

# 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 😊

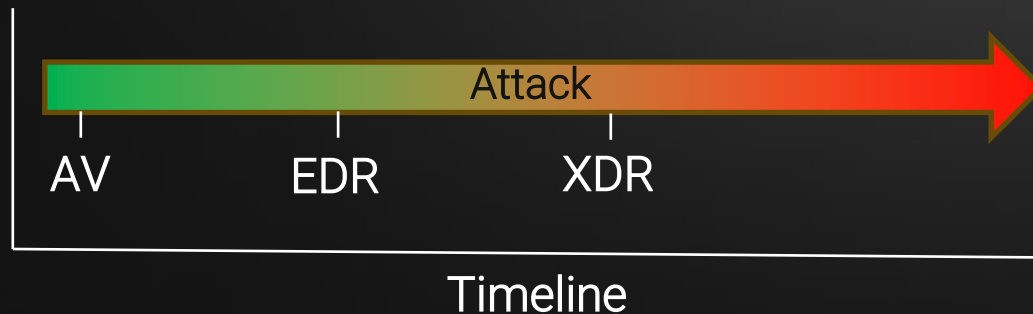


# Disclaimer: the difference between AV and EDR/XDR

**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 China	 Sandstorm Iran	 Sleet North Korea	 Dust Turkey	 Cyclone Vietnam
 Hail Lebanon	 Tempest South Korea	 Tsunami Financially motivated	 Flood Private sector offensive actor	 Storm Groups in development


Microsoft Threat Actor Naming



# Defender XDR | Threat Intel Profile TTPs & IOCs

Threat actor

December 20, 2023

 Storm-1811

Share

- Description
- TTPs
- Indicators (41)

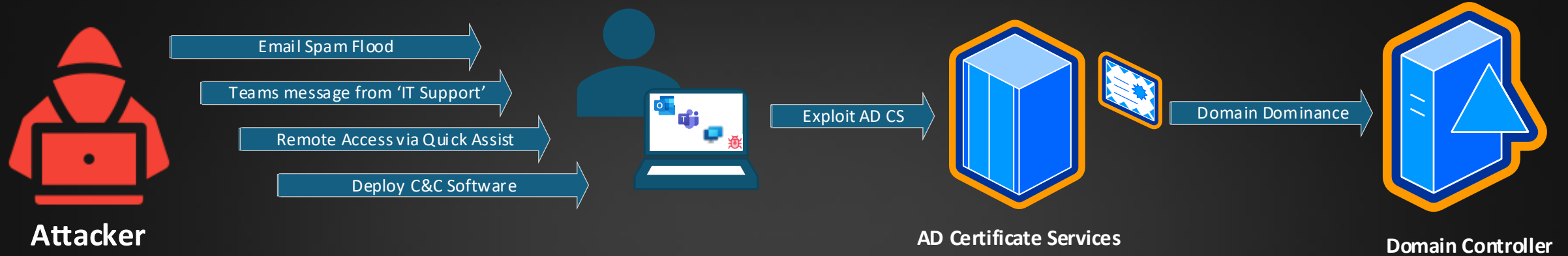
## Snapshot

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.

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.		
Since mid-April 2024, Microsoft Threat Intelligence has observed Storm-1811 misusing the client management tool Quick Assist to target users in social engineering attacks. For example, in some cases, Storm-1811 initiates link listing attacks – a type of email bombing attack, where they sign up targeted emails to multiple email		

