block Risky Sign ins (Risk adaptive access)
- Token Protection

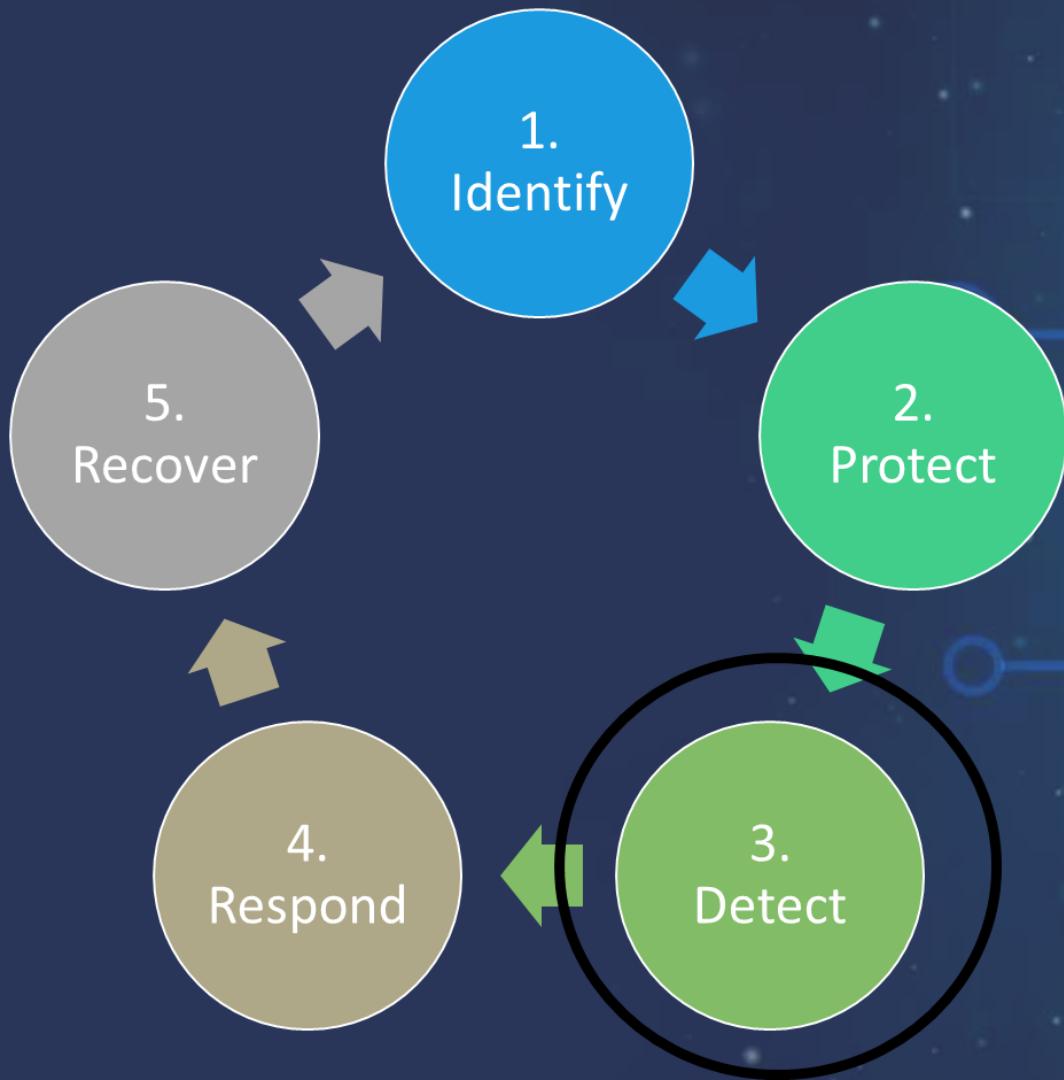
[Token protection in Microsoft Entra Conditional Access](#)
- Microsoft Entra ID | Microsoft Learn

Demo 4



Part 1:
Risky Sign in CA policy

Part 2:
(new) Token Protection Policy



Detect – free options

- M365 Lighthouse
- Powershell script
- Sentinel



M365 Lighthouse

Microsoft 365 Lighthouse

eloef-admin@proxsys.net
PROXSYS® (PROXSYS.ONMICROS..)

