



Defending Against **Storm-1811**

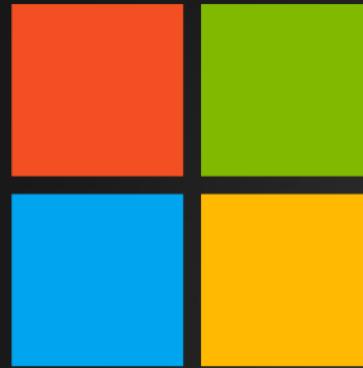
Insights from a real-time Attack Mitigation



Derk van der Woude
CTO @ Nedscaper

Thanks

Some research was done in cooperation with **Microsoft Security Research**



Microsoft Security



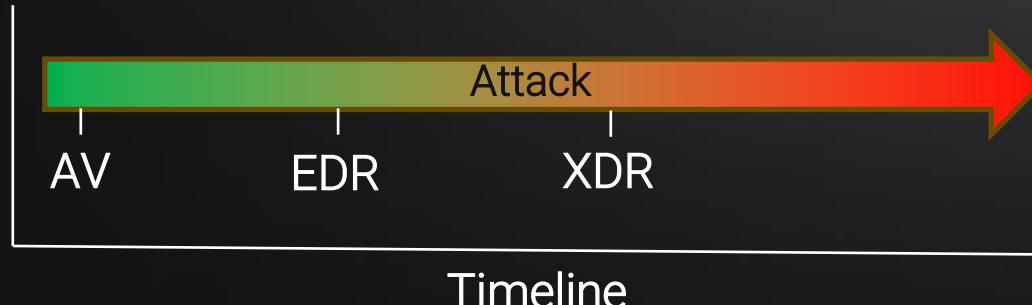
Big Thanks 😊

Disclaimer: the difference between AV and EDR/XDR

AV - AntiVirus blocks a threat(s) directly via signature detection

EDR - Endpoint Detection & Response detects malicious behavior (*compared to the baseline*) on the endpoint and blocks the threat(s)

XDR - eXtenderd Detection & Response detects the attack chain (multi-source) from '*patient-0 to the breach*' and blocks well known threats (e.g. BEC/AiTM & HumOR)



Example:

- Mimikatz install is AV detection
- Mimikatz execution is EDR detection
- Mimikatz DCsync to AD is XDR detection

Overview of the Storm-1811 Threat Actor

Very Sophisticated & Financially Motivated Cybercriminal Group

[Research](#) [Threat intelligence](#) [Microsoft Defender](#) [Social engineering / phishing](#) · 10 min read

Threat actors misusing Quick Assist in social engineering attacks leading to ransomware

June 2024 update: At the end of May 2024, Microsoft Threat Intelligence observed Storm-1811 using Microsoft Teams as another vector to contact target users. Microsoft assesses that the threat actor uses Teams to send messages and initiate calls in an attempt to impersonate IT or help desk personnel. This activity leads to Quick Assist misuse, followed by credential theft using EvilProxy, execution of batch scripts, and use of SystemBC for persistence and command and control.

Likely  Russia and state-sponsored

Typhoon	Sandstorm	Sleet	Dust	Cyclone
China	Iran	North Korea	Turkey	Vietnam
Hail	Tempest	Tsunami	Flood	
Lebanon	South Korea	Financially motivated	Influence operations	
Groups in development				

Microsoft Threat Actor Naming



Defender XDR | Threat Intel Profile TTPs & IOCs

威胁行动者 December 20, 2023

Storm-1811

Share ▾

Description TTPs Indicators (41)

Description TTPs Indicators (41)

Initial access

At the end of December 2023, Microsoft Threat Intelligence observed a new ZLoader malvertising campaign after a long hiatus since the takedown action by Microsoft in April 2022. In this recent campaign, ZLoader was distributed through malicious advertisements spoofing legitimate software downloads. The campaign operators behind ZLoader infections monetize their access to domain-joined devices by selling access-as-a-service to other groups, including ransomware affiliates. In addition to other capabilities, ZLoader can be used to download additional malicious payloads, like Cobalt Strike Beacon. Microsoft identified instances where ZLoader infections have led to Black Basta ransomware deployment by Storm-1811.

Snapshot

The actor that Microsoft tracks as Storm-1811 is a financially motivated cybercriminal group known to deploy Black Basta ransomware in opportunistic attacks. For initial access, the actor has been observed abusing the client management tool Quick Assist to target users in social engineering attacks in April 2024. These attacks have led to malware like Qakbot and Cobalt Strike, followed by Black Basta ransomware deployment. Storm-1811 also uses remote monitoring and management (RMM) tools like ScreenConnect, Syncro Agent, and NetSupport Manager (also referred to as NetSupport RAT) to conduct lateral movement within the compromised environment, download and install additional malware, and launch arbitrary commands. The actor has also been observed dumping lsass.exe to access credentials. For ransomware deployment, Storm-1811 primarily uses PsExec, a legitimate tool from the Sysinternals suite, to deploy the ransomware payload remotely.