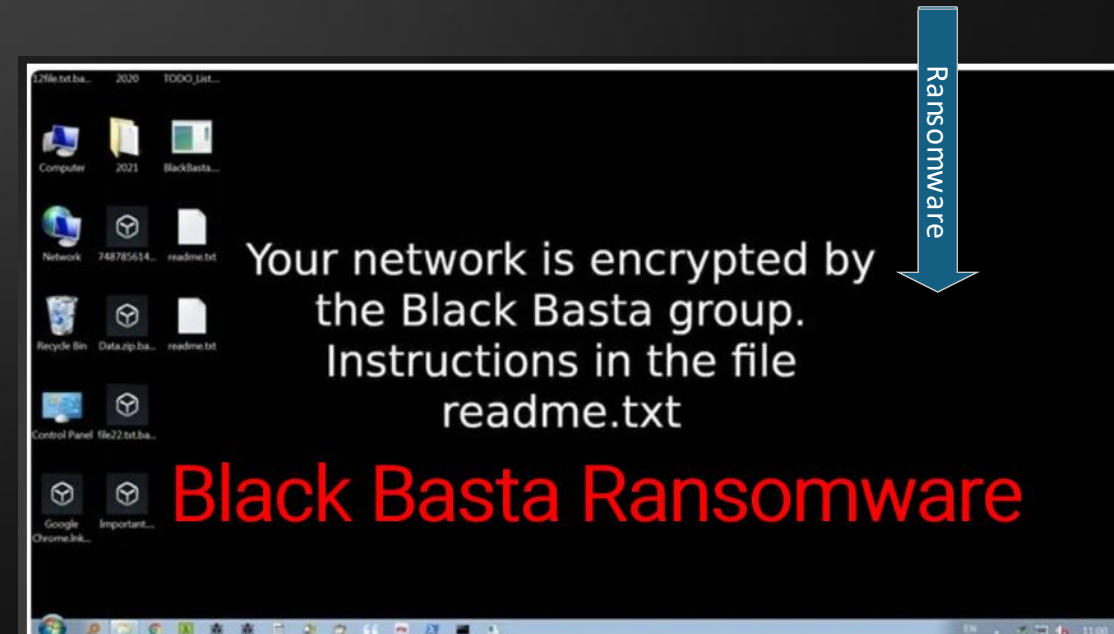


# Overview of the Storm-1811 Attack Techniques



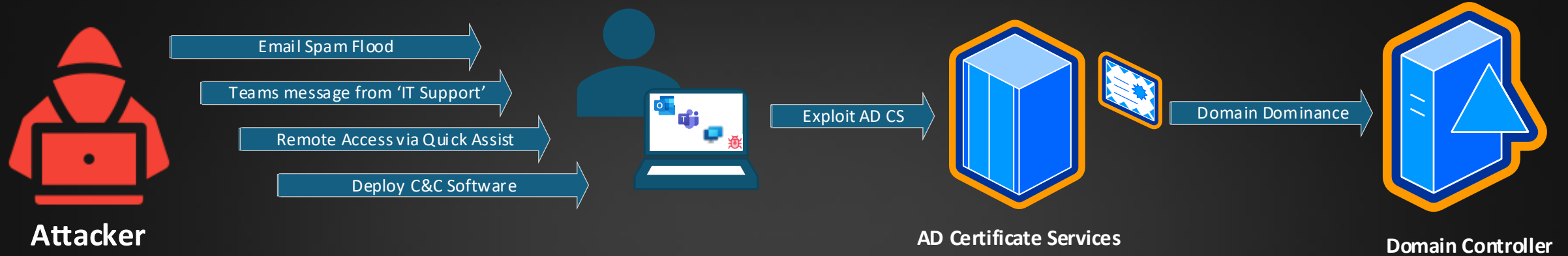
**<45:00**

Minutes      Seconds





# Overview of the Storm-1811 Attack Techniques



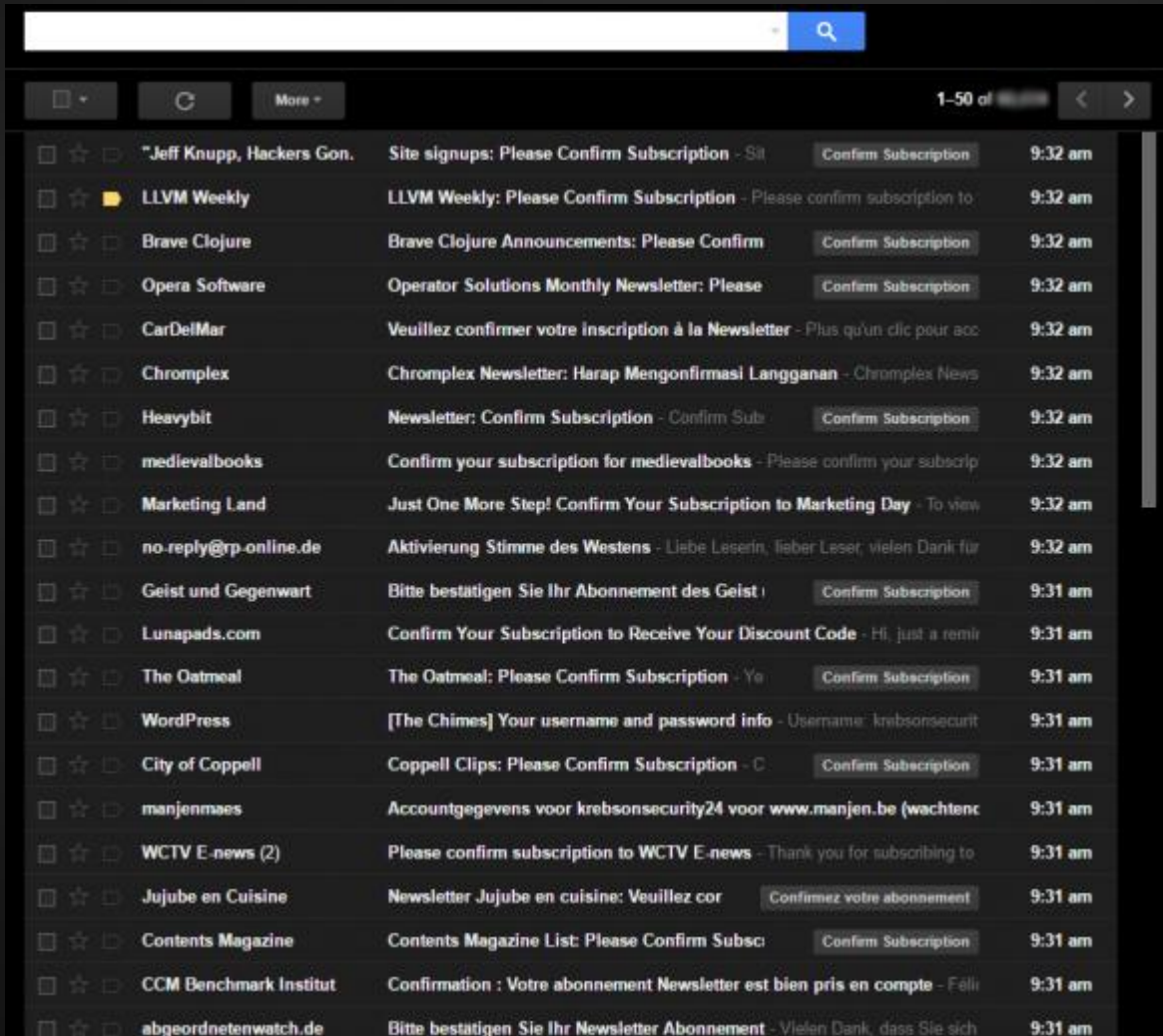
**<45:00**

Minutes      Seconds





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]



