TLP:GREEN

Ransomware in de zorg (en elders)

COMPUTER EMERGENCY
RESPONSE TEAM
VOOR DE ZORG

CERT

Mijn naam is

Jan Hanstede

Security specialist Z-CERT

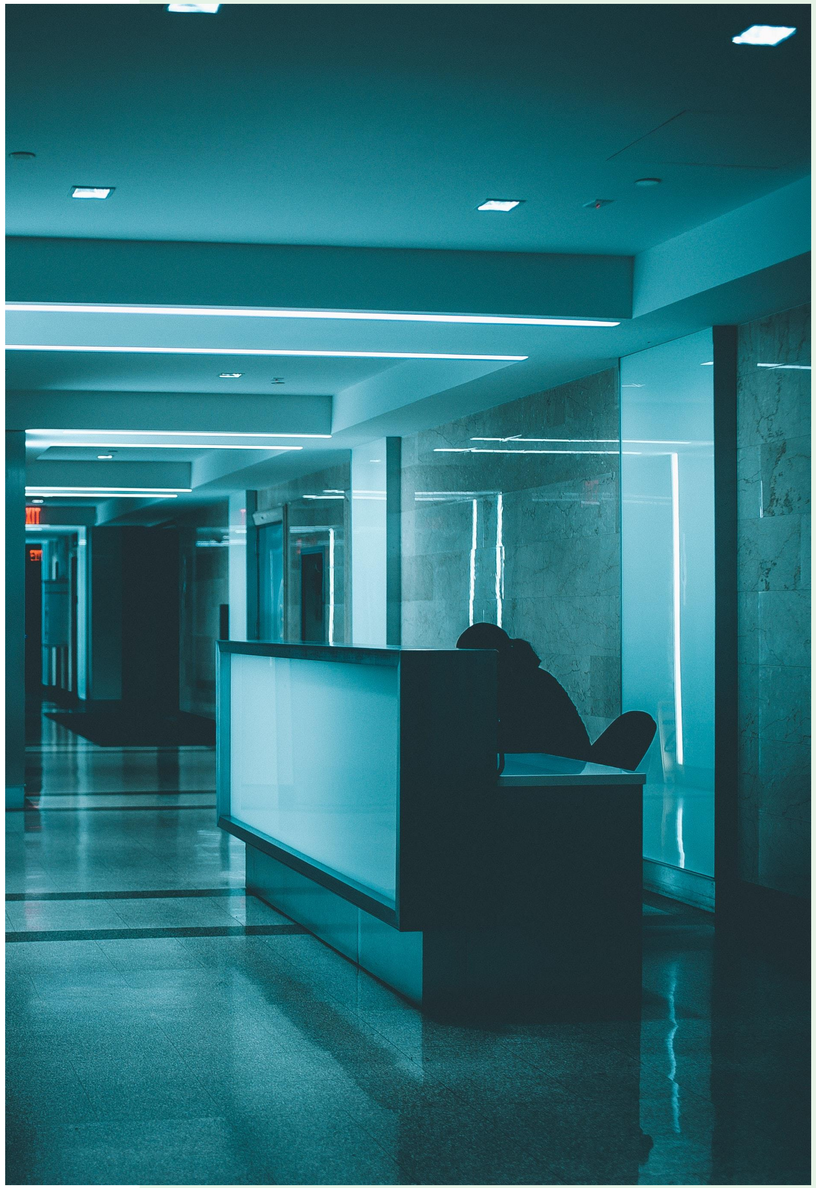
IT specialist

Webdeveloper

Onderwijs

Inhoud presentatie

- Update dreigingsbeeld / impact
- Hoe gaan ze te werk? Prioriteiten?



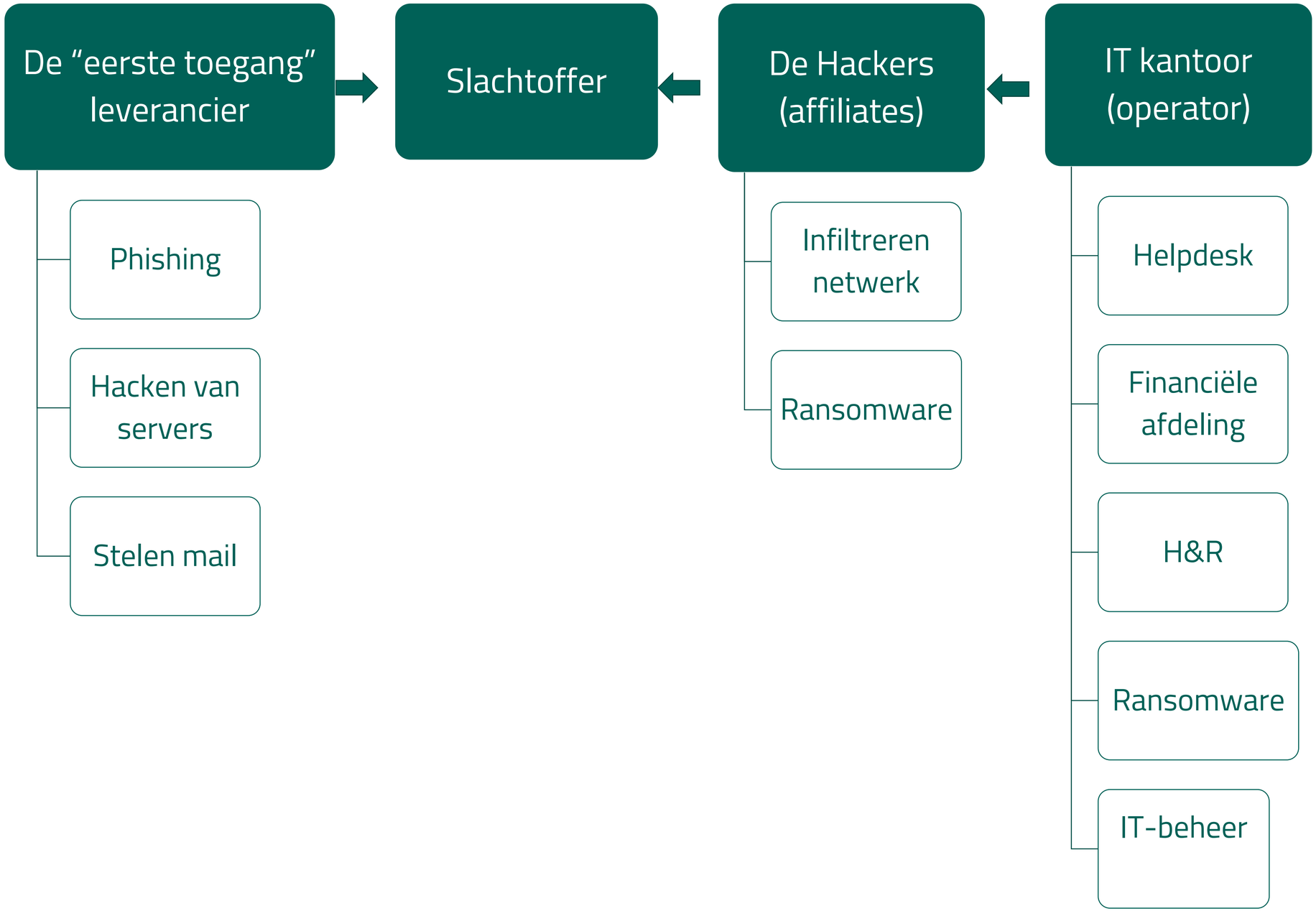
TLP:GREEN

Update dreigingsbeeld

COMPUTER EMERGENCY
RESPONSE TEAM
VOOR DE ZORG

CERT

Wie zijn ze? Het “ransomware as a service” model



Proces

- **Eerste toegang leverancier** valt slachtoffer aan
- Verkoopt toegang aan affiliate of operator
- Affiliate infiltreert netwerk en rolt ransomware uit (IT’er)
- Operator ondersteund de hacker met allerlei diensten (kantoor)