Overview of the Storm-1811 Attack Techniques



Attacker

AD Certificate Services

Domain Controller

<45:00

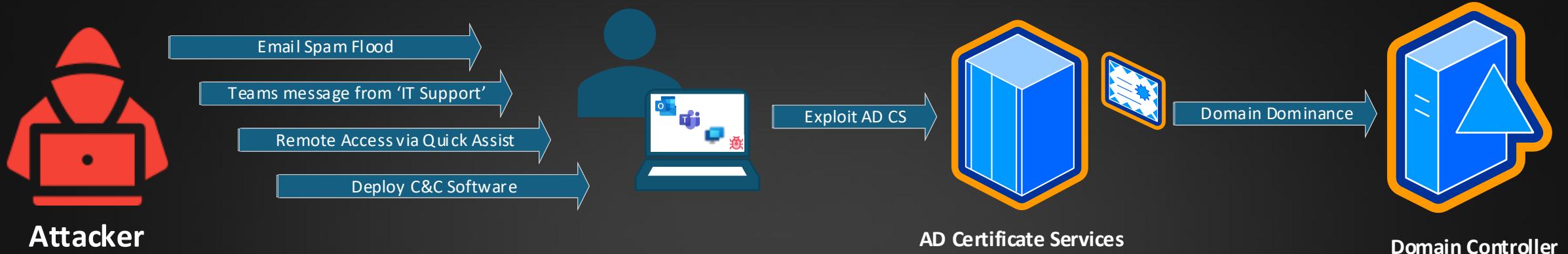
Minutes

Seconds

Attack



Overview of the Storm-1811 Attack Techniques



Attacker

AD Certificate Services

Domain Controller

<45:00

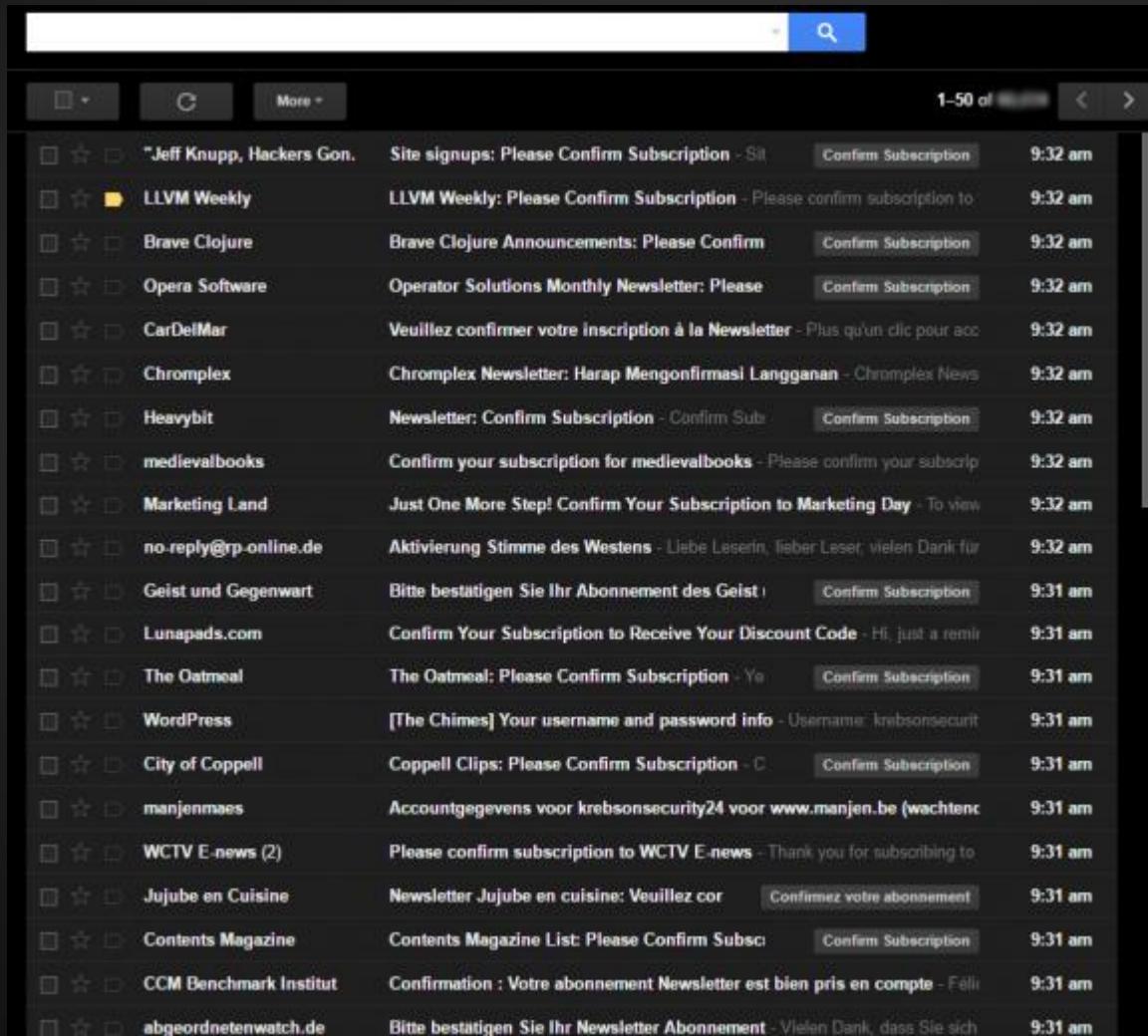
Minutes

Seconds

Attack



E-mail Spam Flood [E-mail Bomb] send hundreds of ‘Spam’ e-mails to a user in a short period of time [10-20 minutes]

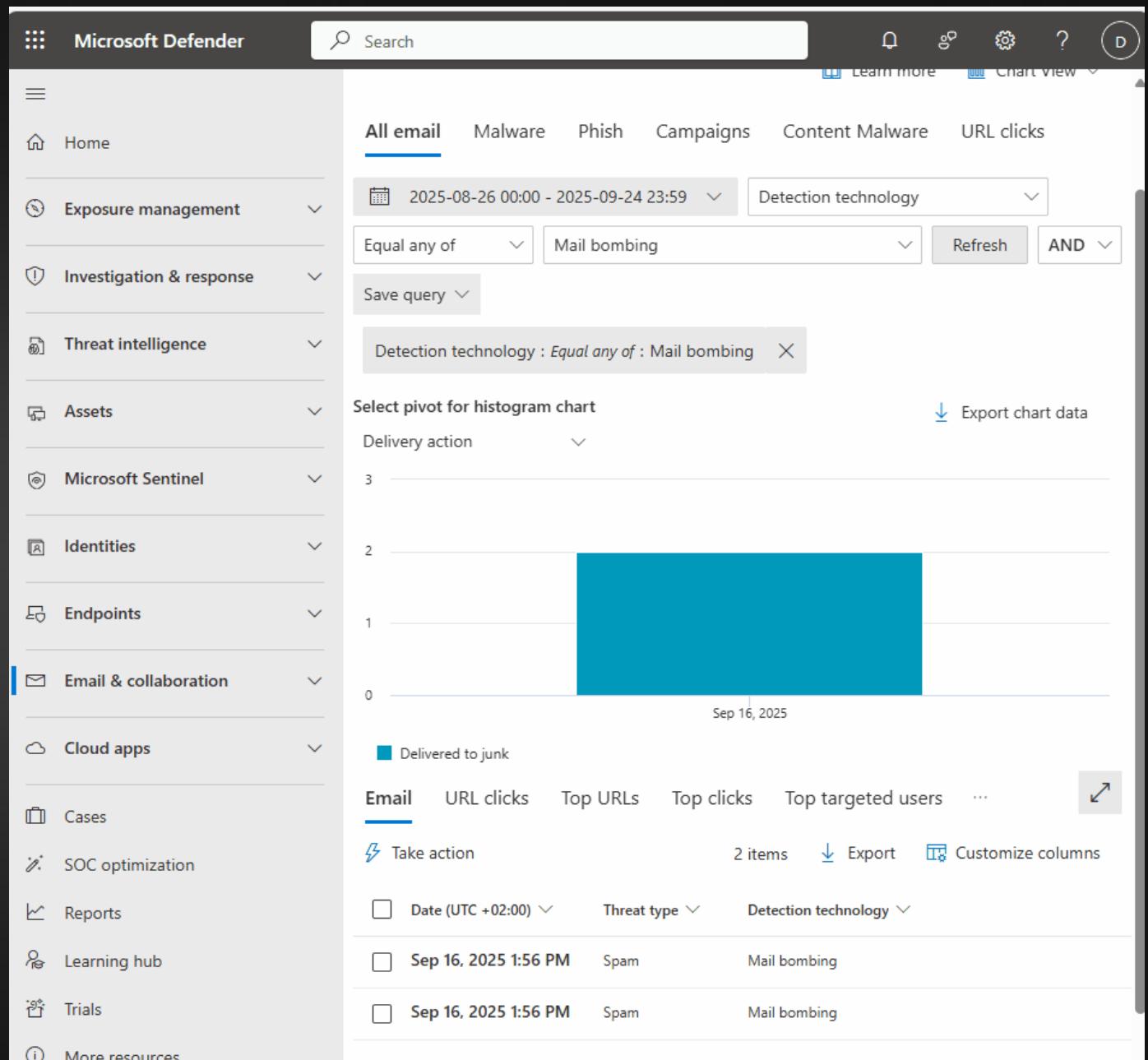


June 2025 UPDATE

Detection by MDO Defender for Office 365

Visible in the Threat Explorer,
Email Entity and Advanced
Hunting

Detection Technology Mail Bombing



Outsourced ‘IT Support’ send a Teams message to the end user to fix the ‘broken’ Spam filter

The image shows a split-screen view. On the left is the Microsoft Teams desktop application. On the right is a web browser window displaying a Microsoft Teams message.

Microsoft Teams (Left):

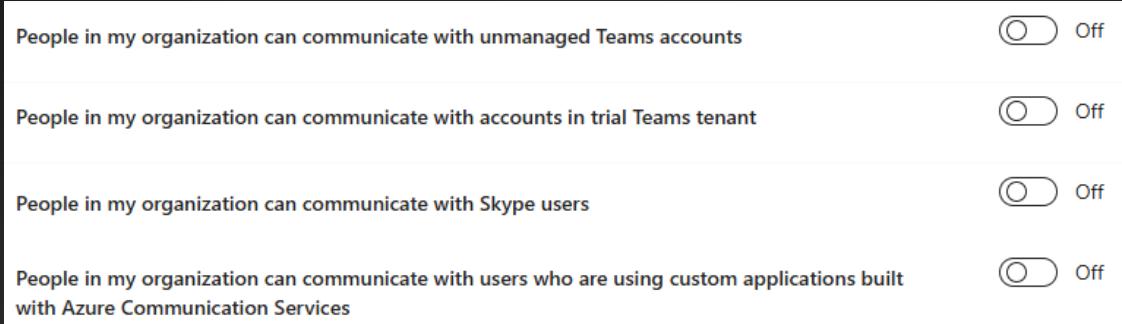
- Sidebar:** Activity (2 notifications), Chat, Teams, Calendar, Calls, Shifts, OneDrive, Apps.
- Chat View:** Recent messages from Copilot, IT Support (itsupport@blue1) at 3:46 PM (This message was deleted, External).