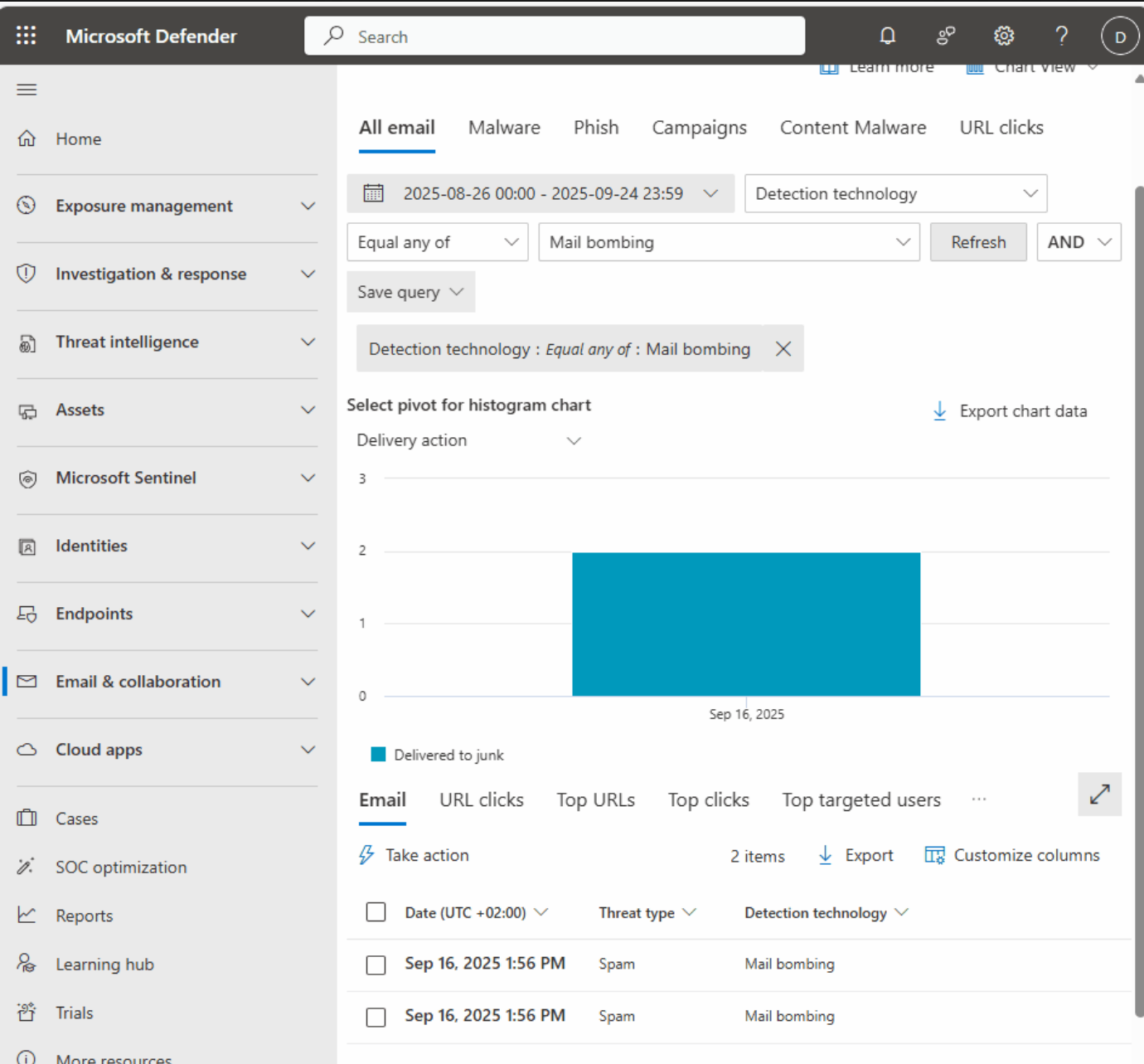


June 2025 UPDATE

Detection by MDO  
Defender for Office 365

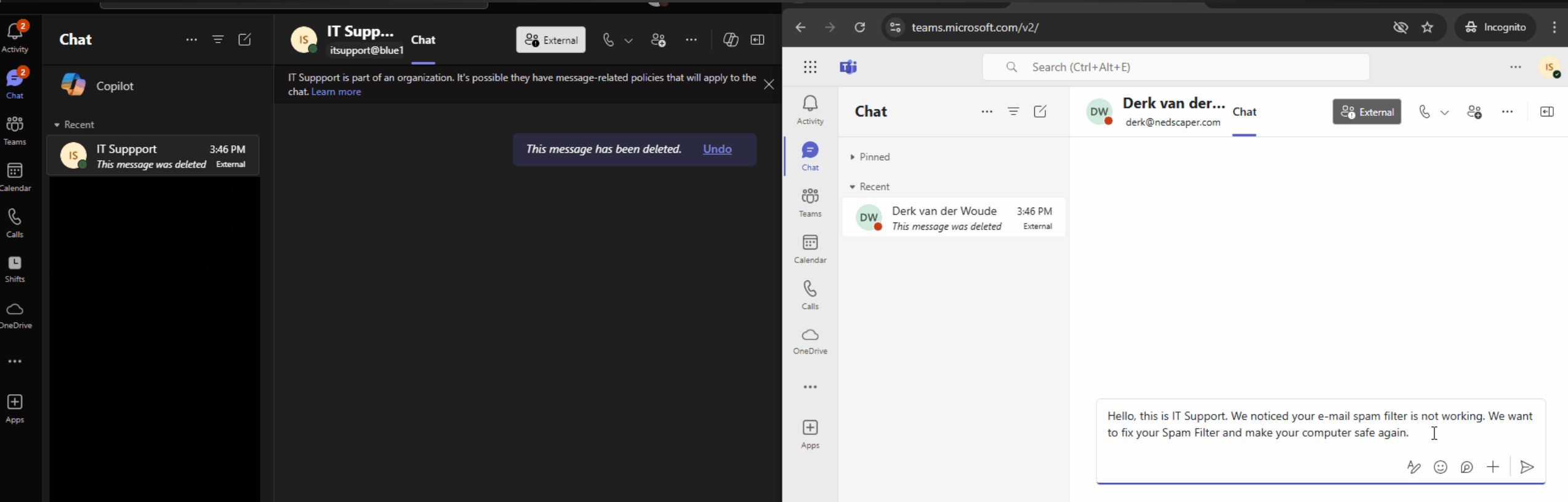
Visible in the Threat Explorer,  
Email Entity and Advanced  
Hunting

Detection Technology  
Mail Bombing





*Outsourced 'IT Support'* send a **Teams message** to the end user to fix the 'broken' Spam filter





## Prevention #1

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

People in my organization can communicate with unmanaged Teams accounts	<input type="radio"/> Off
People in my organization can communicate with accounts in trial Teams tenant	<input type="radio"/> Off
People in my organization can communicate with Skype users	<input type="radio"/> Off
People in my organization can communicate with users who are using custom applications built with Azure Communication Services	<input type="radio"/> Off

## Prevention #2

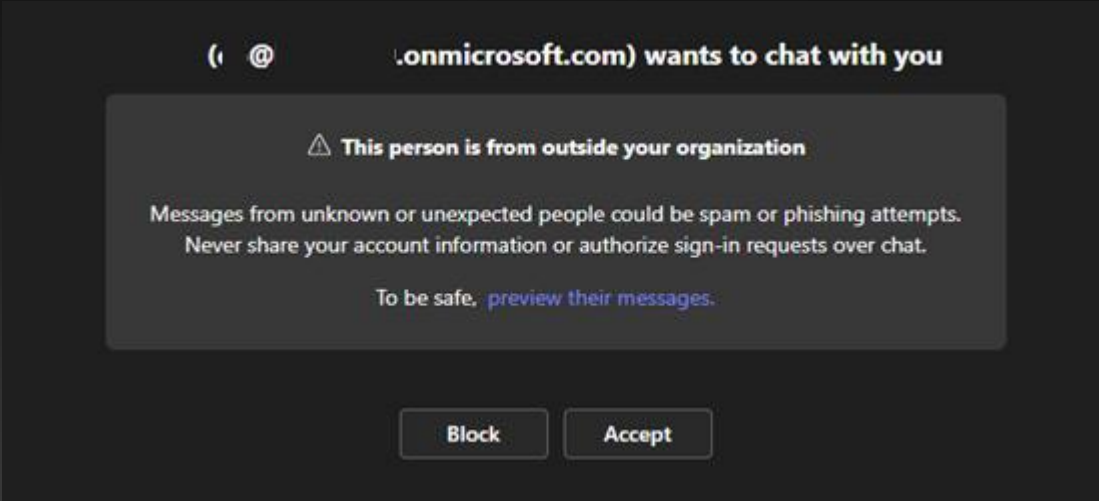
Microsoft Teams can **allow** all (**default**) or specific domains, or **block** all or specific domains.