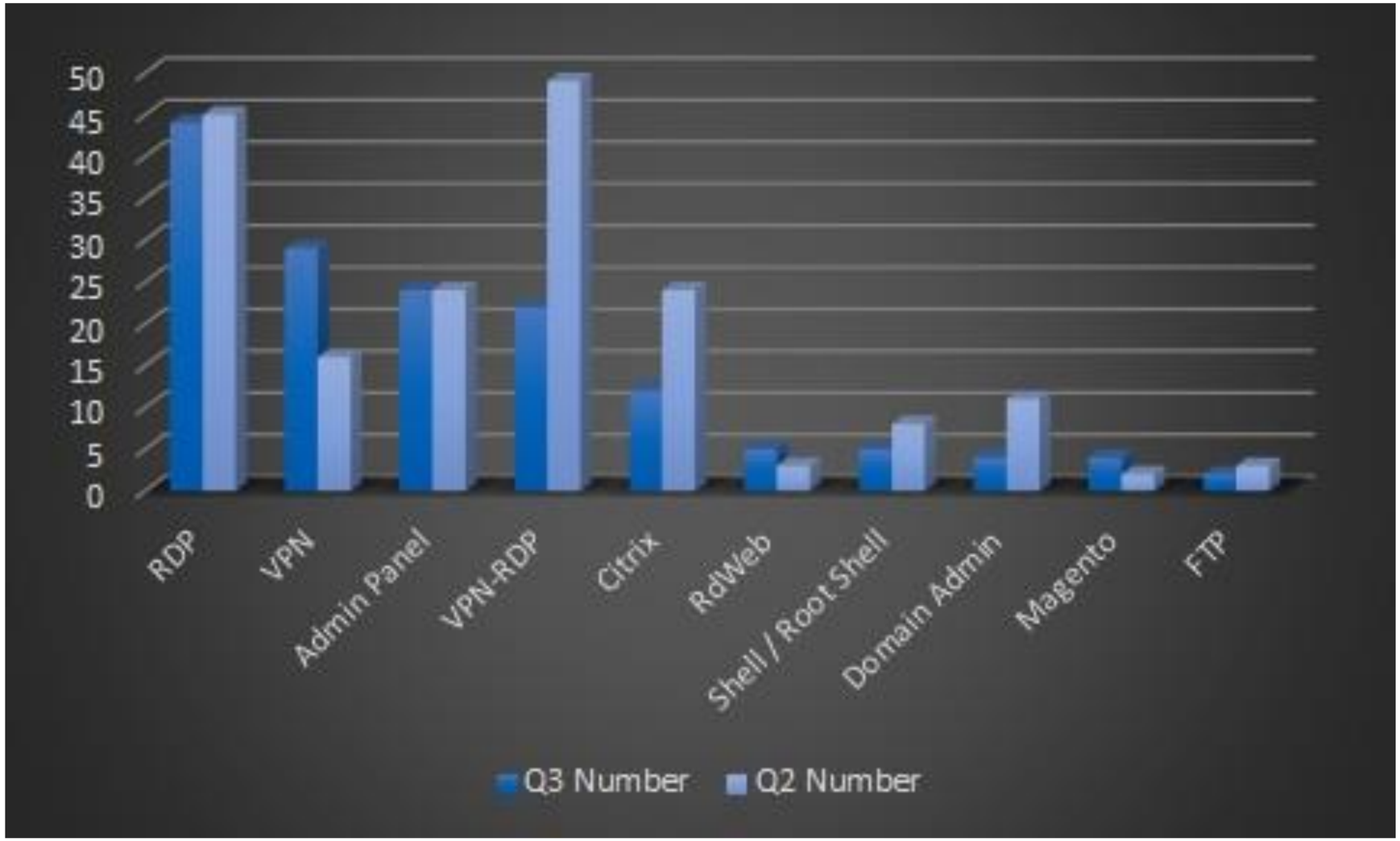
Waarom relevant om te weten

De “eerste toegang” leverancier

Producten in assortiment:

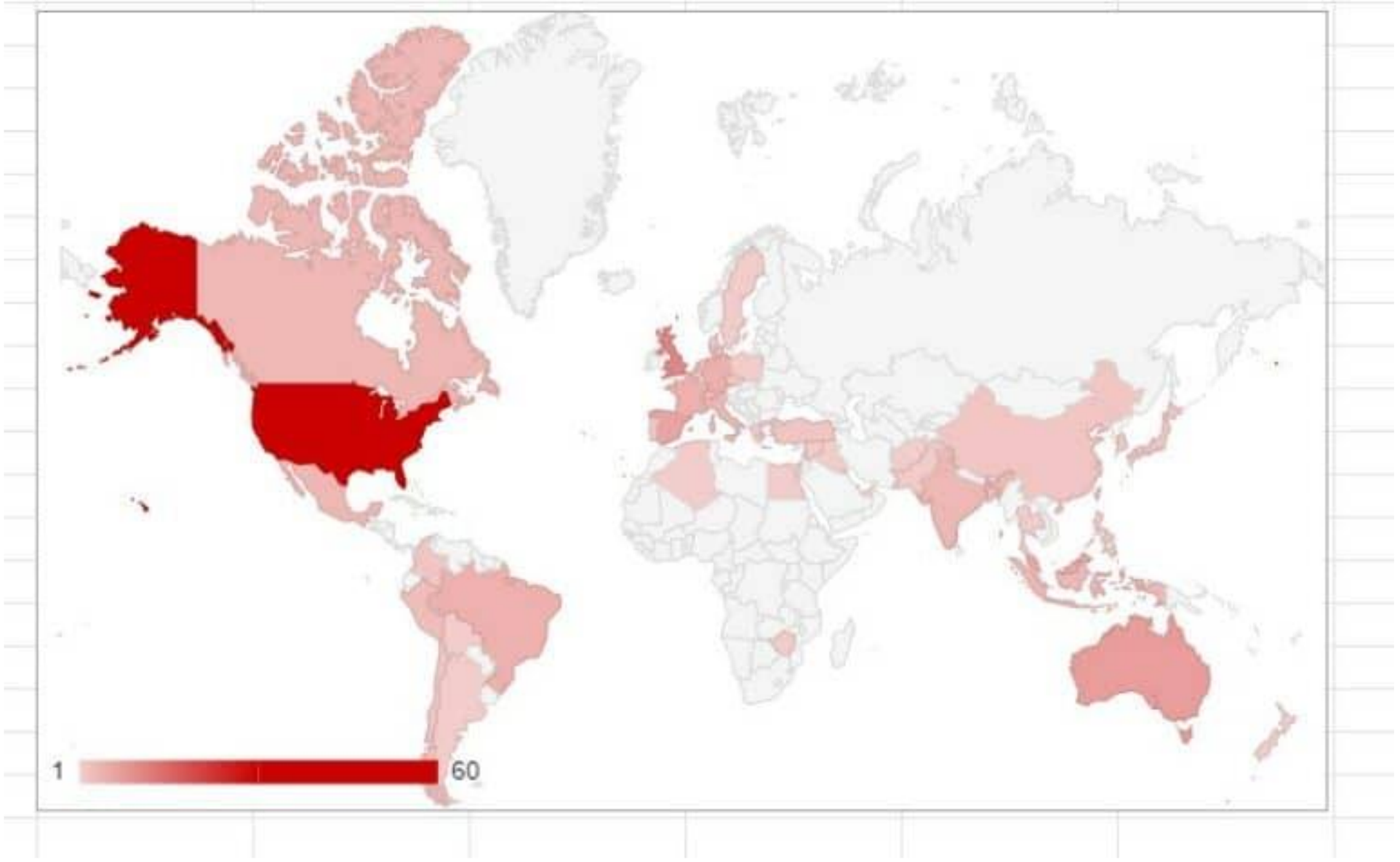
- Gebruikersnamen en wachtwoorden
- Gestolen mail
- Malware infecties
- Gecompromitteerde servers

Verkoop toegang tot netwerken door “eerste toegang” leveranciers



https://www.digitalshadows.com/blog-and-research/initial-access-brokers-in-q3-2021/

https://www.digitalshadows.com/blog-and-research/initial-access-brokers-in-q3-2021/


1
60

Wat zou jij doen als “leverancier” van eerste toegang?

- Er komt een publieke exploit uit voor een kwetsbaarheid in VPN oplossing
- Een systeembeheerder van jou organisatie zet RDP open

Antwoord

Business model zegt voor de VPN oplossing:

- als een dolle scannen wie kwetsbaar is
- Kwetsbare servers compromitteren
- Toegang verkopen op darkweb

Business model zegt voor de RDP oplossing:

- Standaard wachtwoorden en gebruikersnaam uitproberen
    - Gebruiker:admin wachtwoord: welkom123!
- Gelekte wachtwoorden
    - Oude wachtwoorden uit b.v. linkedin datalek, dropbox datalek

Vraag ransomware hackers

Stel je hebt toegang tot 100 netwerken → welk netwerk neem je?

Hacker vriendelijk netwerk!

- Veel “verplaats mogelijkheden”
- Legacy systemen
- Update cyclus traag
- Veel mensen met localadmin rechten


Given 2,500 potential target orgs
Access brokers sell access to compromised networks to ransomware-as-a-service affiliates, who run the ransomware attack
60 encounter activity associated with known ransomware attackers
RaaS affiliates prioritize targets by intended impact or perceived profit
20 are successfully compromised
Attackers take advantage of any security weakness they find in the network, so attacks vary
The ransomware payload is the culmination of a chain of malicious activity
1 org sees a successful ransomware event

