

State of Ransomware in SA

The true impact on businesses in SA



State of Ransomware in SA



Anna Collard

SVP of Content Strategy
& Evangelist, KnowBe4
Africa



Charl van der Walt

Head of Security
Research, Orange
Cyberdefense



Agenda

- Ransomware Trends
- Survey Results
- Prevent & Mitigate
- Systemic & criminology response

Public Shaming



LEAKED DATA

CONDITIONS FOR PARTNERS AND CONTACTS

pulmuonewildwoo...

80 1M 31M 33 S

another small parts of files

MORE

ebarc.adv.br

80 20M 16M 33 S

EDUARDO BIONDI & ANTONIO RICARDO CORRÊA ADVOGADOS ASSOCIADOS

MORE

wijnendeclerck....

50 18M 29M 34 S

Wijnen De Clerck is a family wine trade from Kortrijk that was founded in 1972 by Paul De Clerck. Meanwhile, the second generation is active in the company. Bert and Emanuele both received different...

MORE

hoffsuemmer.de

80 18M 27M 34 S

Nearly 150 years of tradition and experience in paper manufacturing. In 1895, the brothers Clemens August, Carl and Gustav Hoffmüller founded our company Gebr. Hoffmüller Spezialpapier GmbH & Co...

MORE

esopro.com

80 18M 21M 34 S

eSoftware Professionals is a Gold Certified member of the Microsoft Partner Network and customizes Enterprise Resource Planning (ERP) software for distribution chains, the food processing industry, an...

MORE

drhrlaw.com

70 7M 51M 33 S

More than twenty-five years ago, James Elai Doyle, Ronald J. Restrepo, Andrew R. Harvin and Michael D. Robbins opened the firm, having previously practiced together at a large multi-city firm for sever...

MORE

The GDPR at Article 33 requires that, in the event of a personal data breach, data controllers should notify the appropriate supervisory authority without undue delay and, where feasible, not later than 72 hours after having become aware of it.

Griefs in progress...

CROMOLOGY SERVICES
Worse than we are

Complete Griefs...

Mobile County, Alabama
PCM Group
ATV CYBER SECURITY
LENSBURY LIMITED
Kocks Arden Kranbau GmbH

Grief came to: _

CROMOLOGY SERVICES

URL: <https://www.cromology.com/>

READ MORE

Views: 7164 | Published: 2023-09-10 13:17:55 | Updated: 2023-09-19 23:43:45

★ Mobile County, Alabama

Know your enemy..