- ✓ **Allow all external domains**  
All external organizations are trusted. People in my organization can communicate with users from any external domain.
- ✓ **Allow only specific external domains**  
Create a list of external domains that are allowed. Only the external organizations specified are trusted. All other domains will be blocked.
- ⊖ **Block only specific external domains**  
Create a list of external domains that are blocked. All other domains will be allowed.
- ⊖ **Block all external domains**  
People in my organization can't communicate with users from any external domain.



#1 User Awareness is key!!!

IT Support (External)

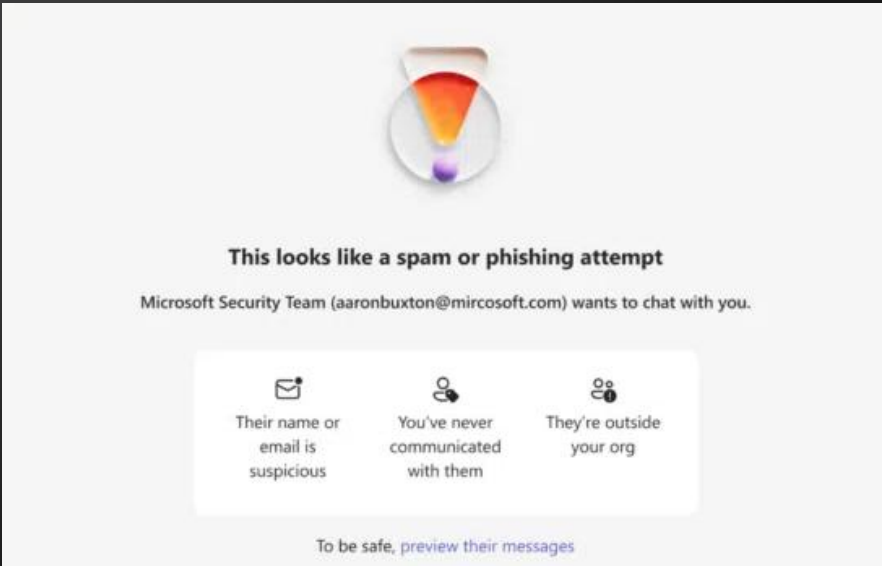


#2 Microsoft Teams: Brand Impersonation Protection for Teams Messaging [Feb-2025]

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



Microsoft 365 (formerly, Office 365)  
Microsoft

## 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

Malicious Teams Message from External .onmicroso...  
Incident number 1

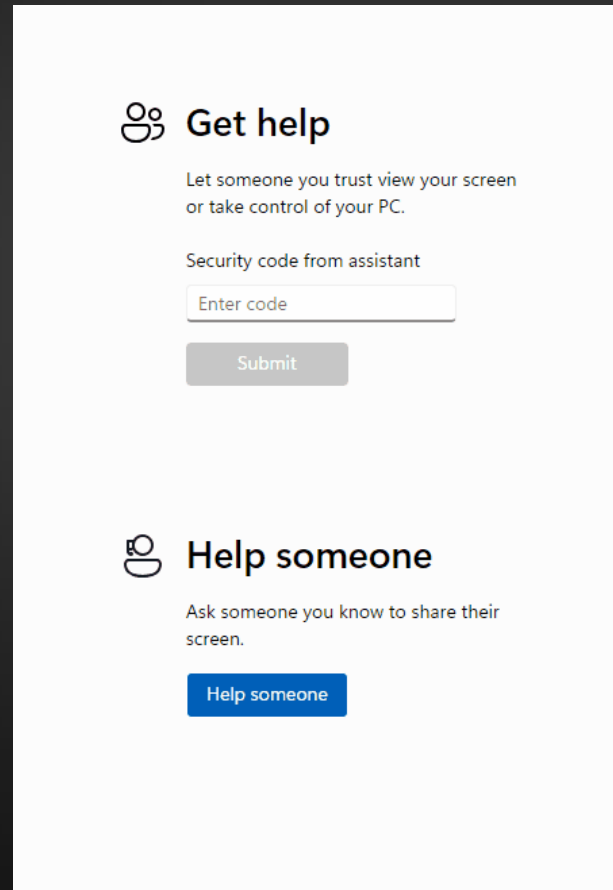
Unassigned  
Owner

New  
Status

High  
Severity



**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 Sideloads as an example) and ransomware



The screenshot displays the Windows Quick Assist application window. It features two main sections. The top section, titled 'Get help' with a person icon, instructs the user to 'Let someone you trust view your screen or take control of your PC.' It includes a text input field labeled 'Enter code' and a 'Submit' button. The bottom section, titled 'Help someone' with a person icon, instructs the user to 'Ask someone you know to share their screen.' and includes a blue 'Help someone' button.




Prevention

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

Windows Defender Firewall with Advanced Security													
File Action View Help													
Windows Defender Firewall with Advanced Security													
Firewall													
Name	Profile	Action	Override	Direction	Program	Local Address	Remote Address	Protocol	Local Port	Remote Port	Authorized Users	Authorized Computers	Authorized Local
Quick Assist - Microsoft Store App (Inbound)	All	Block	No	Inbound	Any	Any	Any	Any	Any	Any	Any	Any	Any
Quick Assist - Microsoft Store App (Outbound)	All	Block	No	Outbound	Any	Any	Any	Any	Any	Any	Any	Any	Any
Quick Assist - Win32 App (Inbound)	All	Block	No	Inbound	C:\Windows\System32\QuickAssist.exe	Any	Any	Any	Any	Any	Any	Any	Any
Quick Assist - Win32 App (Outbound)	All	Block	No	Outbound	C:\Windows\System32\QuickAssist.exe	Any	Any	Any	Any	Any	Any	Any	Any

User Awareness is key!!!

Again 😊



Derk v.

### Allow screen sharing?

If this person contacted you unexpectedly and asked to connect to your device, this might be a scam.