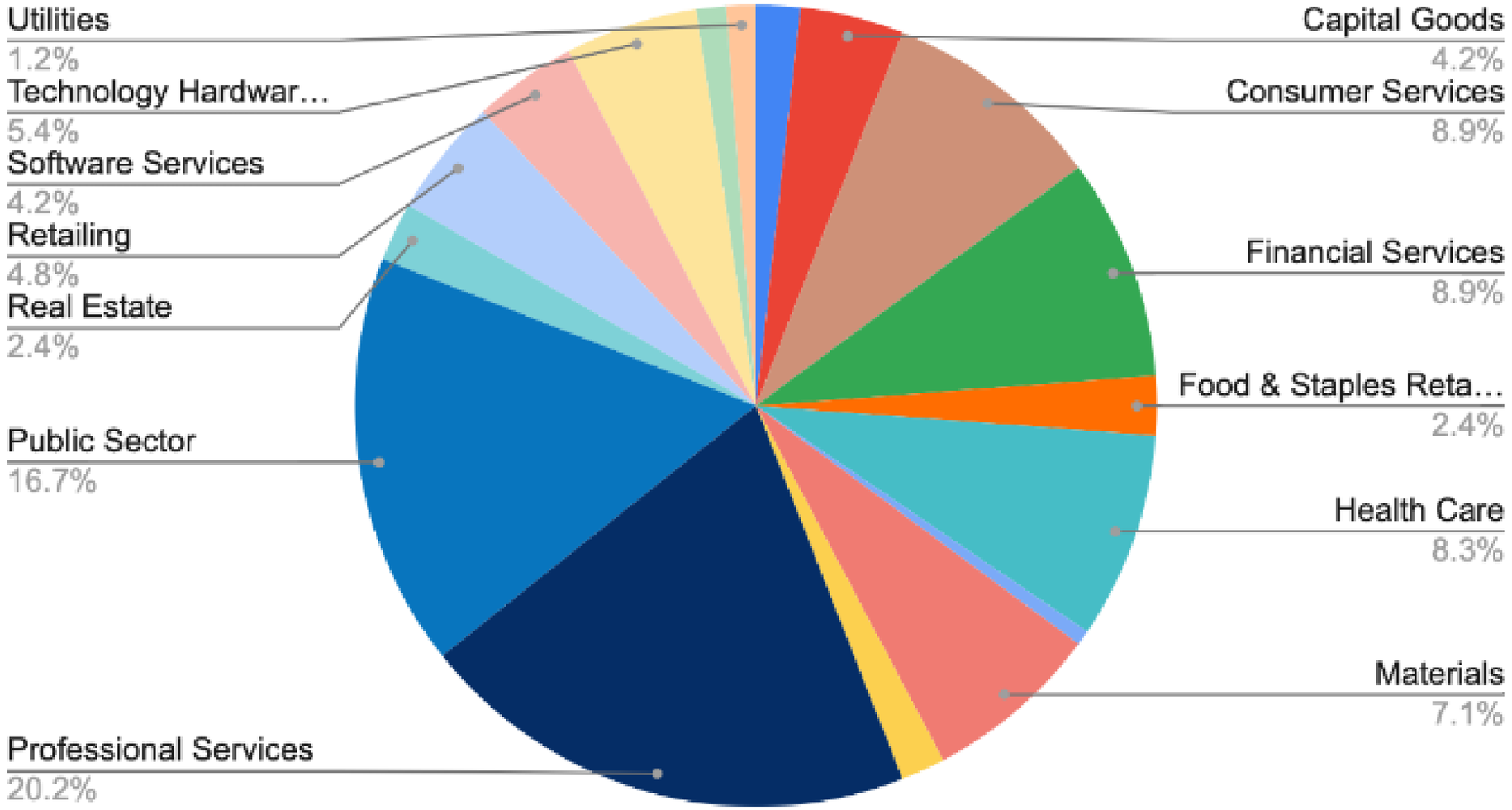
Het dreigingsbeeld

2 belangrijke vragen voor risico inschatting

- Wie is doelwit?
    - Sector?
    - Grootte organisatie?

- Impact

Common Industries Targeted by Ransomware Q1 2022

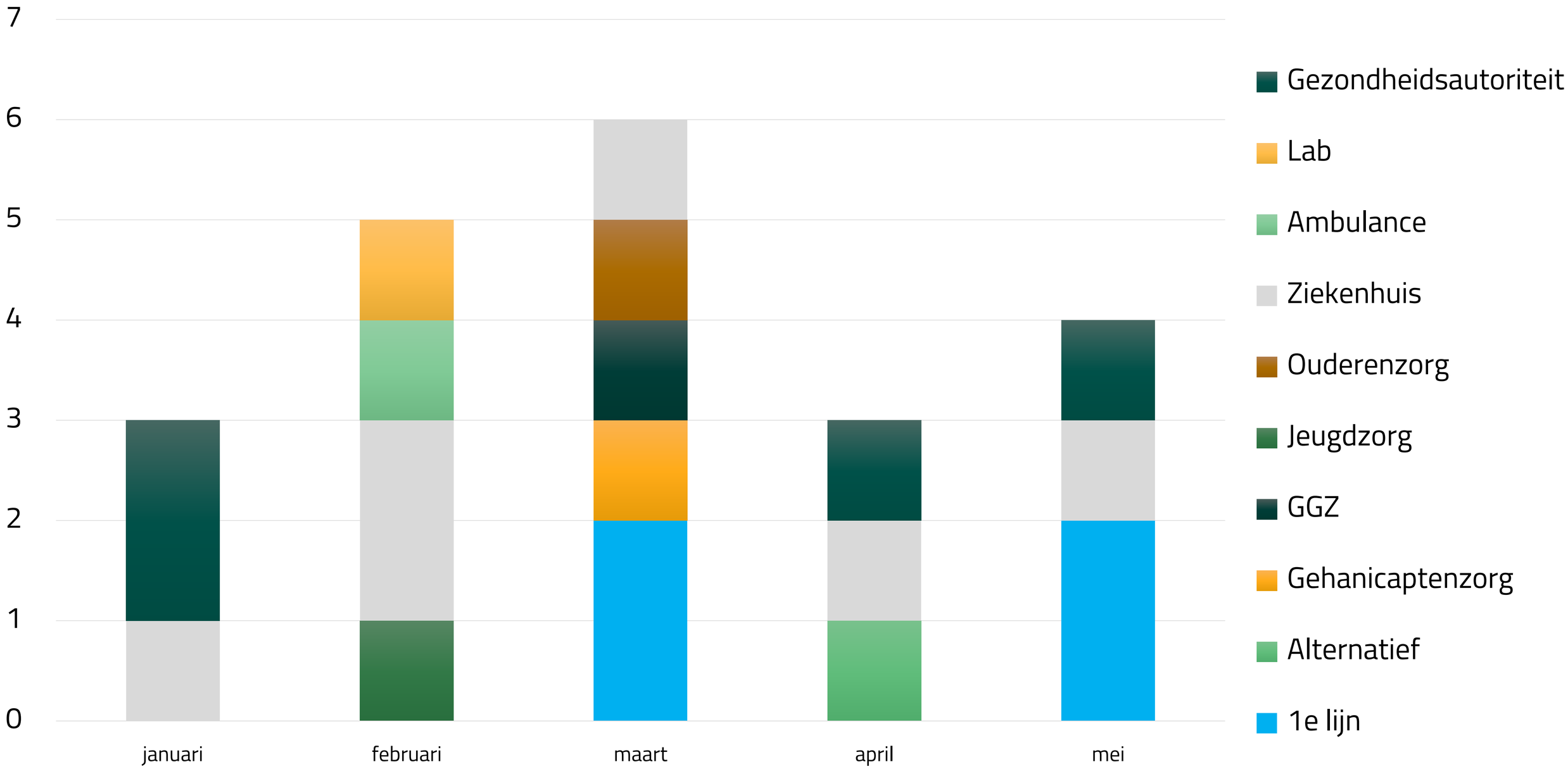


COVEWARE

3 belangrijke vragen voor risico inschatting

- Wie is doelwit?
    - Sector? **Breed spectrum (daar waar geld is)**
    - Grootte organisatie?
    - Hoe doelgericht zijn de aanvallen?

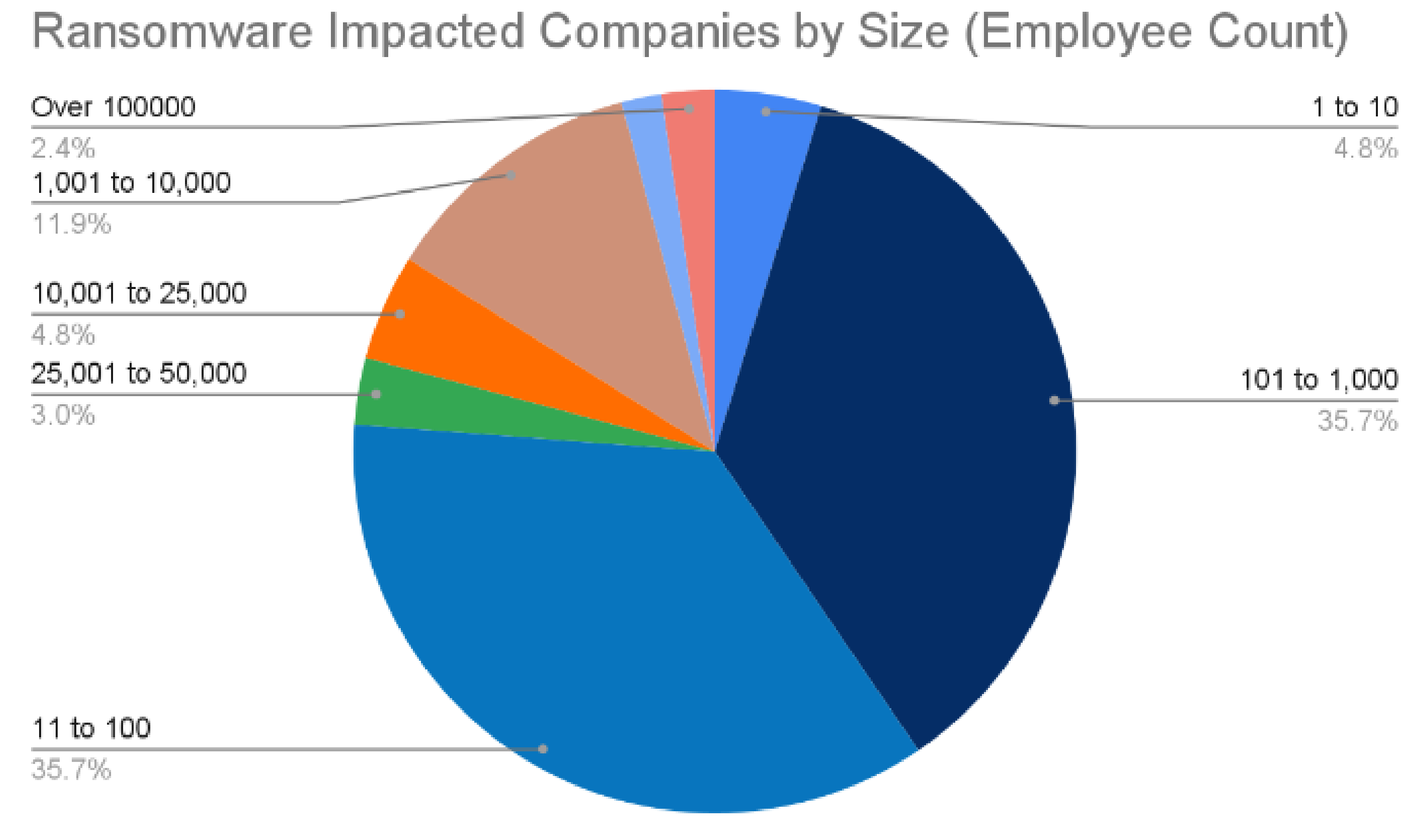
- Impact


7
6
5
4
3
2
1
0
januari
februari
maart
april
mei
Gezondheidsautoriteit
Lab
Ambulance
Ziekenhuis
Ouderenzorg
Jeugdzorg
GGZ
Gehanicaptenzorg
Alternatief
1e lijn