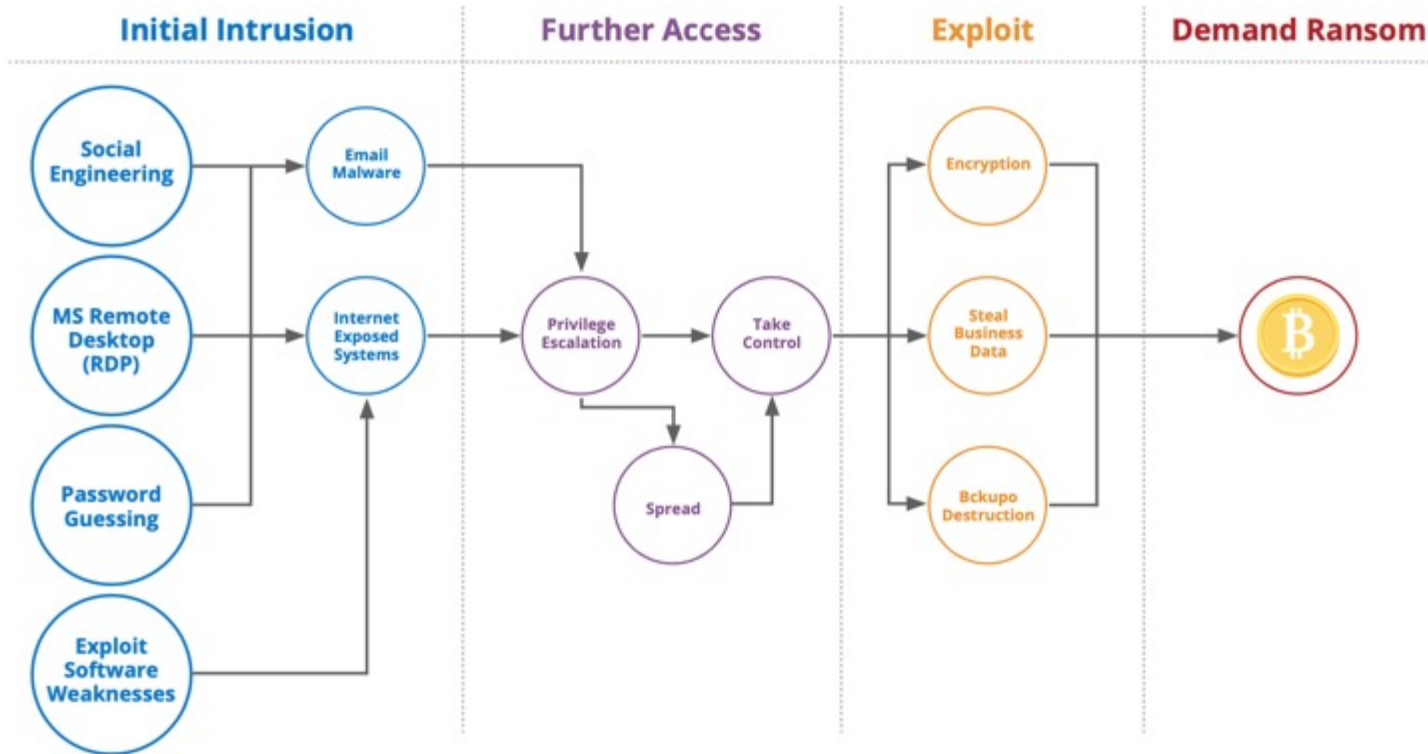



Figure 2: Ransomware kill chain


Public Shaming






Buy the Avaddon decryptor · What's the matter? · Test decryption · 24/7 support · Our Blog · English


Your network has been infected by Avaddon
Don't worry, we can help you to restore all your files!
Avaddon General Decryptor price is: **200000 USD**
If you don't pay before the time runs out, your documents, photos, databases and other important files will be published at our blog - [malwareintelligence.com](#)!
Where they will be freely available and anyone can watch them absolutely free. What will entail the loss of clients, money and lawsuits.




All your documents, photos, databases and other important files have been encrypted!



To restore all your files you need to buy our special software - **Avaddon General Decryptor**!




You can do it right now. Follow the instruction below. But remember that you do not have much time!



200000 USD
= 4.08138467 BTC
bc1gpk7h94eyef5rtxt390v0u0cvc76fkuz5dz7za
NOT RAB

1. Buy the Bitcoin cryptocurrency. You will find instructions how you can do it below.
2. Send 4.08138467 BTC to the address: **bc1gpk7h94eyef5rtxt390v0u0cvc76fkuz5dz7za** (in ONE payment, this amount doesn't include the transaction fee)
3. The transaction will be confirmed after receiving 6 confirmations
4. When the payment is confirmed, you can download the **Avaddon General Decryptor**.

Attention!
Please be careful and visually check the address after copy-paste (because on your PC there is probably a malware monitoring and changing the address in your clipboard)



Congratulations! Payment has been made successfully!

18.08.27.02.2021
<https://pomp.pl/>

18.08.27.02.2021
password: 137925

18.08.27.02.2021
3. Okay thank you. What about the file tree? That was part of the agreement too

18.08.27.02.2021
1. Can you please also tell me how you got onto the network

18.08.27.02.2021
2. About vulnerabilities in your network. These are weak passwords and old operating systems, the operating systems that you used have vulnerabilities, with the help of them an attack was carried out on your network. Use strong passwords and hide them as best as possible and update all your OS to the latest versions.

18.08.28.02.2021
Did you come through RDP then? Do you not have the file tree?

18.08.28.02.2021
4. All files are destroyed, we can no longer provide you with any information.