Web Browser (Right):

- Address Bar:** teams.microsoft.com/v2/
- Message Preview:** A Teams message from IT Support (itsupport@blue1) to Derk van der Woude (derk@nedscaper.com). The message content is: "Hello, this is IT Support. We noticed your e-mail spam filter is not working. We want to fix your Spam Filter and make your computer safe again." Below the message are standard Microsoft message reaction icons (smiley face, etc.).

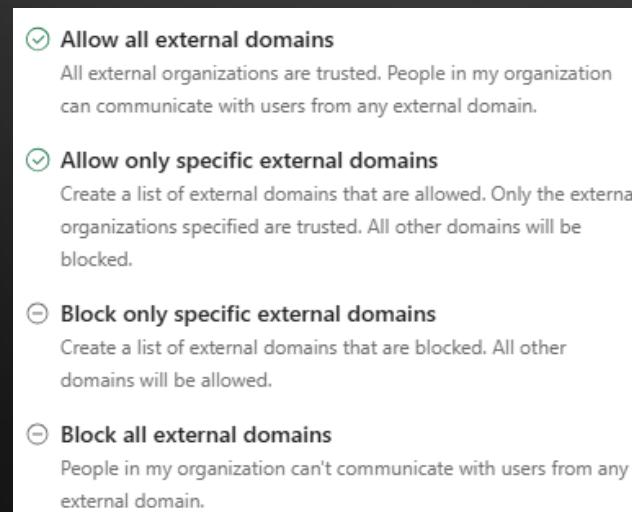
Prevention #1

If not required, Disable the options below in the Teams External Access settings



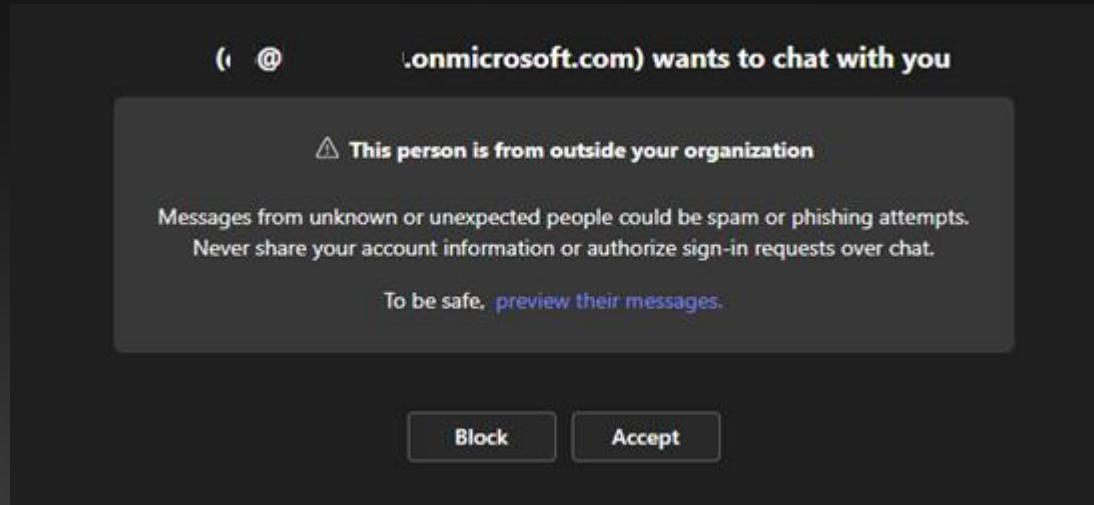
Prevention #2

Microsoft Teams can **allow all (default)** or specific domains, or **block all** or specific domains.



#1 User Awareness is key!!!

IT Support (External)

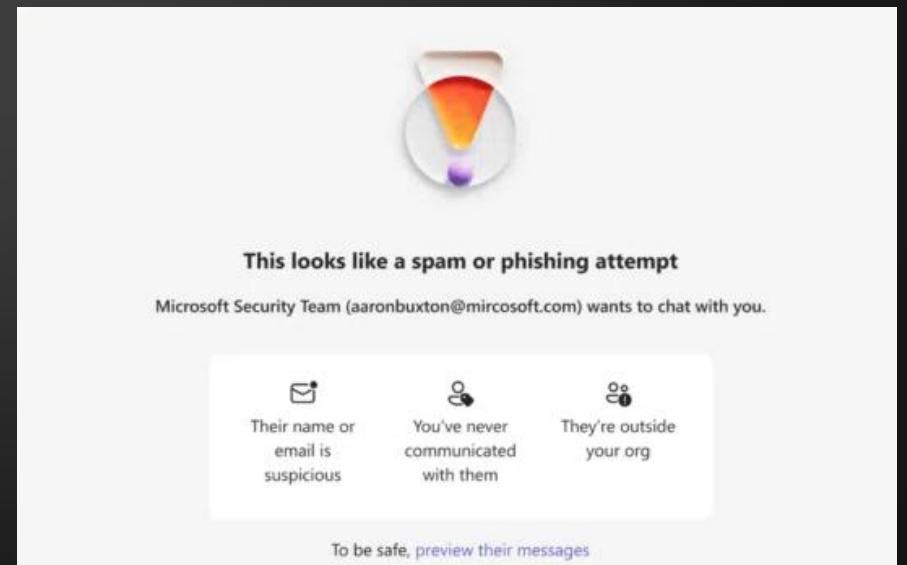
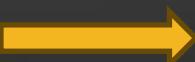



#2 Microsoft Teams: Brand Impersonation Protection for Teams Messaging [Feb-2025]

 Microsoft Teams: Brand Impersonation Protection for Teams Messaging

Identify if an external user is impersonating a brand commonly targeted by phishing attacks, user via Teams messages.

Feature ID: 421190
Added to roadmap: 10/9/2024
Last modified: 11/6/2024
Product(s): Microsoft Teams
Cloud instance(s): Worldwide (Standard Multi-Tenant)
Platform(s): Desktop, Mac
Release phase(s): General Availability



Detection #1 [Microsoft 365 E5]

Microsoft Defender XDR [Defender for Cloud Apps] detects suspicious external Teams messages

 **Suspicious message received in Microsoft Teams from external user**

■■■ Medium | ● Unknown | ● Resolved

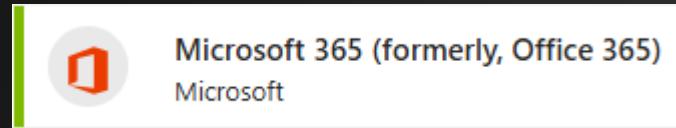
What happened

A user received a suspicious message in Microsoft Teams from an external user. This might indicate an ongoing phishing attempt.

Recommended actions

A. Validate the alert.
1. Inspect whether the user account has been comp...

Detection #2 [Microsoft 365 E3 & Microsoft Sentinel] Microsoft Sentinel detection rule with Severity High Data Connector



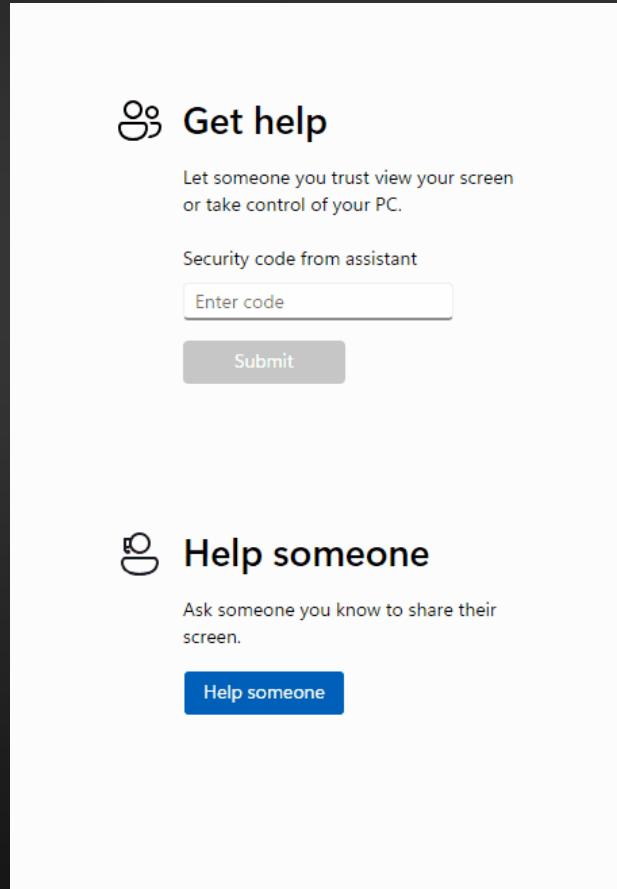
KQL query

```
OfficeActivity
| where RecordType contains "MicrosoftTeams" and Operation contains "ChatCreated"
| where UserId !contains "<tenant>.onmicrosoft.com"
| where UserId contains "onmicrosoft.com"
| project UserId
```