Voorzichtige conclusie

- Ook in de zorg: breed spectrum (daar waar geld is)

- Voor cybercrime geldt: klein = ook fijn!


Ransomware Impacted Companies by Size (Employee Count)
Over 100000
2.4%
1,001 to 10,000
11.9%
10,001 to 25,000
4.8%
25,001 to 50,000
3.0%
11 to 100
35.7%
1 to 10
4.8%
101 to 1,000
35.7%

COVEWARE

Waarom kleinere organisatie ook interessant?

3 belangrijke vragen voor risico inschatting

- Wie is doelwit?
    - Sector? **Breed spectrum (daar waar geld is)**
    - Grootte organisatie? **Breed spectrum (daar waar geld is)**
    - Hoe doelgericht zijn de aanvallen?

- Impact

Hoe doelgericht zijn de aanvallen?

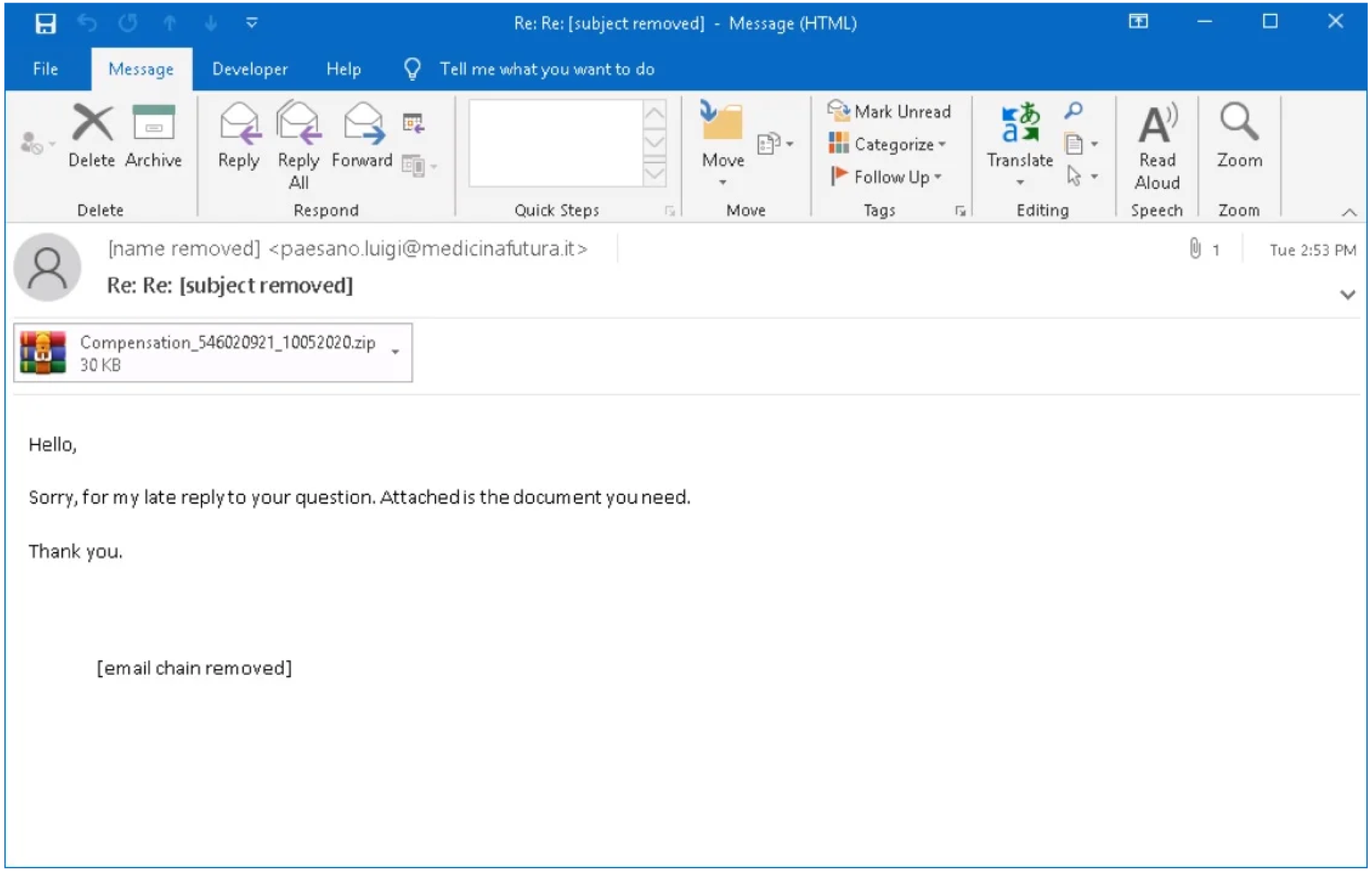
Waarom wil ik dit weten?

- Waarschijnlijkheid van incident groter naar mate de aanvaller doelgerichter wordt