- Home
- Alerts
- Tenants
- Users
 - Account management
 - Risky users
 - Multifactor authentication
 - Self-service password reset
- Devices
- Apps
- Quarantined messages
- Deployment
- Service health
- Audit logs
- Permissions
- Sales Advisor (Project Orl...

Home > Risky users

Risky users

Tenants: All

Risk last updated: All

View risky users for all your managed tenants. Reset passwords for risky users to mitigate the risk. It may take a while for the risk status to be updated.

To investigate risk detections for a user, the tenant should have a license of Microsoft Entra Identity or above.

[Learn how to investigate risk](#)

Confirmed compromised | 1 At risk | 551 Remediated | 2656 Dismissed | 3363

[Export](#) [Refresh](#) [Confirm user\(s\) compromised](#) [Dismiss user\(s\) risk](#) [Reset password](#) [Block sign-in](#) 6598 users Search by name

Filters: [Risk state: Any](#) [User status: Any](#) [Users with risk detections available: All](#)

<input type="checkbox"/>	Name ↑	Username	Tenant	Risk state	Details
<input type="checkbox"/>	Stijn PowerAuthmate	powerauthmate@t...d.nl	Value Added Grouping Al... European Merchant Services B.V.	Remediated	View risk detections
<input type="checkbox"/>	Corinne Pauline Envalue	lot.pauline.envalue@...l.com	Value Added Grouping Al... European Merchant Services B.V.	Remediated	View risk detections
<input type="checkbox"/>	Reinier Valkhouwer	reinier.valkhouwer@...ay.eu	Value Added Grouping Al... European Merchant Services B.V.	Remediated	View risk detections
<input type="checkbox"/>	Andrea van Leeuwen	andrea.vanleeuwen@...ay.eu	Value Added Grouping Al... European Merchant Services B.V.	Remediated	View risk detections
<input type="checkbox"/>	Bart Bekker	bart.bekker@...o.nl	Value Added Grouping Al... Europele Operatie voor 030...	Remediated	View risk detections
<input type="checkbox"/>	Alma Verheijen	alma.verheijen@...ijin.nl	Value Added Grouping Al... Vereniging	Remediated	View risk detections

Microsoft Sentinel



...



X

PROXSYS* (PROXSYS.onmicrosoft.com)

[+ Create](#) [Manage view](#) [Refresh](#) [Export to CSV](#) [Open query](#) | [View incidents](#) Filter for any field...Subscription equals **16 of 98 selected**Resource group equals **all** Location equals **all**

Add filter

Showing 1 to 16 of 16 records.

<input type="checkbox"/> Name	Resource group	Location
1-proxsys-sentinel	proxsys-sentinel-rg	West Europe
2-proxsys-sentinel	proxsys-sentinel-rg	West Europe
3-proxsys-sentinel	proxsys-sentinel-rg	West Europe
-proxsys-sentinel	proxsys-sentinel-rg	West Europe
-proxsys-sentinel	proxsys-sentinel-rg	West Europe
1-proxsys-sentinel	proxsys-sentinel-rg	West Europe
inte2-proxsys-sentinel	proxsys-sentinel-rg	West Europe

No grouping

List view

Subscription ↑↓ Directory ↑↓

4fig1 - Proxsys Sentinel Subsc...	Limborgh & ...
abal1 - Proxsys Sentinel Subsc...	
acco1 - Proxsys Sentinel Subsc...	nics bv
amar1 - Proxsys Sentinel Subsc...	Rivierenland
anbo1 - Proxsys Sentinel Subsc...	niek B.V.
atro1 - Proxsys Sentinel Subsc...	
bail1 - Proxsys Sentinel Subsc...	
beco1 - Proxsys Sentinel Subsc...	
bela1 - Proxsys Sentinel Subsc...	
bokh1 - Proxsys Sentinel Subsc...	
boro2 - Proxsys Sentinel Subsc...	
boro3 - Proxsys Sentinel Subsc...	
city1 - Proxsys Sentinel Subsc...	
clai1 - Proxsys Sentinel Subsc...	
conc1 - Proxsys Sentinel Subsc...	
inte2 - Proxsys Sentinel Subsc...	