18.08.28.02.2021
5. Okay, can you confirm if this was RDP then? Or are you saying we have a different vulnerability somewhere

18.08.28.02.2021
6. Yes, RDP

Type your message...

Online negotiations



CONTI Recovery service

Hello. I have come to the chat and have full authority to negotiate from my manager. What do we need to do to get our data back? Can you help?

15 days ago



Please, introduce yourself (Company name and your position) and we'll provide all necessary information. Sometimes our staff is busy, but we will reply as soon as possible. Be in touch, thank you

14 days ago



I am a IT lead technician with ExaGrid Systems.

14 days ago



As you already know, we infiltrated your network and stayed in it for more than a month(enough to study all your documentation), encrypted your file servers, sql servers, downloaded all important information with a total weight of more than 800 GB: personal data of clients (home addresses, SSN phone numbers of the contract), employees (SSN, home addresses, employment contracts, scans of personal documents, phone numbers), contracts with partners, NDA forms, customer bases, consolidated financial statements, payroll, tax returns, settlements with partners, bank statements, source code and etc. The good news is that we are businessmen. We want to receive ransom for everything that needs to be kept secret, and don't want to ruin your business. The amount at which we are ready to meet you and keep everything as collateral is \$ 7,480,000.

14 days ago

Online negotiations



We are ready to accept \$2.6M

6 days ago

Okay, we will set up a call with the board members to get them to agree to the \$2.6M. It will take an hour or two to get them together. Once we get approval we will start the fund transfer process.

6 days ago



Ok.

6 days ago

It was a tough call but we did get the board approval for \$2.6M. We are starting the process of wiring the funds please give instructions.

6 days ago



Our BTC wallet is 1JWnZmkJwJSK6F21nypCAGzsR6TVhPRA4P

6 days ago

Hello. We are preparing to send the payment shortly. Please confirm that this is the correct BTC wallet. 1JWnZmkJwJSK6F21nypCAGzsR6TVhPRA4P

6 days ago

Hello. Can you confirm before we send it? We don't want it to go to the wrong address. Thanks!

6 days ago

Good Evening. Just checking to see if someone can confirm the BTC wallet, please.

5 days ago



Our BTC wallet is 1JWnZmkJwJSK6F21nypCAGzsR6TVhPRA4P

5 days ago

Good Morning. Thank you for confirming. We will be sending the payment shortly. Please let me know when you receive it.

5 days ago



Payment received. We will now prepare everything you need.

5 days ago

Thank you.

5 days ago

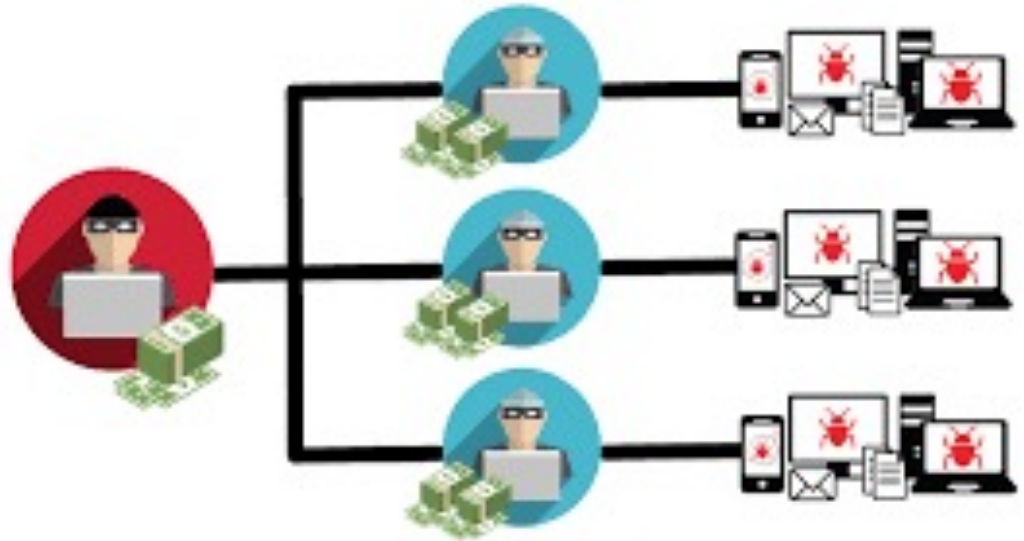


Ransomware Ecosystem



- Run like a business with CEOs, incentives, partners (affiliates)
- FBI tracked 100 different ransomware strains
- Focus on different sectors and regions?