Detection

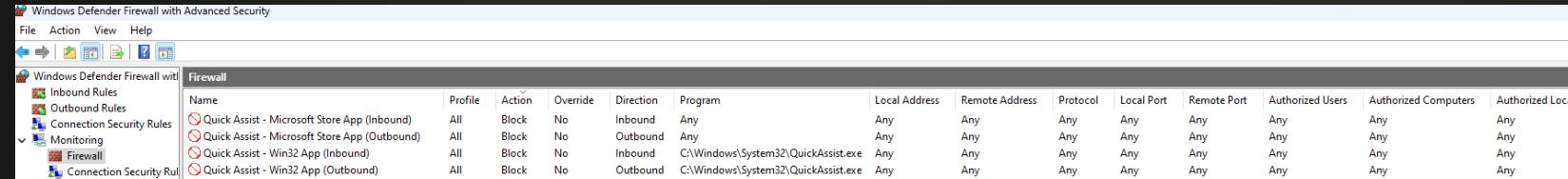
A screenshot of a Microsoft Sentinel incident card. The title is "Malicious Teams Message from External .onmicrosoft.com" with an ellipsis. Below it says "Incident number 1". At the bottom, there are three dropdown menus: "Owner" set to "Unassigned", "Status" set to "New", and "Severity" set to "High".

Quick Assist [standard Microsoft Windows application] is used for **initial access** to the device [domain] to **discover** the environment and install **malicious** software (via DLL Sideload as an example) and ransomware



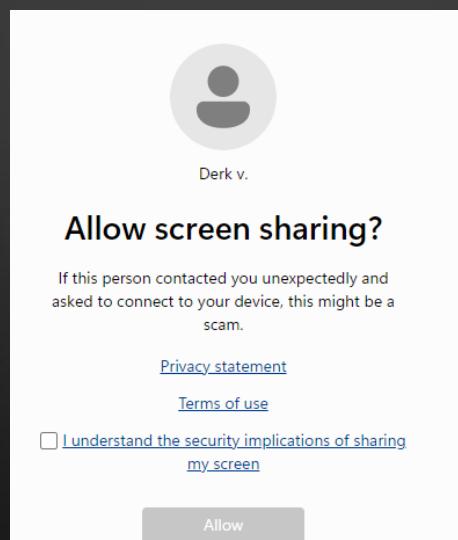
Prevention

Disable Quick Assist or block access from the internet [via FW rules]



User Awareness is key!!!

Again 😊



Detection

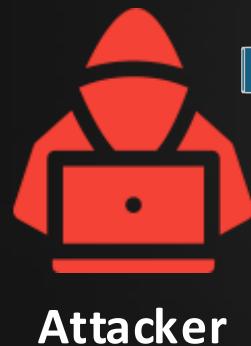
Microsoft Defender XDR [Defender for Endpoint] detects **suspicious** Quick Assist usage on the **managed** Endpoint

The screenshot shows a Microsoft Defender XDR interface titled "Suspicious activity using Quick Assist". A red lightning bolt icon is in the top-left corner. Below it, a legend indicates: "High" (red), "Detected" (red dot), and "Resolved" (green dot). The main pane displays two items under the heading "[20972] quickassist.exe":

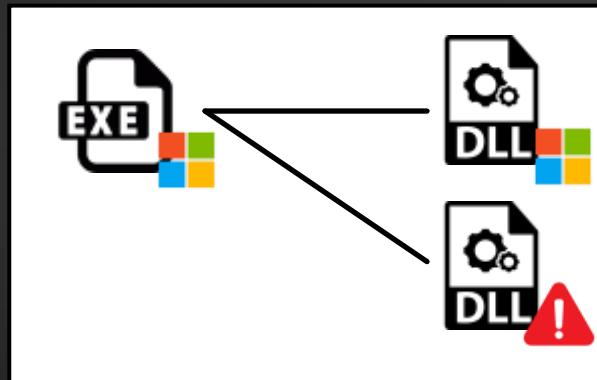
- Suspicious activity using Quick Assist**: High priority, Detected (red dot), Resolved (green dot) (True positive).
- Endpoint attack notifications: Create Process Event**: Medium priority, Detected (red dot), Resolved (green dot) (True positive).

Each item has a blue gear icon and a "..." button.

DLL Sideloaded (also called Living of the Land) is a technique to load malicious .DLL (code) files from a standard Windows Executable.



Launch



DLL search order

Application Directory
C:\Windows\System32
C:\Windows\System
C:\Windows
Current Directory
PATH Variable Directories

Example OneDriveStandaloneUpdater.exe (persistence) which runs every day: Persistence]. Process Monitor [ProcMon] example

The screenshot shows the Process Monitor interface with a list of operations for process ID 29348. The operations involve searching for 'winhttp.dll' in various locations. The results are as follows:

Time ...	Process Name	PID	Operation	Path	Result
20:44:...	OneDriveStand...	29348	CreateFile	C:\Users\DerkvanderWoude\AppData\Local\Microsoft\OneDrive\WINHTTP.dll	NAME NOT FOUND
20:44:...	OneDriveStand...	29348	CreateFile	C:\Windows\System32\winhttp.dll	SUCCESS
20:44:...	OneDriveStand...	29348	QueryBasicInforma...	C:\Windows\System32\winhttp.dll	SUCCESS
20:44:...	OneDriveStand...	29348	CloseFile	C:\Windows\System32\winhttp.dll	SUCCESS

A red box highlights the first four rows of the table, corresponding to the 'Application Directory' entry in the DLL search order list.

DLL search order

Application Directory
C:\Windows\System32
C:\Windows\System
C:\Windows
Current Directory
PATH Variable Directories

A file browser window is overlaid on the Process Monitor window, showing the contents of the 'System32' folder. A red box highlights the 'System32' folder icon. The folder contains two files: 'winfax.dll' and 'winhttp.dll'. The 'winhttp.dll' file is selected and highlighted with a red box.

Prevention

The DLL is loaded in the **context of the executable** (e.g. Administrative Privileges) so **no local admin** for users is key.

From a Microsoft perspective make sure Defender AntiVirus is running

- Real-time-, Cloud-delivered-, Network- and Tamper-Protection

Enable **ASR** (Attack Surface Reduction) rules in Block mode

- Block untrusted and unsigned processes that run from USB
- Block executable files from running unless they meet a prevalence, age, or trusted list criterion

And have a **defence in-depth** strategy

Detection

Microsoft Defender XDR [Defender for Endpoint] detects **DLL Sideload**ing (*and more anomalies*) on the Endpoint

An executable file loaded an unexpected DLL file

⚡ Medium | ● Detected | ● Resolved

[8016] OneDriveStandaloneUpdater.exe -Embedding

⚡ Endpoint attack notifications: Create Process Ev... ■■■ Medium ● Dete... ● Resol... (True positive) ...

[8016] OneDriveStandaloneUpdater.exe loaded image winhttp.dll

⚡ An executable file loaded an unexpected DLL ... ■■■ Medium ● Dete... ● Resol... (True positive) ...