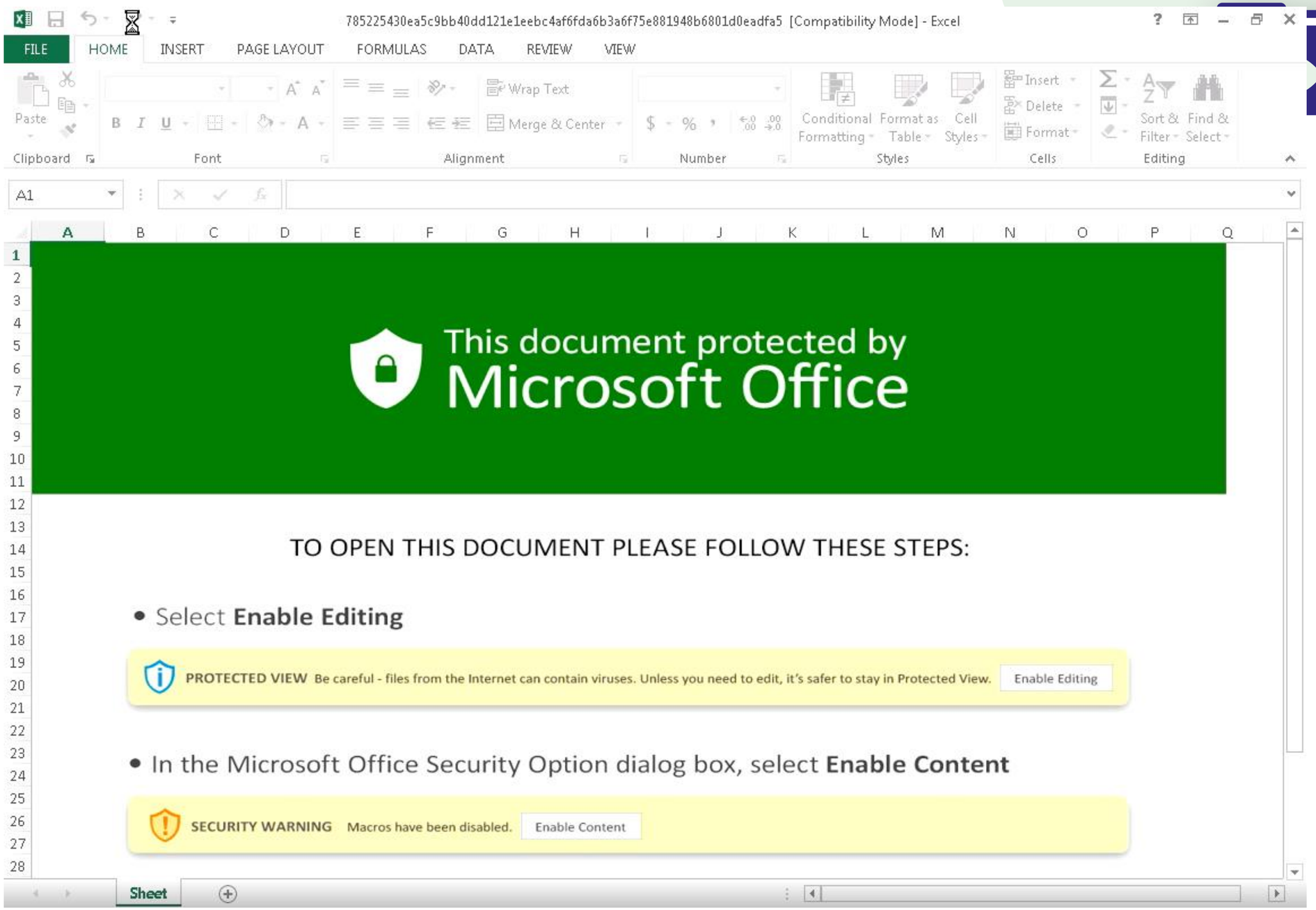
TABLE D-5: ASSESSMENT SCALE – CHARACTERISTICS OF ADVERSARY TARGETING

Qualitative Values	Semi-Quantitative Values		Description
Very High	96-100	10	The adversary analyzes information obtained via reconnaissance and attacks to target persistently a specific organization, enterprise, program, mission or business function, focusing on specific high-value or mission-critical information, resources, supply flows, or functions; specific employees or positions; supporting infrastructure providers/suppliers; or partnering organizations.
High	80-95	8	The adversary analyzes information obtained via reconnaissance to target persistently a specific organization, enterprise, program, mission or business function, focusing on specific high-value or mission-critical information, resources, supply flows, or functions, specific employees supporting those functions, or key positions.
Moderate	21-79	5	The adversary analyzes publicly available information to target persistently specific high-value organizations (and key positions, such as Chief Information Officer), programs, or information.
Low	5-20	2	The adversary uses publicly available information to target a class of high-value organizations or information, and seeks targets of opportunity within that class.
Very Low	0-4	0	The adversary may or may not target any specific organizations or classes of organizations.

Bron: https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-30r1.pdf



Bron: https://www.bleepingcomputer.com/news/security/qbot-uses-windows-defender-antivirus-phishing-bait-to-infect-pcs/


785225430ea5c9bb40dd121e1eebc4af6fda6b3a6f75e881948b6801d0eadfa5 [Compatibility Mode] - Excel
FILE
HOME
INSERT
PAGE LAYOUT
FORMULAS
DATA
REVIEW
VIEW
Paste
Clipboard
Font
Wrap Text
Merge & Center
Alignment
Number
Conditional Formatting
Format as Table
Cell Styles
Styles
Insert
Delete
Format
Cells
Sort & Filter
Find & Select
Editing
A1
This document protected by
Microsoft Office
TO OPEN THIS DOCUMENT PLEASE FOLLOW THESE STEPS:
Select Enable Editing
PROTECTED VIEW Be careful - files from the Internet can contain viruses. Unless you need to edit, it's safer to stay in Protected View.
Enable Editing
In the Microsoft Office Security Option dialog box, select Enable Content
SECURITY WARNING Macros have been disabled.
Enable Content
Sheet

Tip: bepaal de “doelgerichtheid” van je malspam

Doelgerichtheid waarde 10:

- Van boven tot onder doorgelicht

Doelgerichtheid waarde 1:

- Standaard generieke methoden

Impact

Impact

Average Ransom Payment

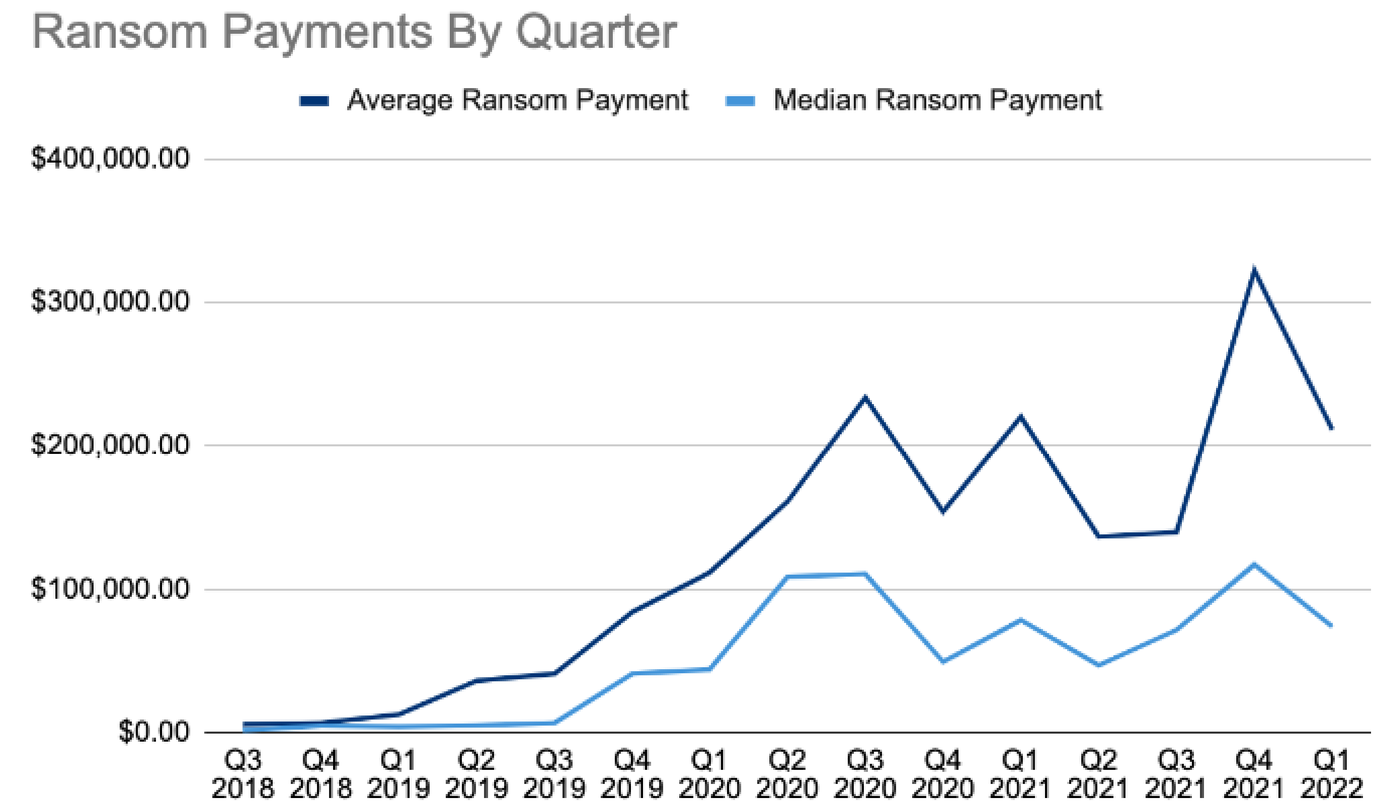
$211,529

-34% from Q4 2021

Median Ransom Payment

$73,906

-37% from Q4 2021



COVEWARE

Impact

- Gemiddeld wordt 61% encrypted data herstelt na betaling ransomwaregroep

Bron: https://assets.sophos.com/X24WTUEQ/at/4zpw59pnkpxxnhfhgj9bxgj9/sophos-state-of-ransomware-2022-wp.pdf

$1.4M

average cost to remediate an attack

ONE MONTH

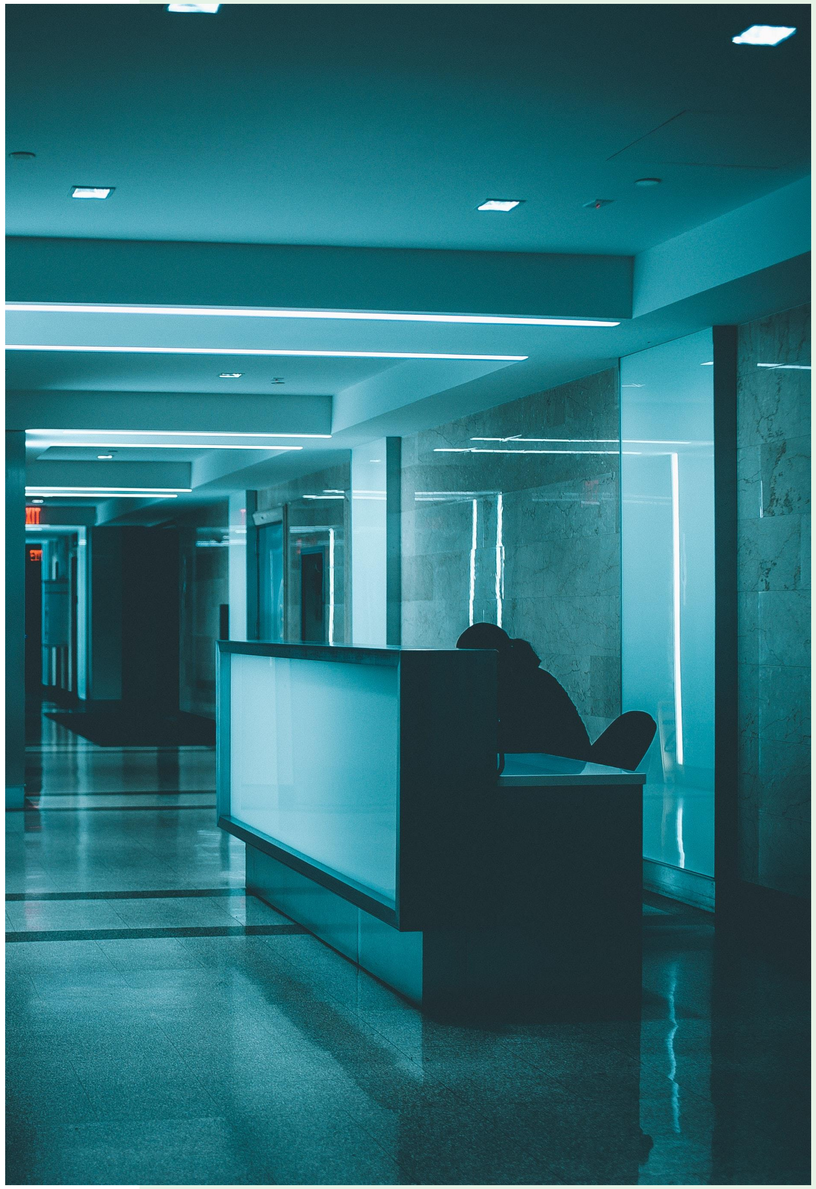
average time to recover from an attack

Bron: https://assets.sophos.com/X24WTUEQ/at/4zpw59pnkpxxnhfhgj9bxgj9/sophos-state-of-ransomware-2022-wp.pdf