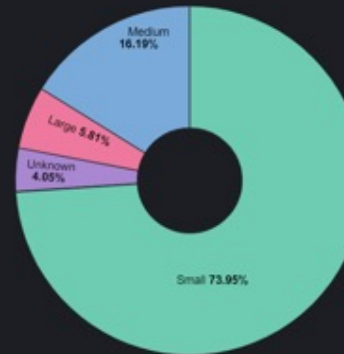
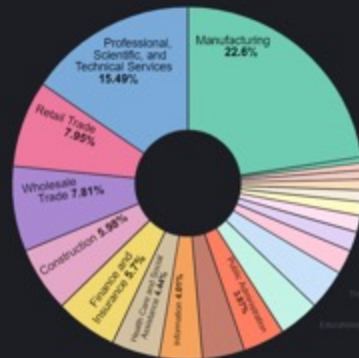
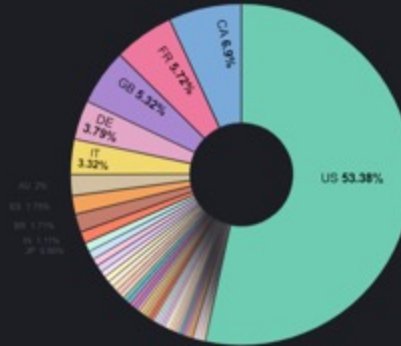
Ransomware-as-a-Service