OneDriveUpdate.lnk was created by OneDriveStandaloneUpdater.exe under the user startup folder

⚡ An uncommon file was created and added to ... ■■■ Medium ● Dete... ● Resol... (True positive) ...

[8016] OneDriveStandaloneUpdater.exe created file OneDriveUpdate.lnk

⚡ An uncommon file was created and added to ... ■■■ Medium ● Dete... ● Resol... (True positive) ...

OneDriveStandaloneUpdater.exe has initiated a connection to 195.123.233.148

Command & Control

Signer
⚠ Unsigned file

PE metadata

Original name	Company
MFC_CalculatorApp.exe	TODO: <Company name>

Product
TODO: <Product name>

Description
MFC_CalculatorApp

File prevalence

Organization devices	Organization cloud apps
2	0
Worldwide devices	
3	

Observed devices (last 30 days)

Time

Dec 11, 2024 5:20:05 PM

Remediation

Isolate the device (*and disable the user*) to prevent the attack from spreading (**lateral movement**)

Device Inventory

The screenshot shows the Microsoft Defender for Cloud Device Inventory interface. At the top, a callout box highlights "1 OT devices are not protected" with a note to onboard devices. A message about transient devices being filtered is also present. Below, a summary bar shows the total number of devices (4) and their categories: Critical assets (0), High risk (0), High exposure (2), Not onboarded (3), and Newly discovered (0). The "All devices" tab is selected. The main table lists four devices:

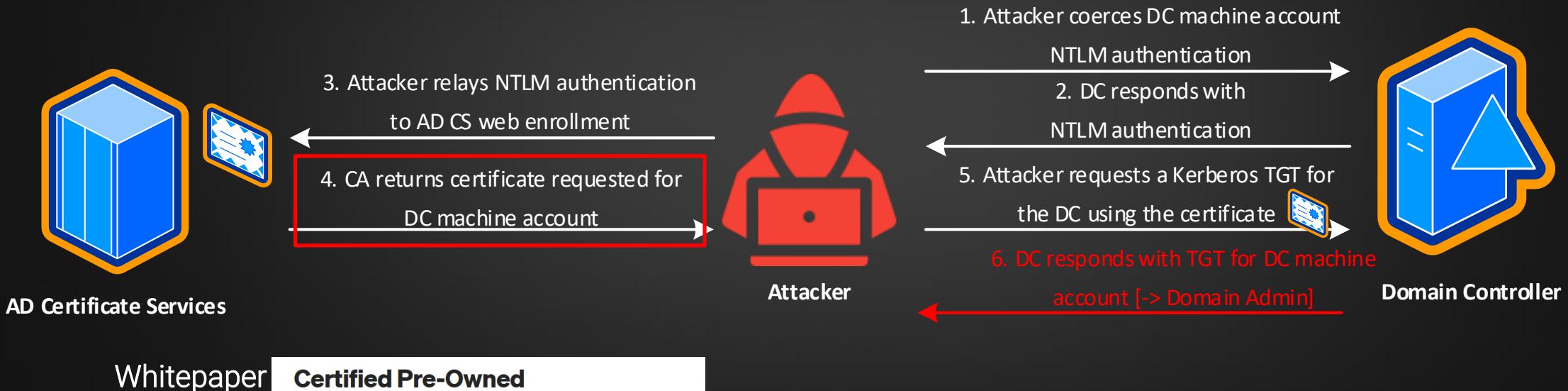
Name	IP	Device category	Device type	Device AAD id	Risk level	Exposure level	Onboarding status	Discovery sources	Tags	Device role
wsrv2016-srv01.s3curity.local	192.168.178.70	Computers and ...	Server		■■■■ No known ...	▲ High	● Can be onboarded			U
WSRV2016-DC02.s3curity.local	192.168.178.11	Computers and ...	Server		■■■■ No known ...	No data available	● Can be onboarded			U
WSRV2016-DC01.s3curity.local	192.168.178.10	Computers and ...	Server		■■■■ No known ...	No data available	● Can be onboarded			Domain Controller
wsrv2022-srv01.s3curity.local	192.168.178.20	Computers and ...	Server		■■■ Medium	▲ High	✓ Onboarded			M

To the right, a terminal window shows a command line with "C:\Windows\system32\cmd.exe" and "C:\>ping 8.8.8.8 -t".



AD CS (Certificate Services) can be vulnerable to attacks.

For example, ESC8 (*insecure ADCS certificate enrollment IIS endpoints*) can be abused by a **NTLM Relay Attack** on the **HTTP Web enrollment endpoint** which uses **NTLM as authentication method**.



Whitepaper

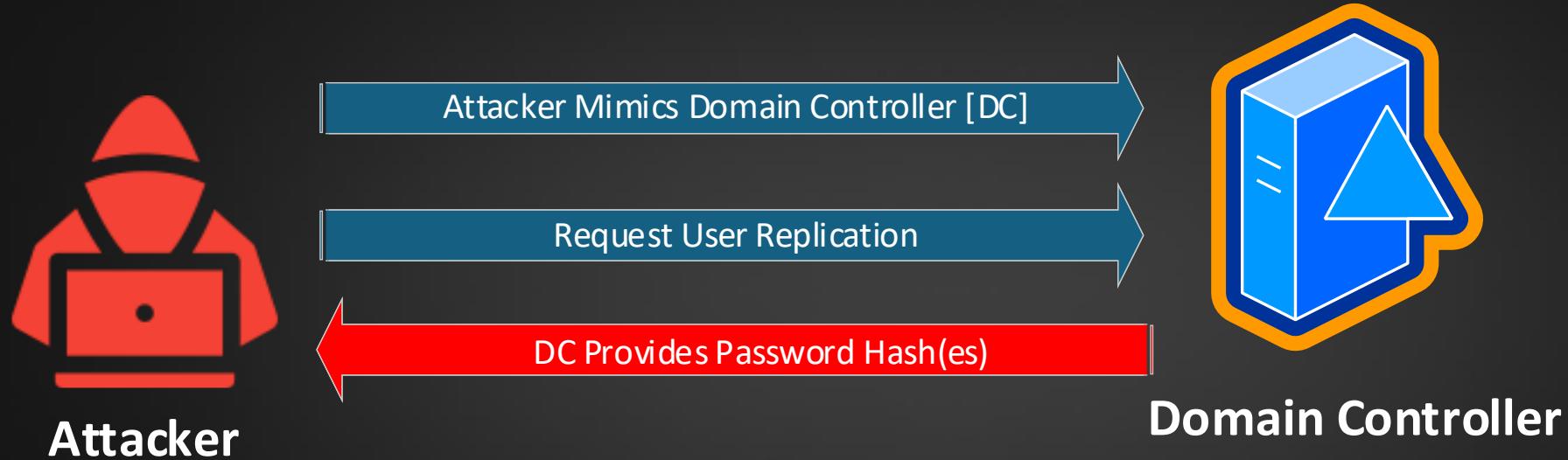
Certified Pre-Owned

Will Schroeder · Follow
Published in Posts By SpecterOps Team Members · 22 min read · Jun 17, 2021

496 4

TL;DR Active Directory Certificate Services has a lot of attack potential! Check out our whitepaper "[Certified Pre-Owned: Abusing Active Directory Certificate Services](#)" for complete details. We're also presenting this material at [Black Hat USA 2021](#).

DCSync extracts all domain passwords [hashes] resulting in Domain Dominance



DCSync requires Domain Admin permissions.

Demo on the next slide

DEMO

Demo

WELCOME TO SERVER MANAGER

1 Configure this local server

Remove server roles

DESTINATION SERVER
LAB-CA01.lab.local

Before You Begin
Server Selection
Server Roles
Features
Confirmation
Results

To remove one or more installed roles from the selected server, clear their check boxes.