[Privacy statement](#)

[Terms of use](#)

☐ [I understand the security implications of sharing my screen](#)

Allow





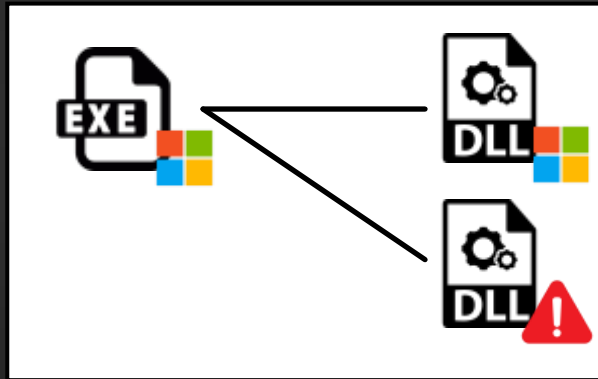


**DLL Sideload** (also called **Living of the Land**) is a technique to load malicious .DLL (code) files from a standard Windows Executable.



**Attacker**

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

Process Monitor - Sysinternals: www.sysinternals.com

File Edit Event Filter Tools Options Help

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	QueryBasicInforms...	C:\Windows\System32\winhttp.dll	SUCCESS
20:44:...	OneDriveStand...	29348	CloseFile	C:\Windows\System32\winhttp.dll	SUCCESS

**System32**

Search Results in Local Disk (C:)

Name	Date modified	Type	Size
winfax.dll	16/11/2023 21:57	Application exten...	
<b>winhttp.dll</b>	16/11/2023 21:56	Application exten...	

DLL search order

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



## 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 Sideloading** (*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...MediumDetec...Resol...

(True positive)

[8016] OneDriveStandaloneUpdater.exe loaded image winhttp.dll

An executable file loaded an unexpected DLL ...MediumDete...Resol...

(True positive)

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

An uncommon file was created and added to ...MediumDete...Resol...

(True positive)

[8016] OneDriveStandaloneUpdater.exe created file OneDriveUpdate.lnk

An uncommon file was created and added to ...MediumDete...Resol...

(True positive)

OneDriveStandaloneUpdater.exe has initiated a connection to 195.123.233.148

Signer

Unsigned file

PE metadata

Original name

MFC\_CalculatorApp.exe

Company

TODO: <Company name>

Product

TODO: <Product name>

Description

MFC\_CalculatorApp

File prevalence

Organization devices

2

Worldwide devices

3

Organization cloud apps

0

Observed devices (last 30 days)

Time

Command & Control

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

Create rules for devices

1 OT devices are not protected  
To get full visibility into your OT devices onboard Defender for IoT

Transient devices have been automatically filtered out from some tabs to minimize noise. This filtering is determined by an internal algorithm, which mainly depends on the frequency of appearances of these discovered devices. To disable this automatic filtering, navigate to the filter menu.

All devicesComputers & MobileNetwork devicesIoT/OT devicesUncategorized devices

Total4Critical assets0High risk0High exposure2Not onboarded3Newly discovered0

Exportwsrv30 DaysCustomize columnsFilter

Filters: Transient device: No

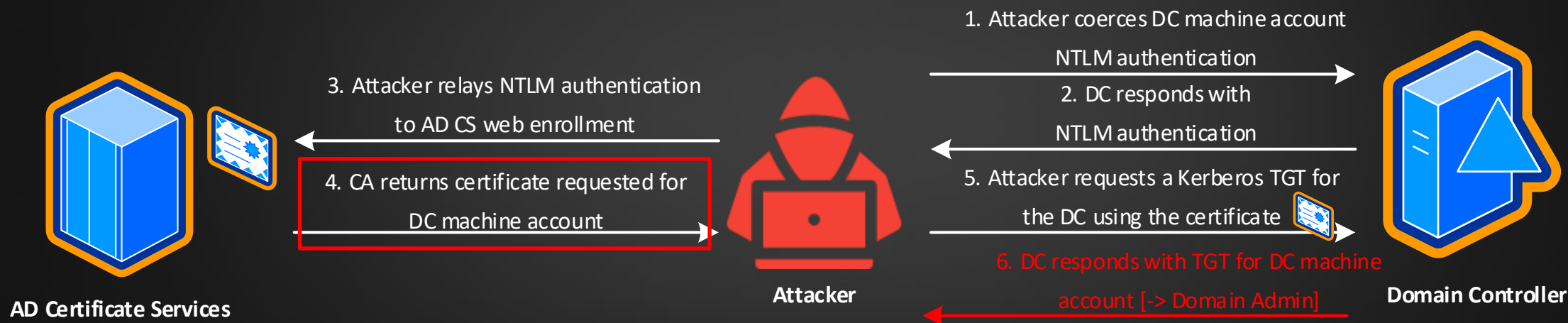
Name	IP	Device category	Device type	Device AAD id	Risk level	Exposure level	Onboarding status	Discovery sources	Tags	Device role
wsrv2016-srv01.s3curity.local	192.168.178.70	Computers and ...	Server		No known ...	High	Can be onboarded			
WSRV2016-DC02.s3curity.local	192.168.178.11	Computers and ...	Server		No known ...	No data available	Can be onboarded			
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			

C:\Windows\system32\cmd.exe  
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

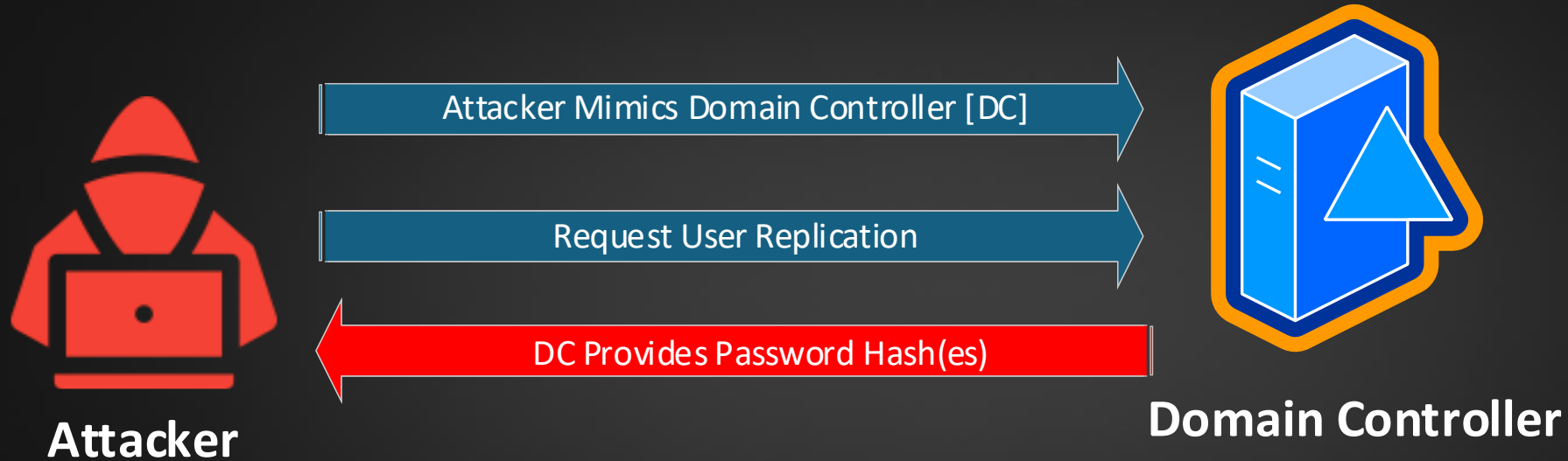
**TL;DR** Active Directory Certificate Services has a lot of attack potential! Check out our whitepaper "[Certified Pre-Owned: Abusing Active Directory Certificate Services](#)" for complete details. We're also [presenting this material at Black Hat USA 2021](#).