Inhoud presentatie

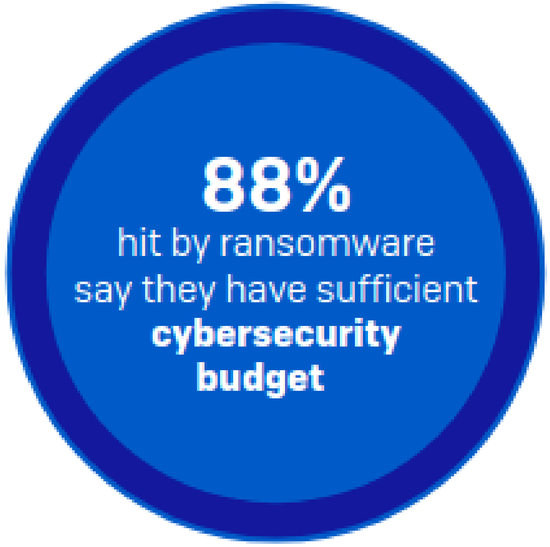
- Update dreigingsbeeld / impact

- **Hoe gaan ze te werk? Prioriteiten?**



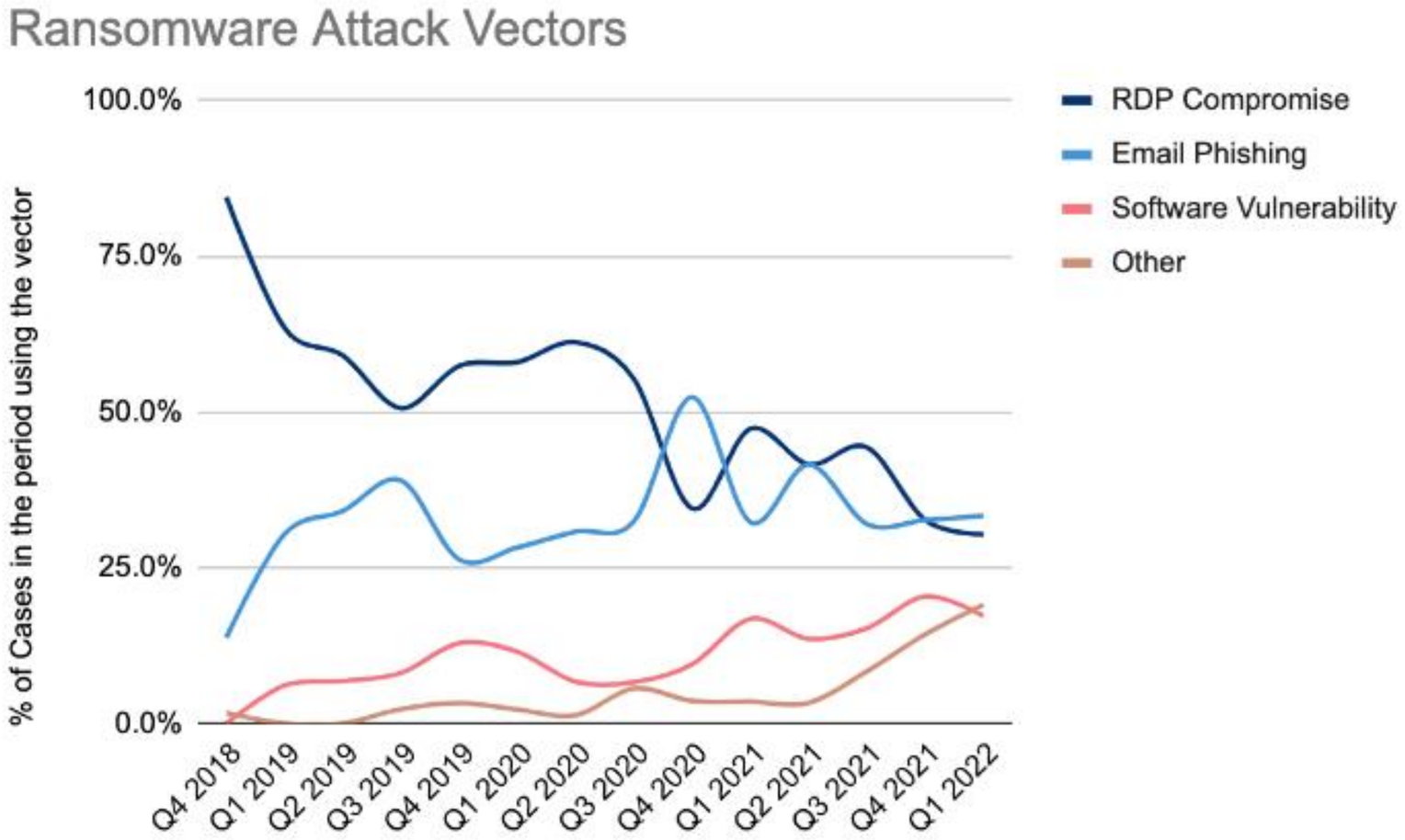
Resources effectiever inzetten!

Hoe? → know your enemy



Bron: https://assets.sophos.com/X24WTUEQ/at/4zpw59pnkpxxnhfhgj9bxgj9/sophos-state-of-ransomware-2022-wp.pdf

Hoe werken ze?



COVEWARE

Prioriteiten lijstje:

1. RDP niet ontsloten aan het internet of alleen via VPN of gatewayoplossing
    - Zorginstelling in Nederland afgelopen jaar
    - Hof van Twente

- Soms per ongeluk ontsloten aan het internet!
    - Monitoring! Niet duur…

- RDP de “even snel doen” oplossing voor sysadmins

Prioriteiten lijstje:

1. RDP niet ontsloten aan het internet
    1. Achter VPN of gateway oplossing (met multi-factor)

2. Phishing met malware
    1. Scripts en programma’s vanaf het internet mogen niet uitgevoerd worden
    2. Office macro’s afkomstig van het internet mogen niet worden uitgevoerd

3. Phishing voor wachtwoorden
    1. Multi-factor authenticatie

4. Vulnerability management

Maar stel ze zijn binnen.....

CSW Cyber SecurityWorks

MITRE ATT&CK MAP Conti Ransomware

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Command & Control	Exfiltration	Impact
Phishing: Spear Phishing Link	User Execution: Malicious Link	Valid Accounts: Domain Accounts	Valid Accounts: Domain Accounts	Valid Accounts: Domain Accounts	Exploitation for Credential Access	System Network Configuration Discovery	Exploitation of Remote Services	Proxy: External Proxy	Exfiltration Over Web Service: Exfiltration to Cloud Storage	Data Encrypted for Impact
Exploit Public-Facing Application	Windows Management Instrumentation	Create Account	Process Injection	Use Alternate Authentication Material: Pass the Hash	OS Credential Dumping	Remote System Discovery	Remote Services: SMB/Windows Admin Shares	Application Layer Protocol		
Valid Accounts: Domain Accounts	Command and Scripting Interpreter		Domain Policy Modification: Group Policy Modification	Process Injection		Network Service Scanning	Remote Services: Remote Desktop Protocol			
	System Services: Service Execution		Access Token Manipulation	Domain Policy Modification: Group Policy Modification		System Owner/User Discovery				
			Impair Defenses	Access Token Manipulation		Permission Groups Discovery				
				Impair Defenses		Account Discovery: Domain Account				

Waar te beginnen?