Roles

- Active Directory Certificate Services
 - Certification Authority
 - Certificate Enrollment Policy Web Service (Not installed)
 - Certificate Enrollment Web Service
 - Certification Authority Web Enrollment
 - Network Device Enrollment Service (Not installed)
 - Online Responder (Not installed)
 - Active Directory Domain Services (Not installed)
 - Active Directory Federation Services (Not installed)
 - Active Directory Lightweight Directory Services (Not installed)
 - Active Directory Rights Management Services (Not installed)
 - Device Health Attestation (Not installed)
 - DHCP Server (Not installed)
 - DNS Server (Not installed)
 - Fax Server (Not installed)
- File and Storage Services
 - Host Guardian Service (Not installed)
 - Hyper-V (Not installed)
 - MultiPoint Services (Not installed)

Description

Active Directory Certificate Services (AD CS) is used to create certification authorities and related role services that allow you to issue and manage certificates used in a variety of applications.

< Previous Next > Remove Cancel

Local Server 1	All Servers 1
Manageability	Manageability
Events	Events
Services	Services

NLD AMSTERDAM ZAF CAPE TOWNS ZAF JOHANNESBURG

3:26 PM 9/15/2021

is classified as Nedscaper General Use

Prevention (is better than cure) -> Dutch philosopher Desiderius Erasmus [year 1500]

Protect Active Directory (Certificate Services) via the Security Recommendations from **Defender for Identity** [Secure Score or Microsoft Security Exposure Management]

<input type="checkbox"/>	2	Resolve unsecure domain configurations	+0.32%	0/5	<input type="radio"/> To address	No	Yes	Identity	Defender for Identity
<input type="checkbox"/>	3	Stop clear text credentials exposure	+0.32%	0/5	<input type="radio"/> To address	No	Yes	Identity	Defender for Identity
<input type="checkbox"/>	4	Remove dormant accounts from sensitive groups	+0.32%	0/5	<input type="radio"/> To address	No	Yes	Identity	Defender for Identity
<input type="checkbox"/>	5	Modify unsecure Kerberos delegations to prevent impersonation	+0.32%	0/5	<input type="radio"/> To address	No	Yes	Identity	Defender for Identity
<input type="checkbox"/>	6	Reduce lateral movement path risk to sensitive entities	+0.32%	0/5	<input type="radio"/> To address	No	Yes	Identity	Defender for Identity
<input type="checkbox"/>	7	Disable Print spooler service on domain controllers	+0.32%	0/5	<input type="radio"/> To address	No	Yes	Identity	Defender for Identity
<input type="checkbox"/>	8	Protect and manage local admin passwords with Microsoft LAPS	+0.32%	0/5	<input type="radio"/> To address	No	Yes	Identity	Defender for Identity
<input type="checkbox"/>	9	Resolve unsecure account attributes	+0.32%	0/5	<input type="radio"/> To address	No	Yes	Identity	Defender for Identity
<input type="checkbox"/>	10	Stop weak cipher usage	+0.32%	0/5	<input type="radio"/> To address	No	Yes	Identity	Defender for Identity
<input type="checkbox"/>	11	Edit misconfigured certificate templates ACL (ESC4)	+0.32%	0/5	<input type="radio"/> To address	No	Yes	Identity	Defender for Identity
<input type="checkbox"/>	12	Edit insecure certificate enrollment IIS endpoints (ESC8)	+0.32%	0/5	<input type="radio"/> To address	No	Yes	Identity	Defender for Identity

Prevention ESC8

Edit insecure certificate enrollment IIS endpoints (ESC8)

To address

Edit status & action plan Manage tags

General Exposed entities Implementation History (3)

Description

Active Directory Certificate Services (AD CS) enables Certificate Enrollment through various methods and protocols, including enrollment via HTTP-based methods - the Certificate Enrollment Service (CES) and the Web Enrollment interface (Certsrv). If these IIS endpoints have insecure configurations, they may be vulnerable to relay attacks (ESC8).

User impact

If the IIS endpoint allows NTLM authentication without enforcing protocol signing (HTTPS) or without enforcing Extended Protection for Authentication (EPA), it becomes vulnerable to NTLM relay attacks.



General	Exposed entities	Implementation	History (3)
Export			
Certificate Authority	Server hostname	Endpoints	
S3CURITY-CA	WSRV2016-DC02	Click to view endpoints	



General	Exposed entities	Implementation	History (3)
Prerequisites			
<ul style="list-style-type: none"> ✓ You have Defender for Identity. 			
Next steps			
<p>For each endpoint, follow these steps:</p> <ol style="list-style-type: none"> 1. Determine whether the endpoint is necessary and in regular use. If it is not used, it is advisable to disable it. 2. Deactivate NTLM and Negotiate authentication providers for the IIS endpoint. 3. If NTLM cannot be disabled, enable "Require SSL" and "Require Extended Protection" for the IIS endpoint. <p>For more information, please refer to the security advisory in the Learn more section.</p>			

Detection

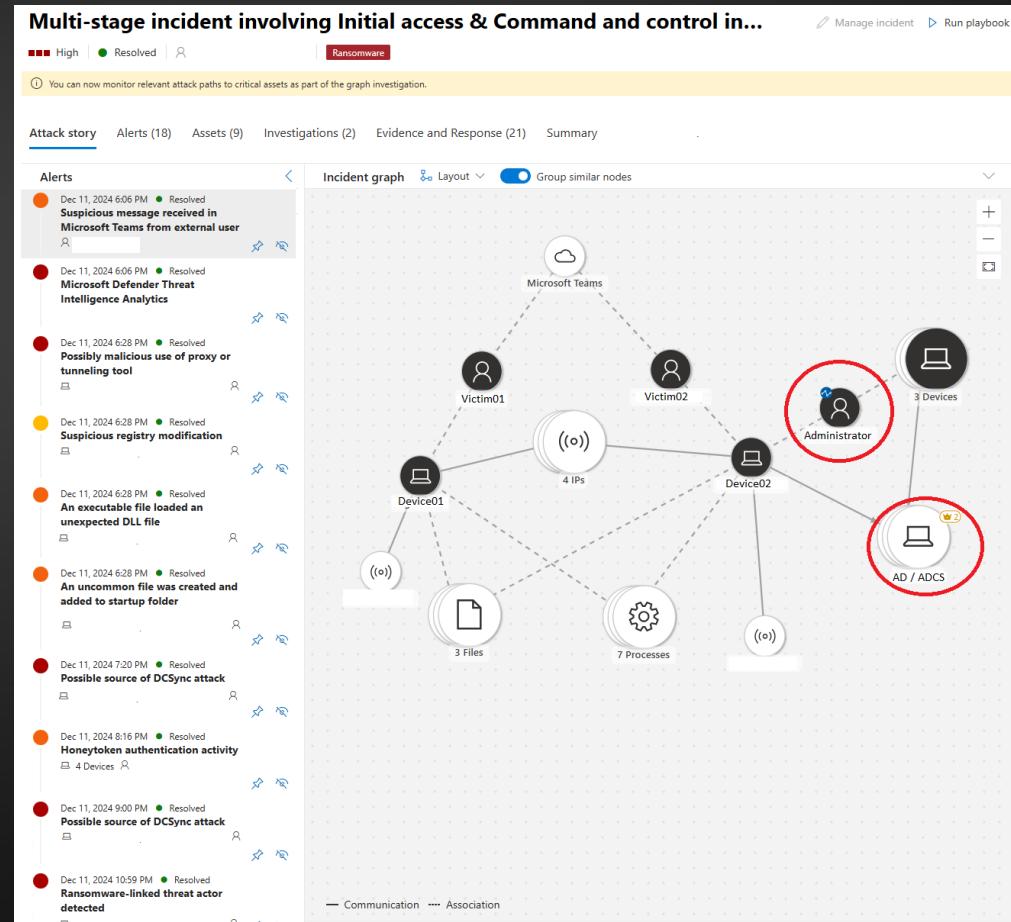
Defender XDR detects the attack as **Multi-stage incident**
[from patient-zero to domain dominance / ransomware]...

Time is critical!!