NLD AMSTERDAM  
ZAF CAPE TOWN  
ZAF JOHANNESBURG



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

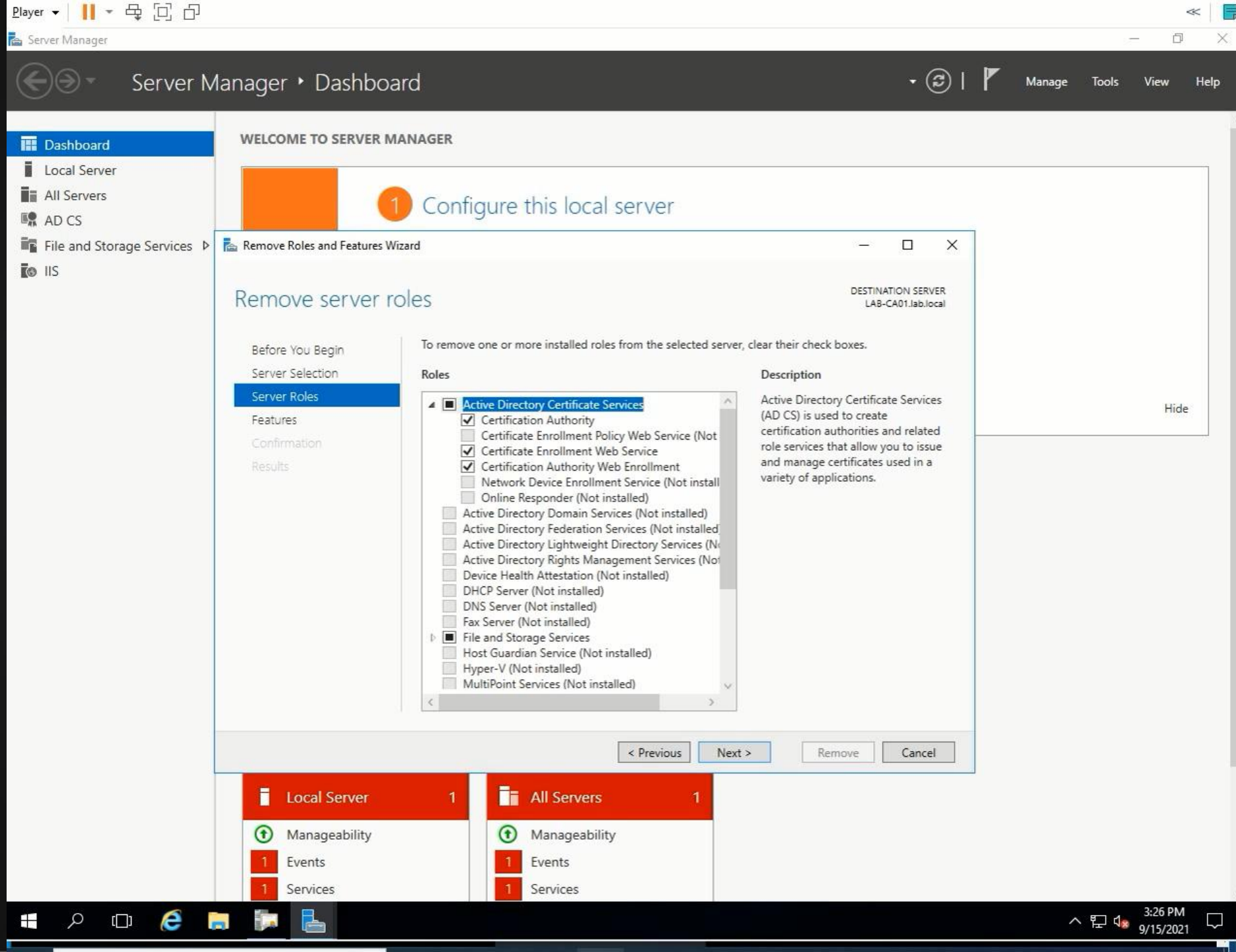


**DCSync** requires **Domain Admin** permissions.

Demo on the next slide



# Demo





**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	<a href="#">Click to view endpoints</a>

General Exposed entities **Implementation** History (3)

### Prerequisites

✓ You have Defender for Identity.

### Next steps

For each endpoint, follow these steps:

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.
- For more information, please refer to the security advisory in the "Learn more" section.