Microsoft Sentinel | Incidents

Search X <<

+ Create incident (Preview)

Refresh

Last 24 hours

Actions

Delete

Columns

Guides & Feedback

Threat management

Incidents

17
Open incidents

17
New incidents

0
Active incidents

Open incidents by severity

High (0)

Medium (1)

Search by ID, title, tags, owner or product

Severity : All

Status : 2 selected

More (5)

Auto-refresh incidents

Severity ↑↓

Title ↑↓

Medium

Risky User [REDACTED]

Low

Application Proxsys - CDI M...

Status ↑↓

Owner

New

[REDACTED]

Sentinel automation

 Microsoft Sentinel | Automation ...
Selected workspace: 'mssp-sentinel'

Search Create Refresh Automation health workbook Edit Enable Move up Move down ...

General

-  Overview (Preview)
-  Logs
-  News & guides
-  Search

Threat management

Content management

Configuration

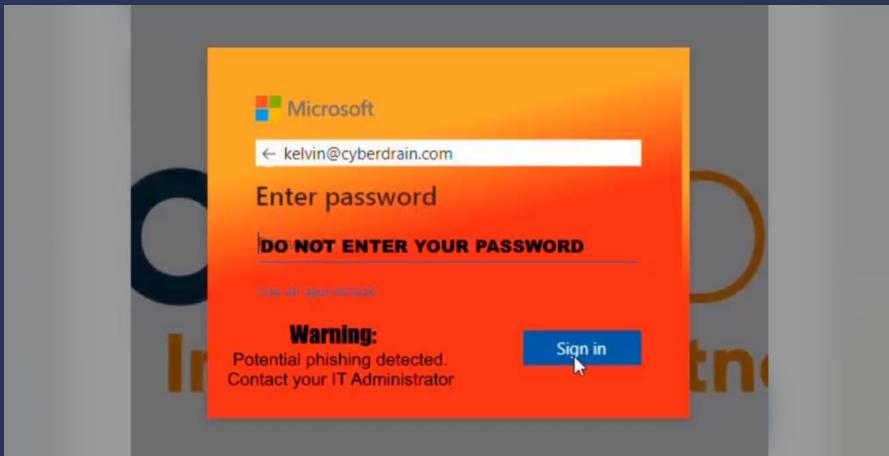
-  Workspace manager (Preview)
-  Data connectors
-  Analytics

4 Automation rules 3 Enabled rules 5 Enabled playbooks More content at Content Hub

Automation rules Active playbooks Playbook templates (Preview)

 Search	Add filter				
Order	Display name	Trigger	Analytic rule names	Actions	Ex
<input type="checkbox"/>	100 Proxsys - Auto close informational	 Incident created	All	Change status, ...	In
<input type="checkbox"/>	200 Proxsys - Incident Automation Rule	 Incident created	All	Run playbook '...'	In
<input type="checkbox"/>	300 Proxsys - Create risky user ticket	 Incident created	All	Run playbook '...'	In
<input type="checkbox"/>	400 Proxsys - Create MDE ticket	 Incident created	All	Run playbook '...'	In

Demo 5:



Inform your users with a simple CSS Trick

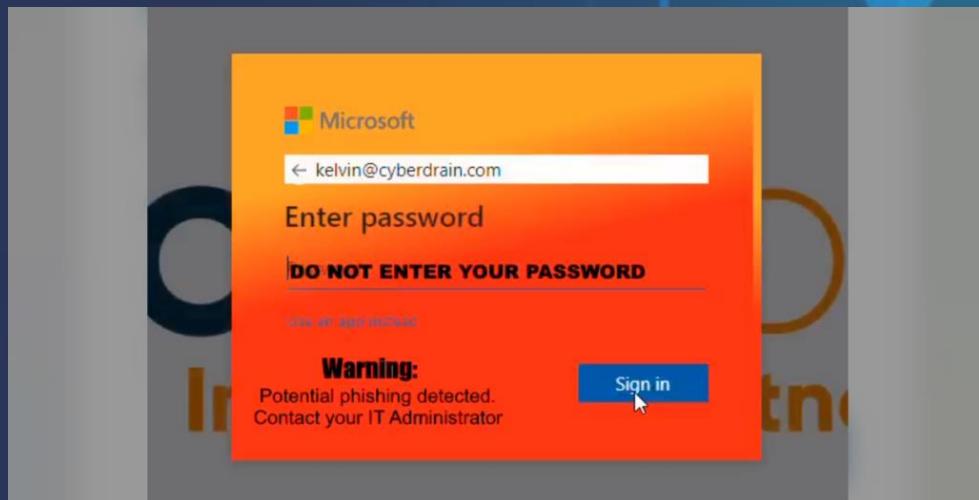
Change logi CSSs

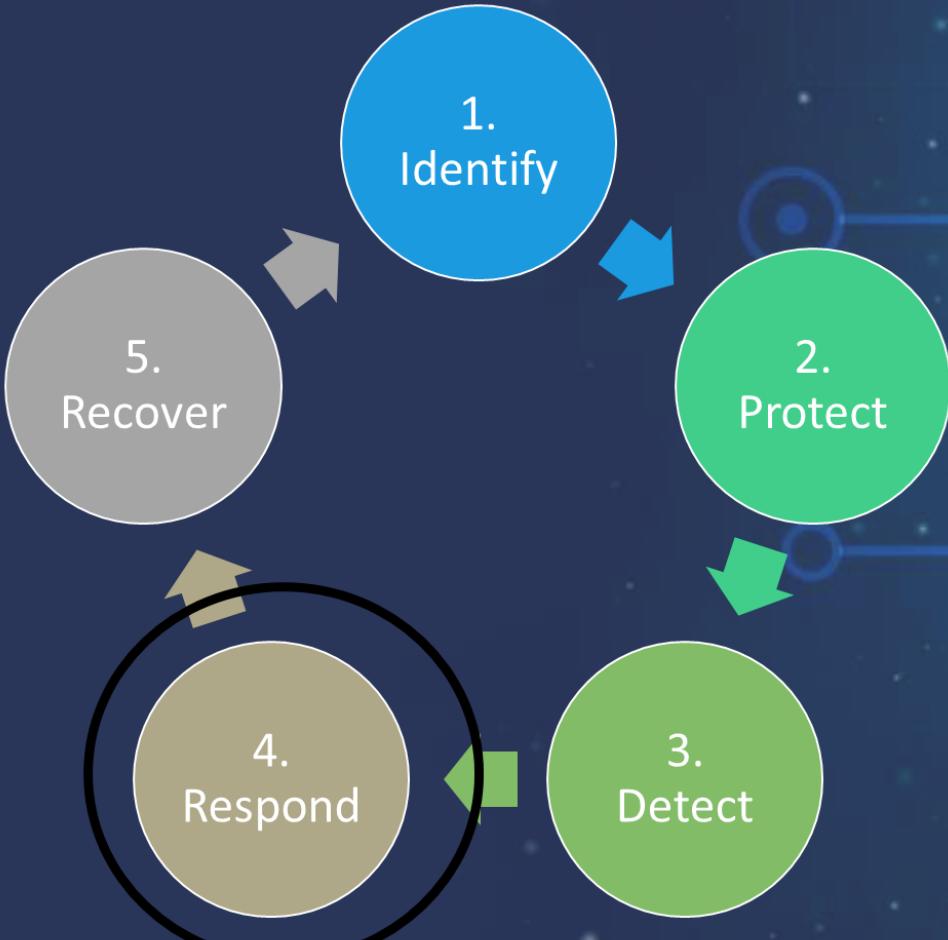
Cipp.app | zolder.io

Change the CSS

Using honeytokens to detect (AiTM) phishing attacks on your Microsoft 365 tenant – Zolder B.V.

Be careful with modifying CSS, it can also break stuff !!





Respond – What to do ?