<45:00

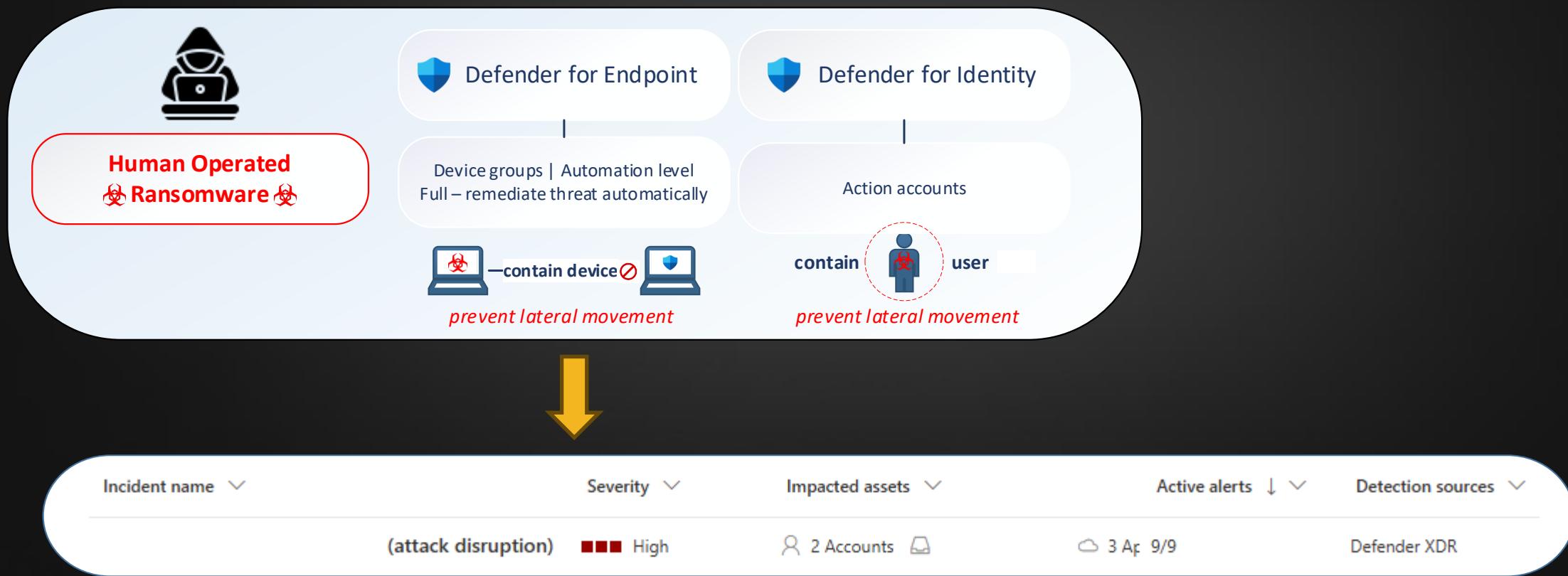
Minutes

Seconds



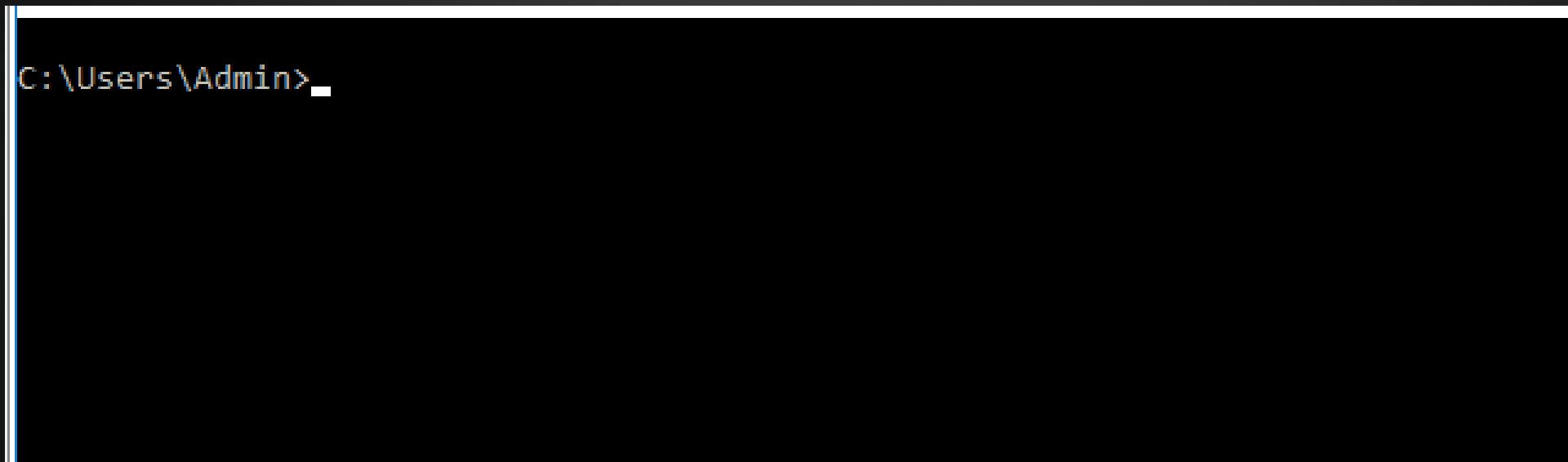
Defender XDR | Automatic Attack Disruption

HumOR (*Human Operated Ransomware*) can be disrupted via **Automatic Attack Disruption** where the compromised device(s) and user(s) are contained to prevent **lateral movement**.



The Active Directory BTG (Break The Glass) account (*used only in case of emergency*) is a target for the Storm 1811 attackers

- rename the account from Administrator to ‘something else’ to avoid brute-force attack from the internet
- inside Active Directory there is no hiding (SID S-1-5-domain-500)



Pro-tip

Pro-tip 😊 add the Active Directory BTG [Break The Glass] as Honeytoken in Defender for Identity. Each Active Directory Logon results in an Alert

Microsoft Defender for Identity

Honeytoken accounts are used as traps for malicious actors. Any authentication associated with these honeytoken accounts triggers an alert. [Learn more](#)

General

- Sensors
- Activation
- Directory services accounts
- Manage action accounts
- VPN
- Adjust alerts thresholds
- About

Entity tags

- Sensitive
- Honeytoken

Users Devices

+ Tag users Export 1 item

Name	Domain	UPN name	SAM name	SID
Administrator	s3cur1ty.local		Administrator	S-1-5-21-2