## Detection

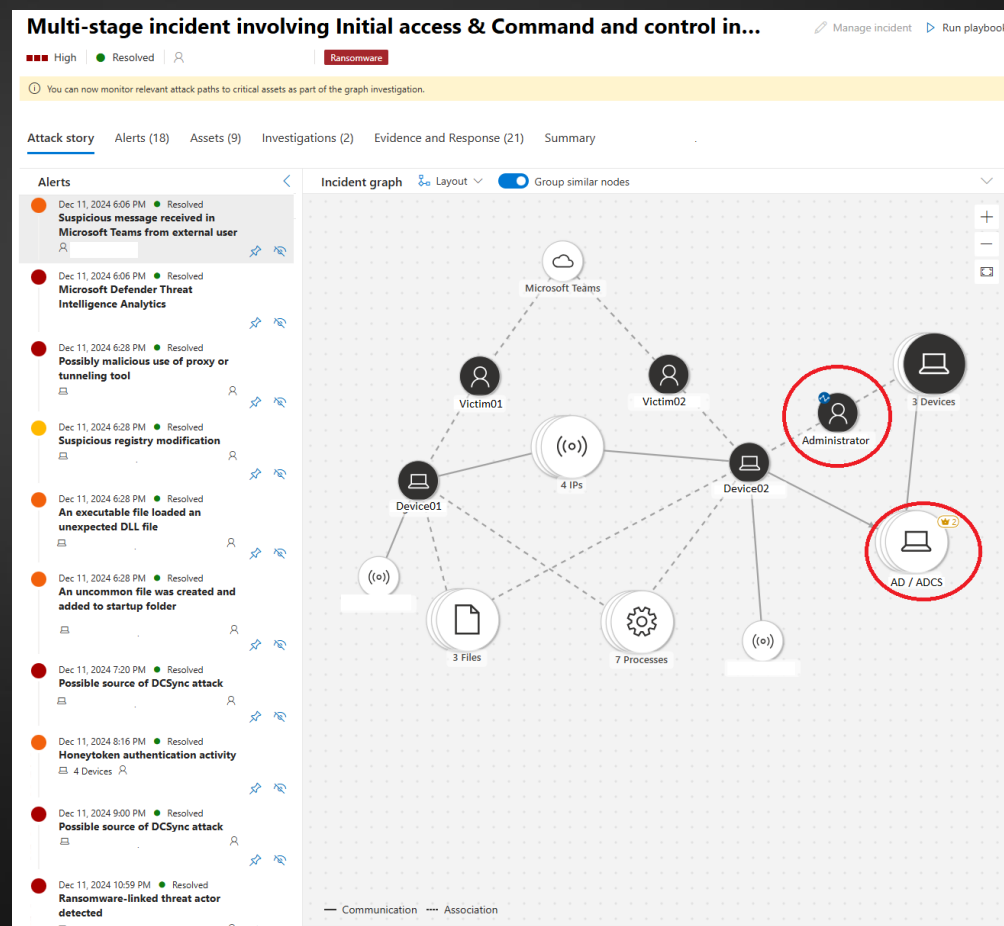
Defender **XDR** detects the attack as **Multi-stage incident**  
[from patient-zero to domain dominance / ransomware]...

Time is critical!!

<45:00

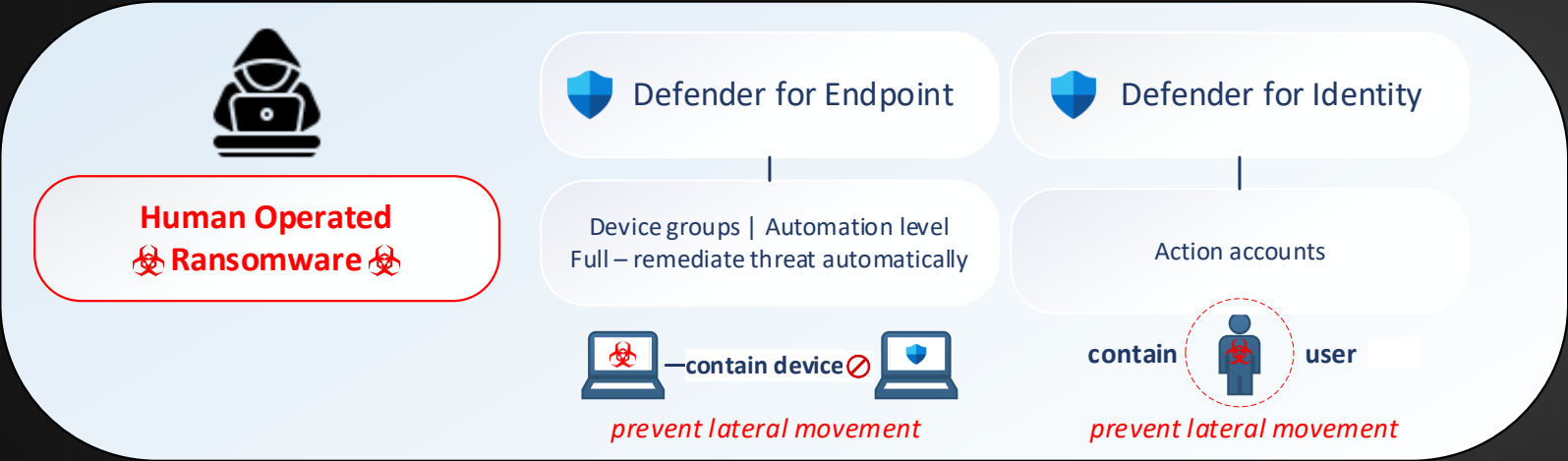
Minutes

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.



Incident name ▾

Severity ▾

Impacted assets ▾

Active alerts ↓ ▾

Detection sources ▾

(attack disruption) ■■■ High

👤 2 Accounts 📁

☁ 3 Aff 9/9

Defender XDR



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**)

```
C:\Users\Admin>_
```



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

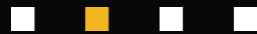
<input type="checkbox"/>	Name	Domain	UPN name	SAM name	SID
<input type="checkbox"/>	Administrator	s3cur1ty.local		Administrator	S-1-5-21-4