- Revoke session
- Check for extra MFA methods
- Check Sign in Logs

Respond

Step 1: revoke sessions

Step 2: check for logged in sessions

Step 3: disable account

Step 4: reset password

Step 5: collect all audit logs

Step 6: check for extra MFA methods

Step 7: check for mail forwards

Step 8: take the phising mail

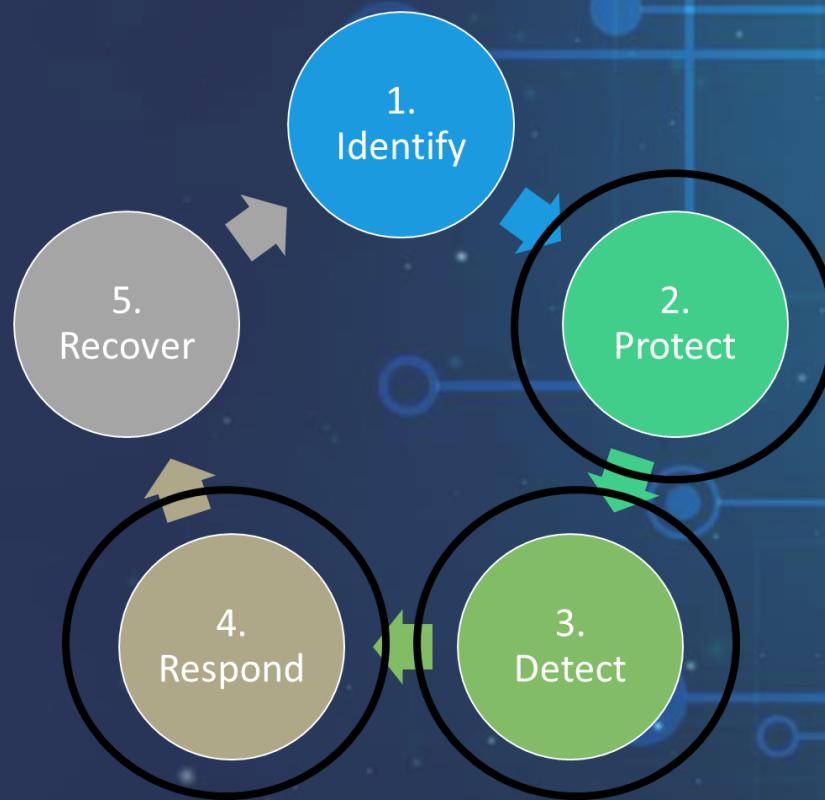
Step 9: 4 eyes with security cons

Checklist (11/11) [Hide Completed Items](#)

- Trek alle sessies per direct in ! 17/09/2024 12:50 by Koen van Burken
- Onderzoek de melding en volg de rest van de checklist wanneer de aanmelding malafide was ! 17/09/2024 12:50 by Koen van Burken
- Schakel het account van de gebruiker uit (let op dat in geval van aad connect je de on-premise user uitschakelt) ! 17/09/2024 12:52 by Koen van Burken
- Reset het wachtwoord van de gebruiker ! 17/09/2024 13:40 by Kevin van de Luijtgaarden
- Verzamel en onderzoek de Azure en M365 audit logs van de gebruiker (is er bijvoorbeeld een extra authenticator toegevoegd en/of zijn er andere zaken geopend?) ! 17/09/2024 13:54 by Kevin van de Luijtgaarden
- Controleer de mailbox op ongewenste regels (bijv: doorsturen/verwijderen van e-mail) ! 17/09/2024 13:54 by Kevin van de Luijtgaarden
- Probeer het originele phishing bericht veilig te stellen (inclusief mail headers) ! 17/09/2024 13:46 by Kevin van de Luijtgaarden
- Verzamel en onderzoek e-mail logs van de gebruiker (zijn er phishing berichten uit naam van de gebruiker gestuurd) ! 17/09/2024 13:46 by Kevin van de Luijtgaarden
- Zorg er voor dat ontvangers in het geval dat er phishing is verstuurd via de getroffen mailbox genotificeerd worden ! 17/09/2024 13:54 by Kevin van de Luijtgaarden
- Indien er geen MFA oplossing actief is dient dit verkocht/aangezet te worden ! 17/09/2024 13:40 by Kevin van de Luijtgaarden
- Overleg met Security specialist/CISO of er aan de hand van de verzamelde informatie verdere acties nodig zijn voor het SI gesloten kan worden ! 17/09/2024 14:27 by Koen van Burken

Take Away

- Summary and takeaways
- Protect | Detect | Respond



THANK YOU