 Honeytoken authentication activity

■ Medium | ● Unknown | ● Resolved



... ■ ■ ■

Azure Subscription Hijacking

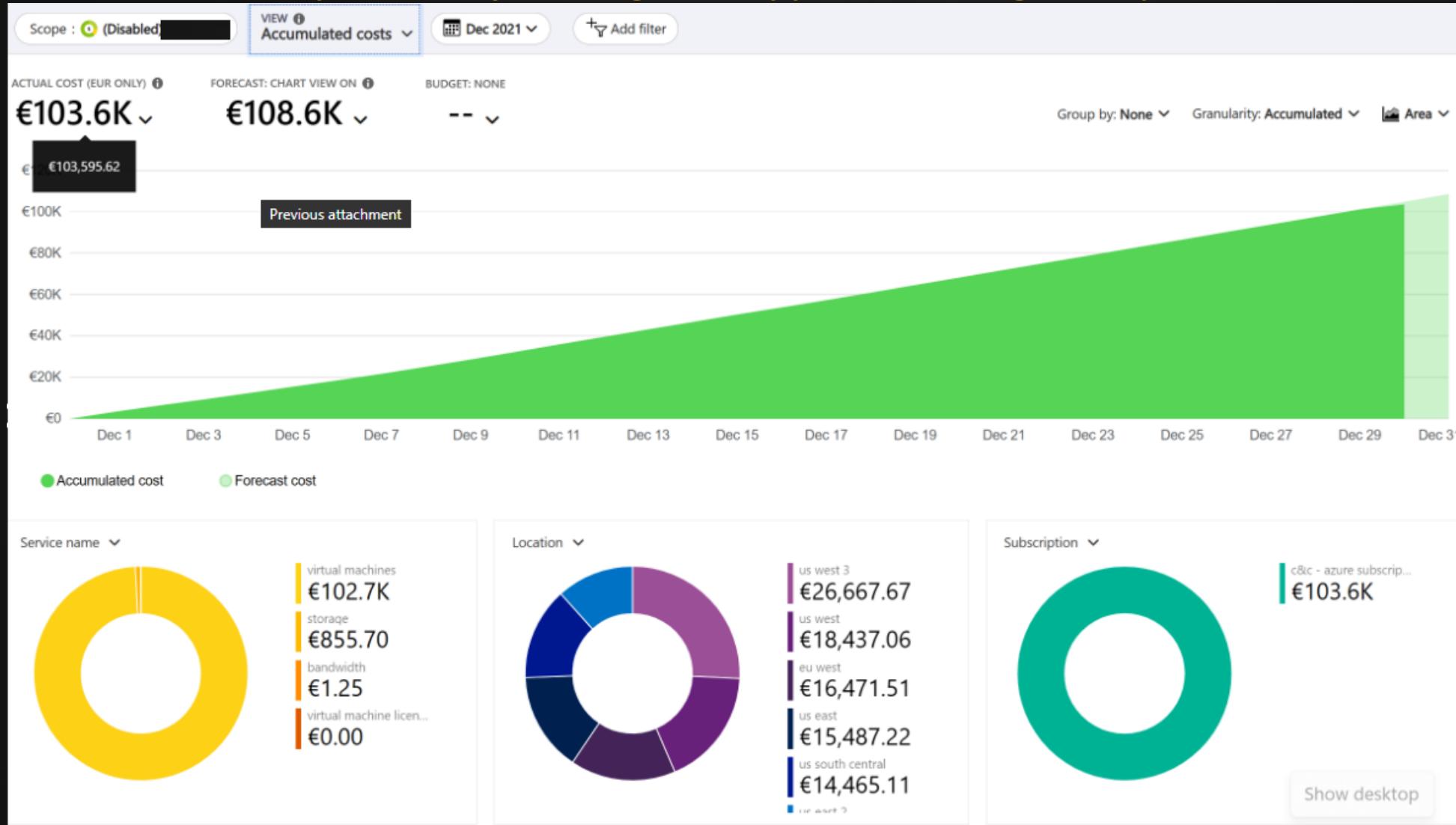
Bonus ☺



Derk van der Woude
CTO @ Nedscaper

Pro-tip

Azure Subscription Hijacking & Crypto mining story ...



NED
AMSTERDAM
ZAF
CAPE TOWN
ZAF
JOHANNESBURG

<https://derkvanerwoude.medium.com/azure-subscription-hijacking-and-cryptomining-86c2ac018983>



33

Azure Subscription Hijacking & Crypto mining



Important to know

- Payment information (**Credit Card**) is bound to the Subscription
- Audit Logs [**Activity Log**] are bound to the Subscription

A screenshot of the Azure Activity Log interface. On the left, there's a sidebar with icons for Overview, Activity log (which is selected and highlighted in grey), Access control (IAM), and Tags. The main area shows a list of four recent activities, each with a blue info icon, the action name, and the status "Succeeded".

> i Delete Virtual Network	Succeeded
> i Delete Public Ip Address	Succeeded
> i Delete Disk	Succeeded
> i Delete System Topic	Succeeded

- Entra allows access to **All Azure Subscriptions** with one button

A screenshot of the Azure Access management for Azure resources page. It shows a message from Derk van der Woude stating he can manage access to all Azure subscriptions and management groups in the tenant. Below the message is a blue toggle switch labeled "Yes".

Access management for Azure resources

Derk van der Woude (derk.van.der.woude@nedscaperlab.onmicrosoft.com) can manage access to all Azure subscriptions and management groups in this tenant.

[Learn more](#)

Yes

Azure Subscription Hijacking & Crypto mining attack

Hacker 6 steps:

- Compromise Admin Account in Microsoft Tenant (@victim.com)
- Create Guest (account from Attacker Tenant, e.g. @hacker.com)
- Assign Azure Subscription Owner permissions to new Guest
- Logon with Attacker account @hacker.com
- Switch Directory to Victim Subscription
- Change Directory from @victim.com to @hacker.com

GAME OVER

Azure services

Create a resource

Resources

Recent

Favo

Name

Pay-As-You-

WIN-N48QT

Nedscaper

425show

KV-SecureM

datascannin

Malware06

CSAT

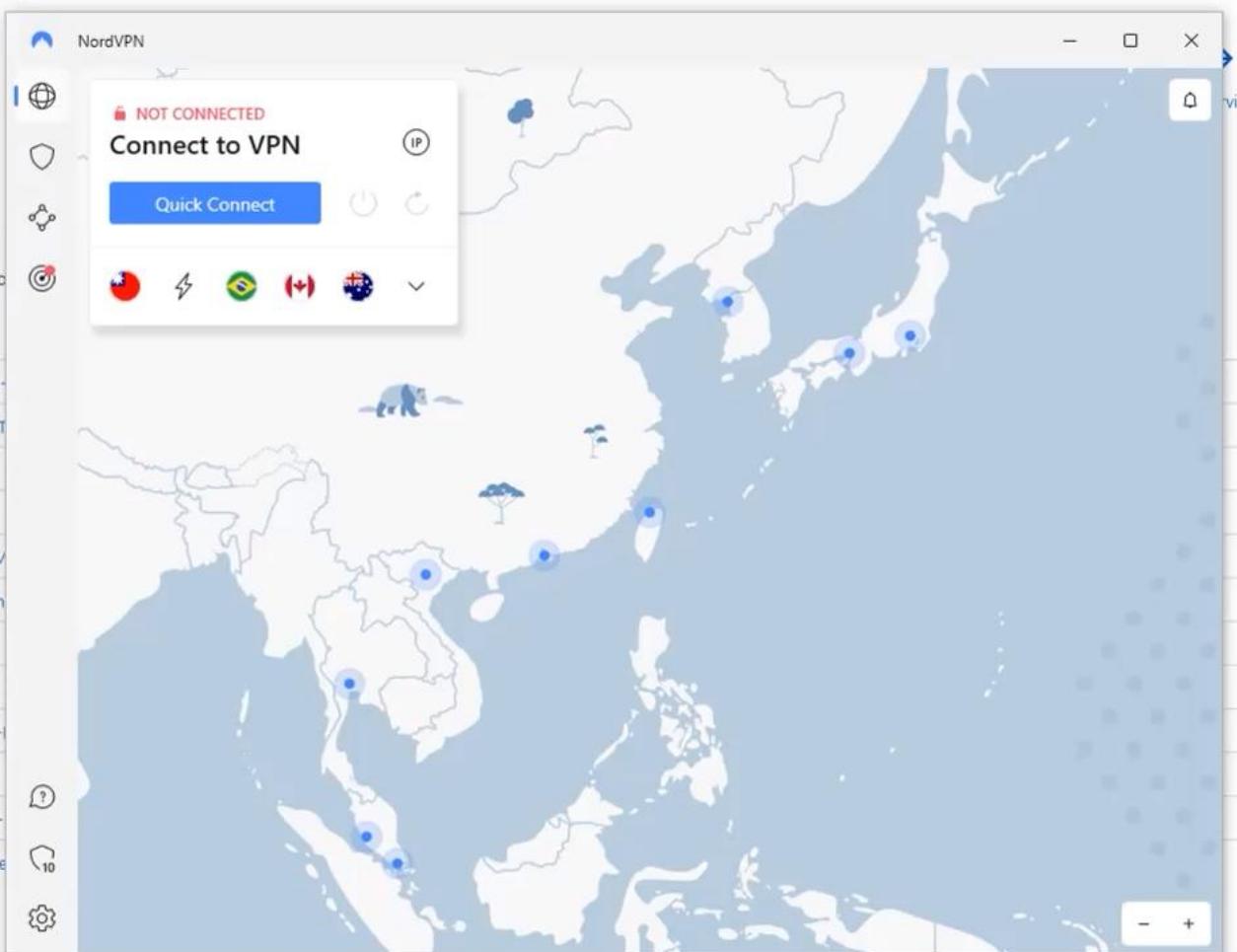
Consultant-i

Malware02

Malware02-

RG-Malware

See all



Navigate

Subscriptions

Resource groups

All resources

Dashboard



Questions?