### Honeytoken authentication activity

■ ■ ■ Medium   ● Unknown   ● Resolved





# Azure Subscription Hijacking

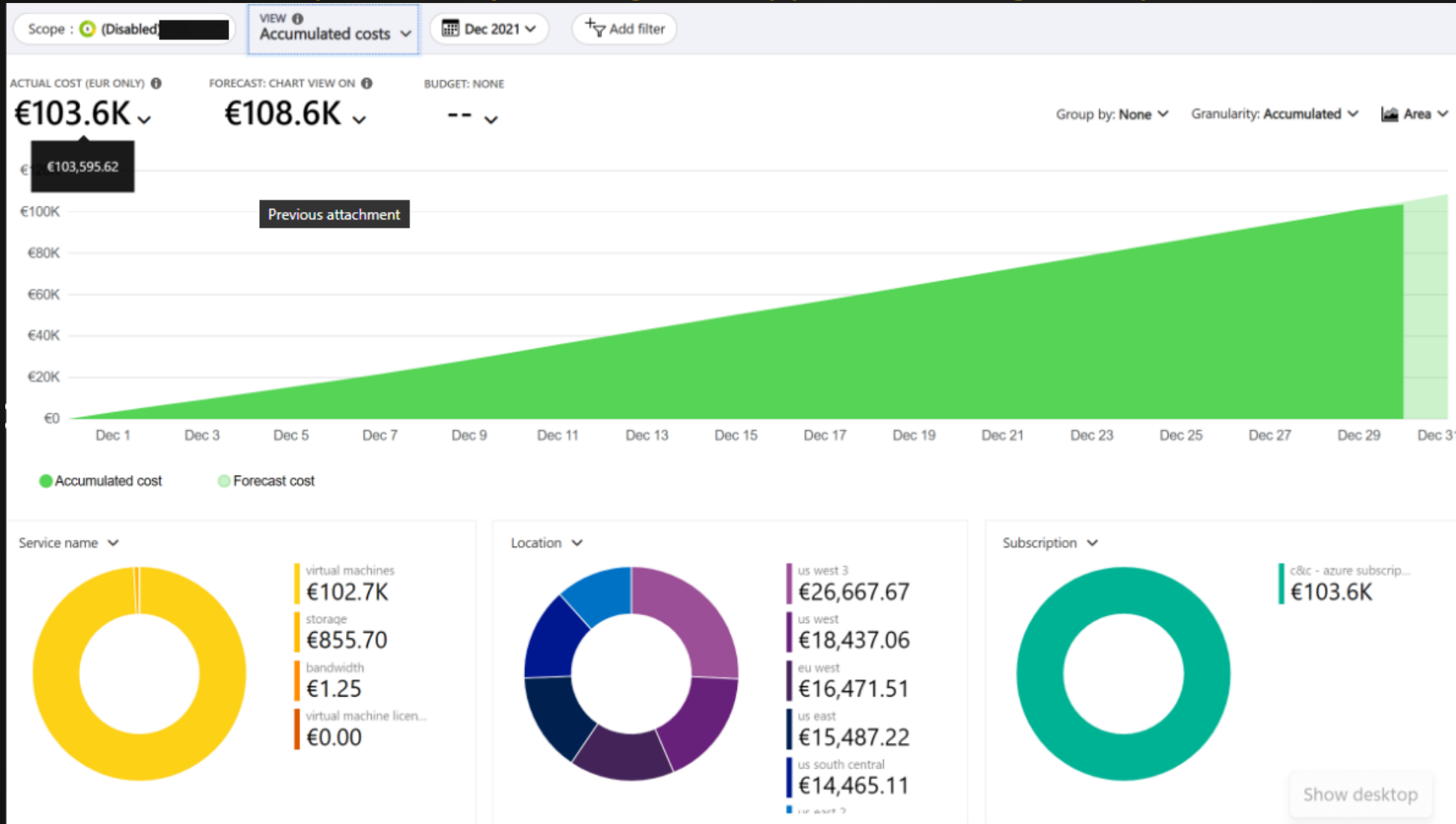
## Bonus 😊



Derk van der Woude  
CTO @ Nedscaper



# Azure Subscription Hijacking & Crypto mining story ...





# 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

Overview	> Delete Virtual Network	Succeeded
Activity log	> Delete Public Ip Address	Succeeded
Access control (IAM)	> Delete Disk	Succeeded
Tags	> Delete System Topic	Succeeded

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

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 Fav

Name

-  Pay-As-You-
-  WIN-N48QT
-  Nedscaper
-  425show
-  KV-SecureM
-  datascannin
-  Malware06
-  CSAT
-  Consultant-
-  Malware02
-  Malware02-
-  RG-Malware


See all

NordVPN




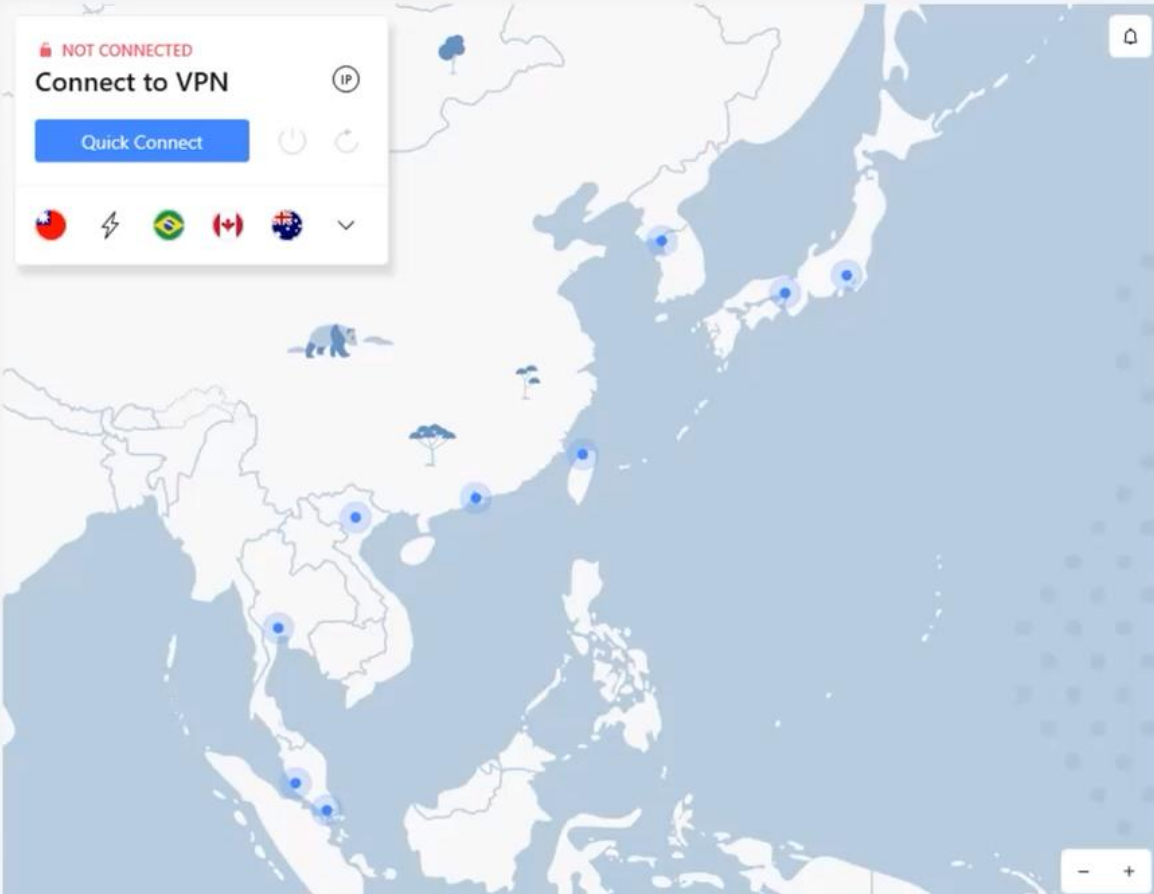
NOT CONNECTED

Connect to VPN



Quick Connect





Navigate

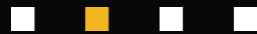
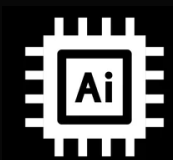
 Subscriptions

 Resource groups

 All resources

 Dashboard





# Questions?