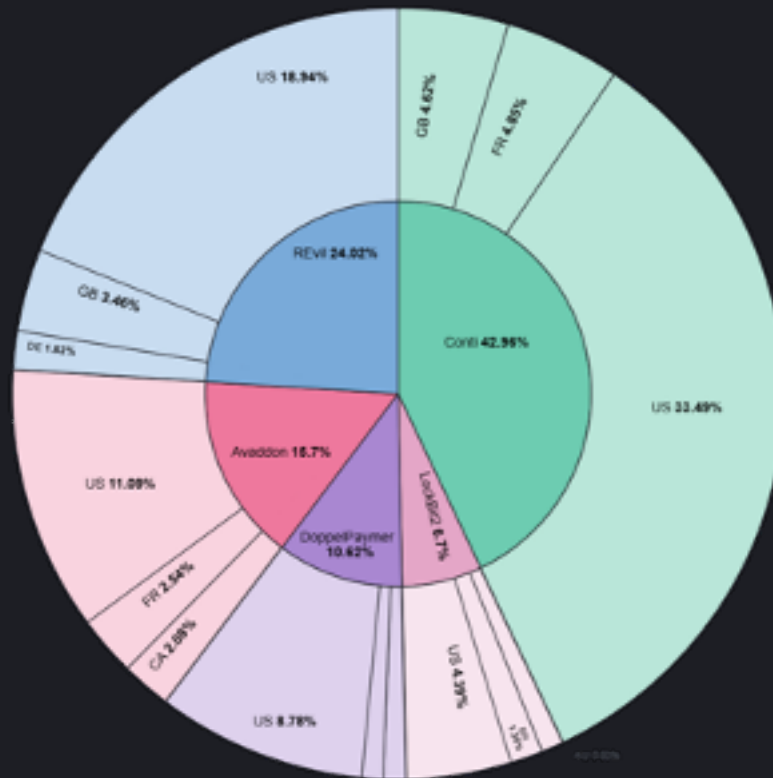
Players and Victims



2,841 leaks



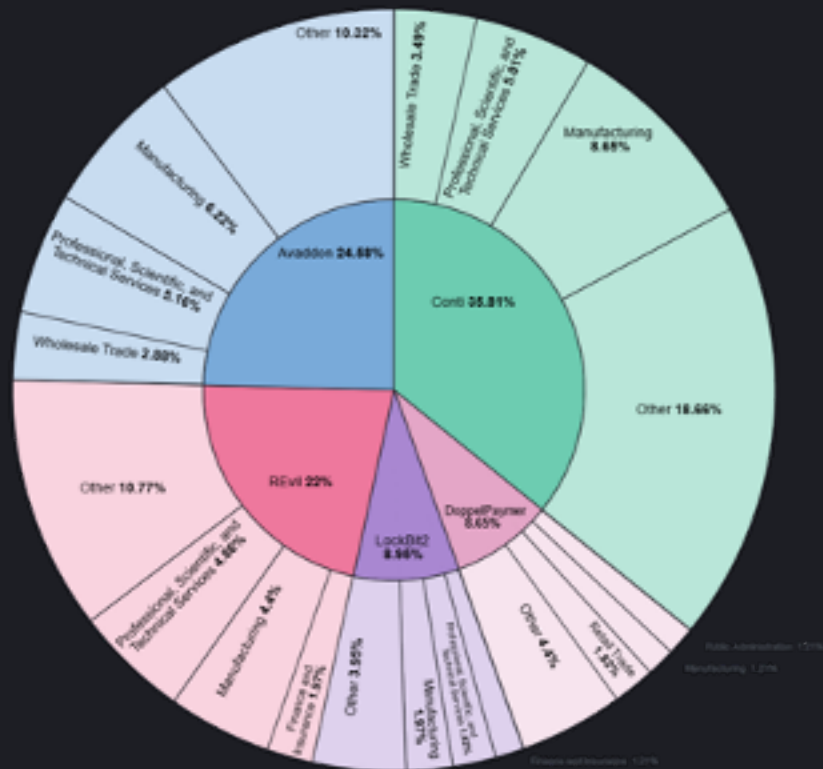
Victimology and Targetting



Victimology and Targetting



- Conti
- Avaddon
- REvil
- LockBit
- DoppelPaymer





Malware: any software that has been designed to operate in a malicious, undesirable manner, without the informed consent of the computer owner or user.



Ransom: a consideration paid or demanded for the release of someone or something from captivity¹.



Ransomware: malware that holds the data of a computer user for ransom.



Big game hunting: a targeted ransomware operation that involves infiltrating large corporate or government networks that will be significant and lucrative.



Extortion: is the act or practice of wresting anything from a person by force, duress, menace, authority².



Cy-X is a form of computer crime in which the security of a corporate digital asset (Confidentiality, Integrity or Availability) is compromised and exploited in a threat of some form to extort a payment.



Ransomware 2.0



[Bonaci Group](#) [Blog](#) [Data Market](#) [About Us](#) [Contact Us](#)

About Us

Welcome to our insider team "Bonaci Group".