De regels van het spel

De regels van het spel

- Doel 1: stelen wachtwoorden
    - Waarom?
- Doel 2: “localadmin” toegang
    - Waarom?
- Doel 3: verplaatsen naar computer waar iemand (of een service) draait met hogere rechten
    - Waarom?
- Doel 4: stelen hogere rechten/wachtwoorden
- Doel 5 en 6: data-exfiltratie en uitrollen ransomware

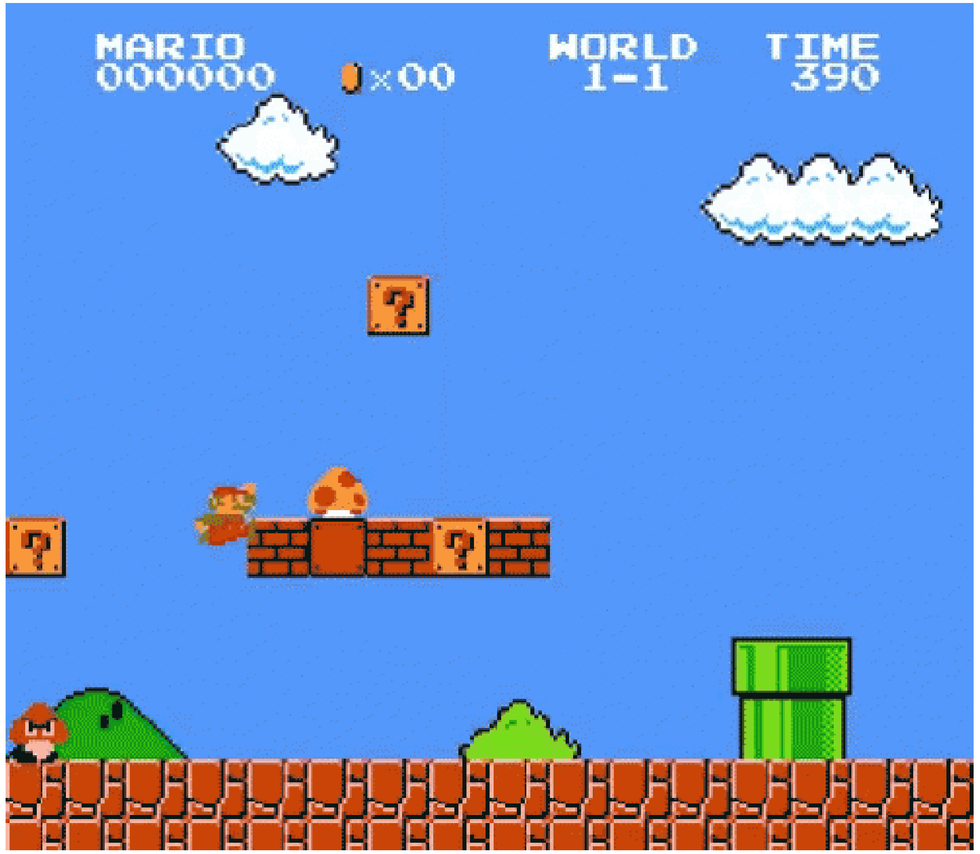
Doel 2: local admin rechten

- Kan stelen van iedereen die is ingelogd (ook domain admins)
  - Tickets
  - Wachtwoorden
  - Actieve sessies

- Wanneer mogelijk?
  - Iemand heeft al local admin rechten
  - “Privelage escalation” kwetsbaarheid
  - Configuratie fout

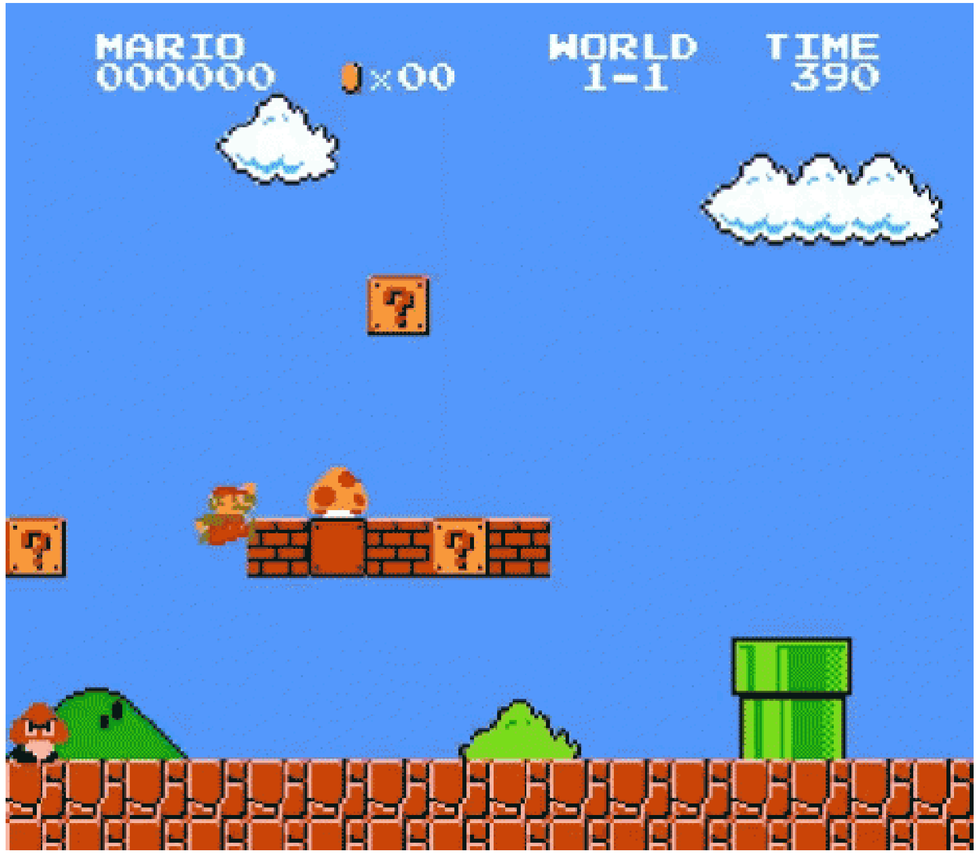
Doel 2:

- Upgrade van hacker wat betreft rechten

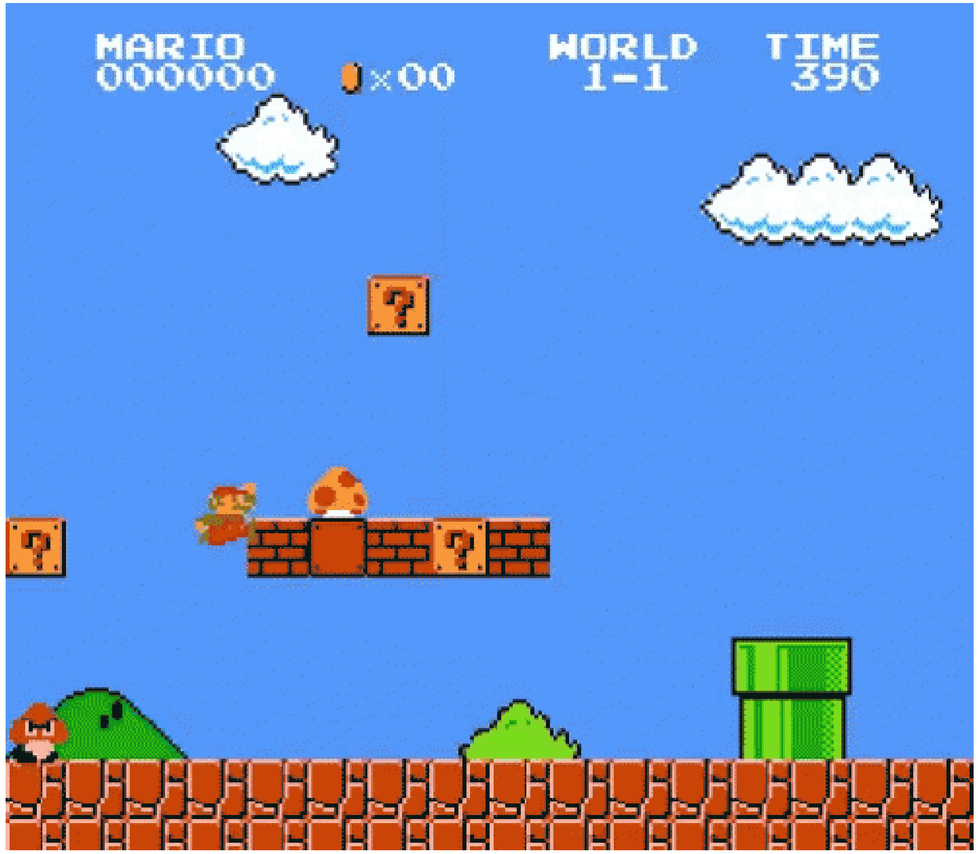


Bij OS niet gepatched denk je voortaan:

- Upgrade van hacker wat betreft rechten



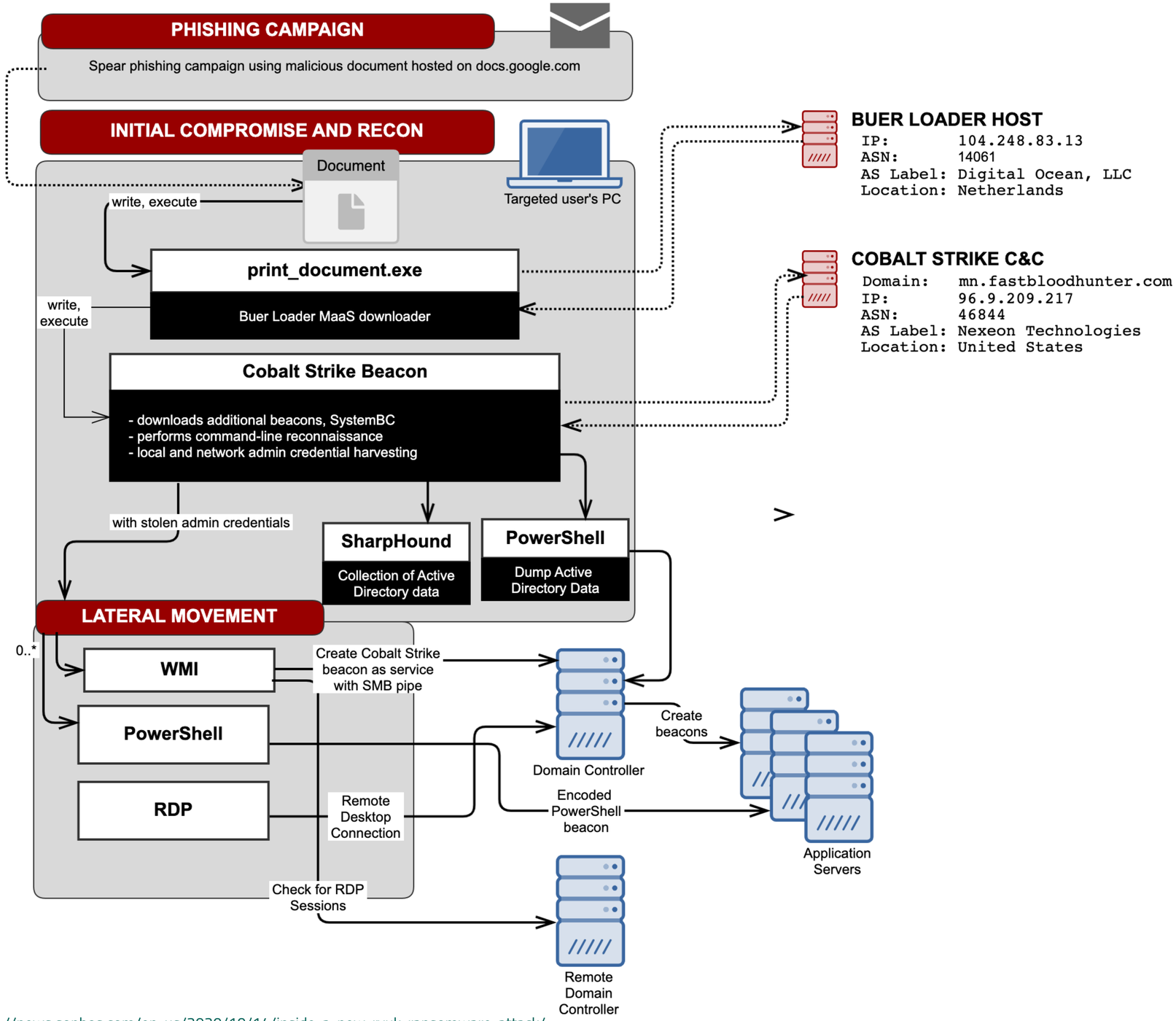
Bij localadmin rechten denk je voortaan



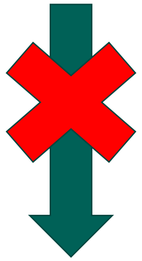
De regels van het spel

- Doel 1: stelen wachtwoorden
    - Waarom?
- Doel 2: “local admin” toegang
    - Waarom?
- **Doel 3:** verplaatsen naar computer waar iemand (of een service) draait met hogere rechten
    - Waarom?
- Doel 4: stelen hogere rechten/wachtwoorden
- Doel 5 en 6: data-exfiltratie en uitrollen ransomware

RDP
SMB/RPC
Powershell remoting
WMI



Bron: https://news.sophos.com/en-us/2020/10/14/inside-a-new-ryuk-ransomware-attack/



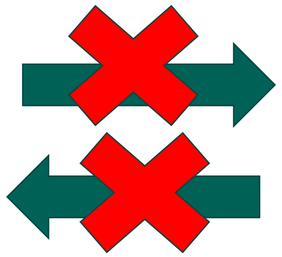
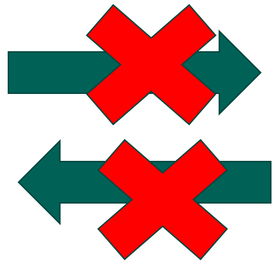
RDP
SMB/RPC
WMI
Powershell remoting
NIET inloggen met HOGE rechten

Localadmin rechten = is wachtwoordsteelrechten + rechten steel rechten

- Serverbeheerder op gebruikerscomputer = happy hacker
  - Hacker kan alle rechten overnemen
  - Kan wachtwoorden stelen
  - Kan sessies overnemen



RDP
WMI
SMB!!!
Powershell remoting

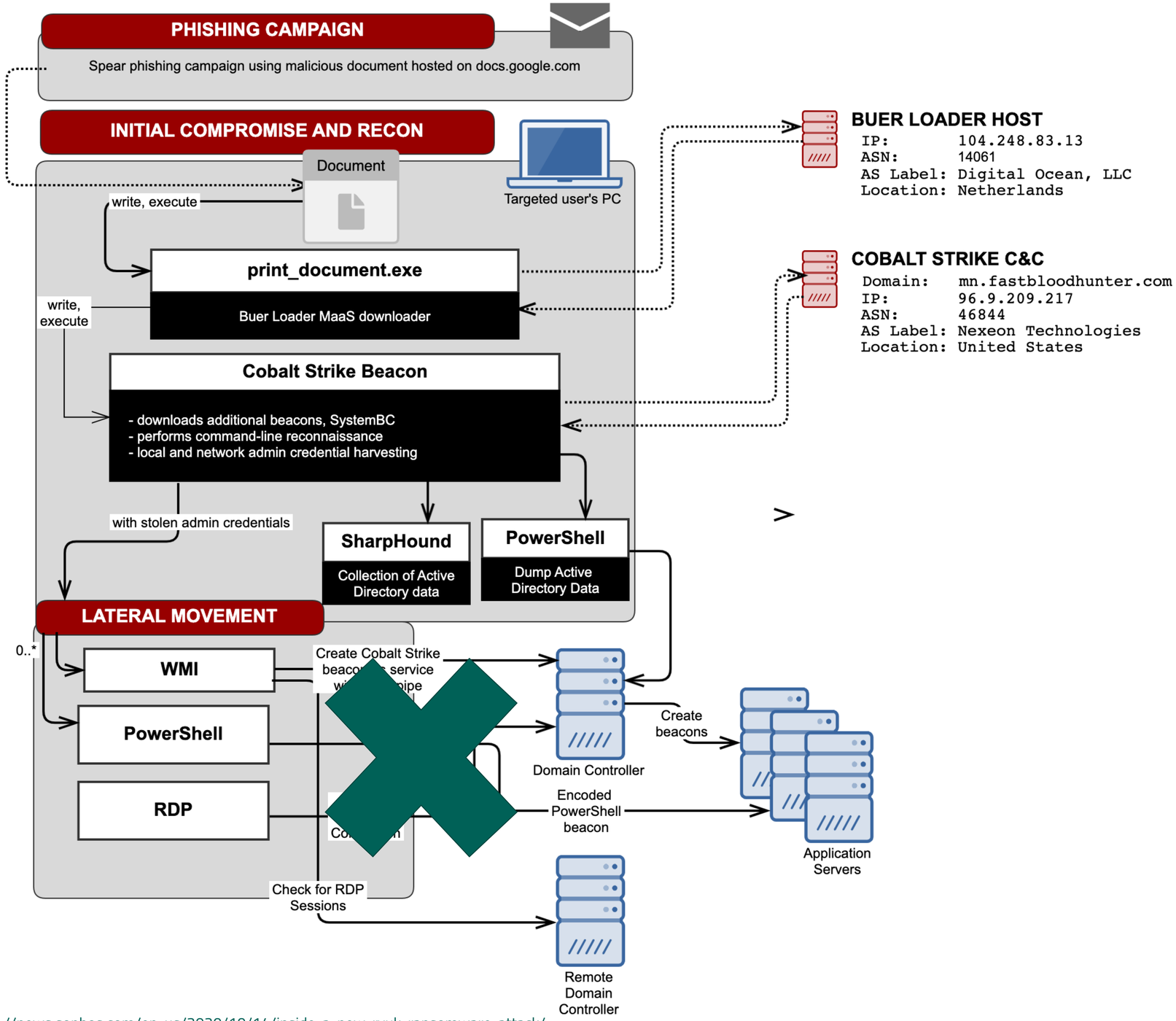

Hoe dan wel

RDP
SMB
Powershell remoting

Privilege access workstation

Met LAPS (iedere PC eigen unieke localadmin)

Geen localadmin rechten!



Bron: https://news.sophos.com/en-us/2020/10/14/inside-a-new-ryuk-ransomware-attack/

Take away message

- Denk vanuit het ransomware business plan
- Innitial access: 4 prioriteiten
- Inventariseer de sluiproutes en reguleer/blokkeer
- Localadmin rechten = “gebruiker overneem rechten”
- Ongepatchte Windows → localadmin rechten door misbruik kwetsbaarheden

Vragen?

Stichting Z-CERT
www.z-cert.nl

Lateral Movement

Lateral Movement

T1021: Remote Services	27.4%	T1021.001: Remote Desktop Protocol	23.4%
		T1021.004: SSH	4.8%
		T1021.002: SMB/Windows Admin Shares	4.0%
		T1021.005: VNC	0.5%
		T1021.006: Windows Remote Management	0.2%
T1550: Use Alternate Authentication Material	0.8%	T1550.002: Pass the Hash	0.5%
		T1550.001: Application Access Token	0.2%
		T1550.003: Pass the Ticket	0.2%
T1570: Lateral Tool Transfer	0.6%		
T1534: Internal Spearphishing	0.5%		

Initial Compromise

Initial Access

T1190: Exploit Public-Facing Application	25.8%		
T1195: Supply Chain Compromise	11.1%	T1195.002: Compromise Software Supply Chain	11.1%
T1133: External Remote Services	8.8%		
T1566: Phishing	8.6%	T1566.001: Spearphishing Attachment	4.3%
		T1566.002: Spearphishing Link	3.5%
T1078: Valid Accounts	6.3%		
T1189: Drive-by Compromise	4.3%		
T1199: Trusted Relationship	0.6%		