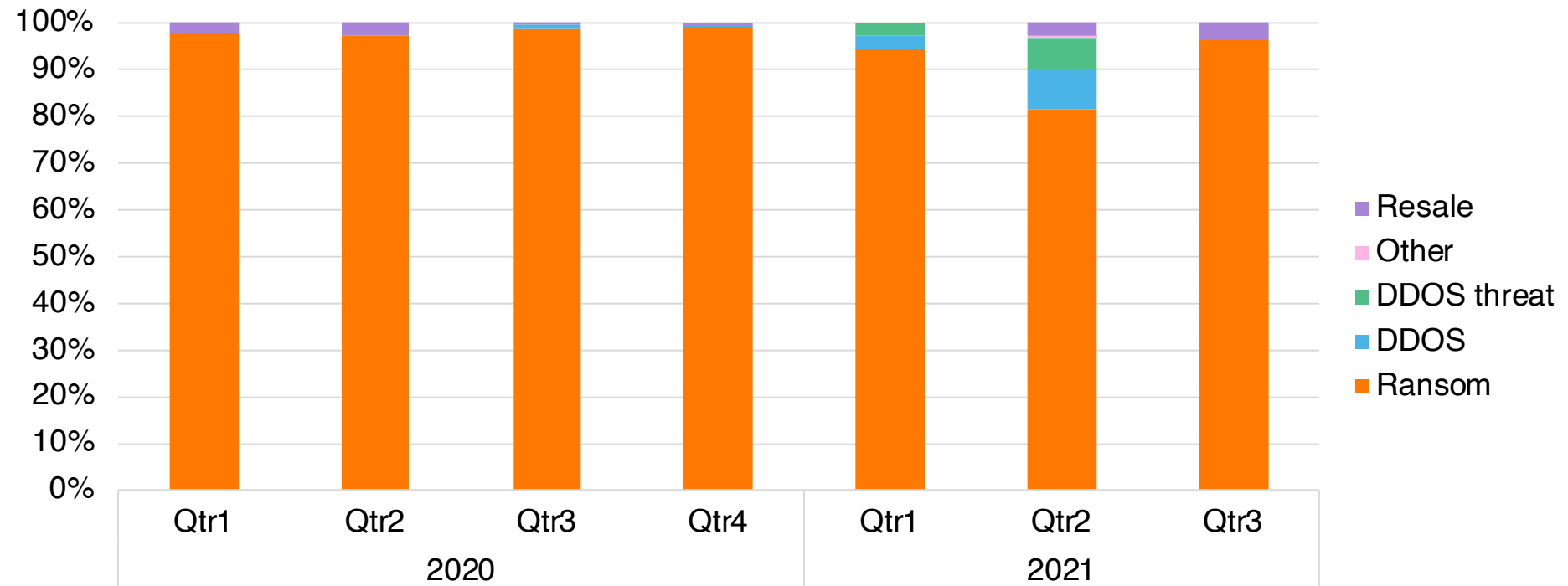
We are testing security systems of companies in order to steal their confidential data.

We are not engaged in data encryption, we only sell our silence about data breaches and security vulnerabilities found.

80% of all funds received are for charitable purposes.

If the company refuses to pay for silence, their data will be posted on the blog, and the fact of confidential data will be made public.

Ransomware 2.0



There is something of an **unexpressed complicity**: between the **pirates**, who threaten liberty but by and large not the lives of crews and maintain their ransom demands at levels which the **industry** can tolerate; the world of **commerce**, which has introduced precautions but advocates the freedom to meet the realities of the situation by the use of ransom payments; and the world of **government**, which stops short of deploring the payment ransom but stands aloof, participates in naval operations but on the whole is unwilling to combat pirates with force



What does this mean for us in SA?



Downtime direct impact on SA economy

SA's advanced economy has sectors highly cyber dependent

Reduced confidence in South Africa as the gateway to Africa

As developed economies clamp down, more attention to African organisations



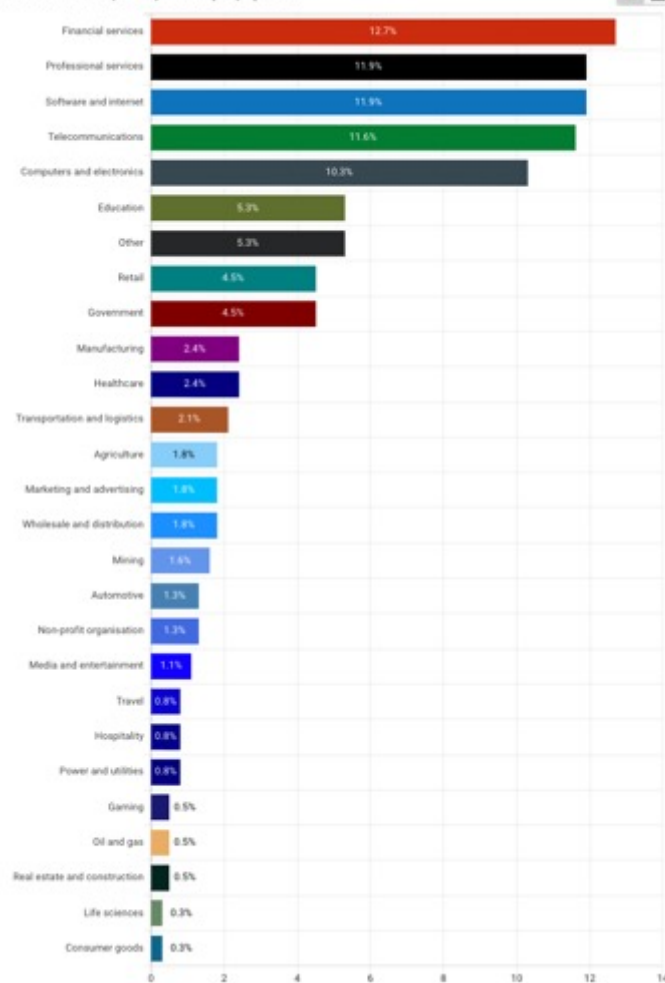
Agenda

- Ransomware Trends
- Survey Results
- Prevent & Mitigate
- Systemic & criminology response

Survey Demographics

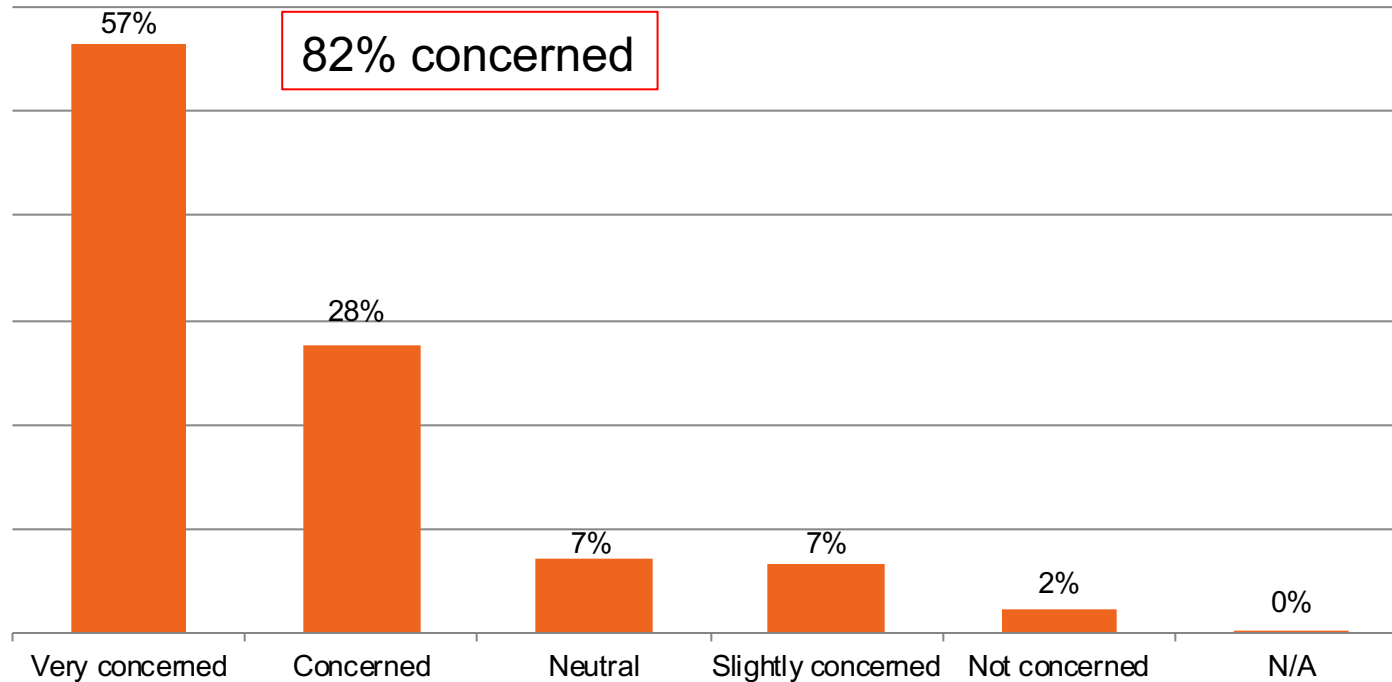
ITWeb and KnowBe4 Ransomware Survey –
September 2021

In which industry does your company operate?



Concern

On a scale from 1 (not at all) to 5 (very concerned) how concerned are you about ransomware?



Poll Question

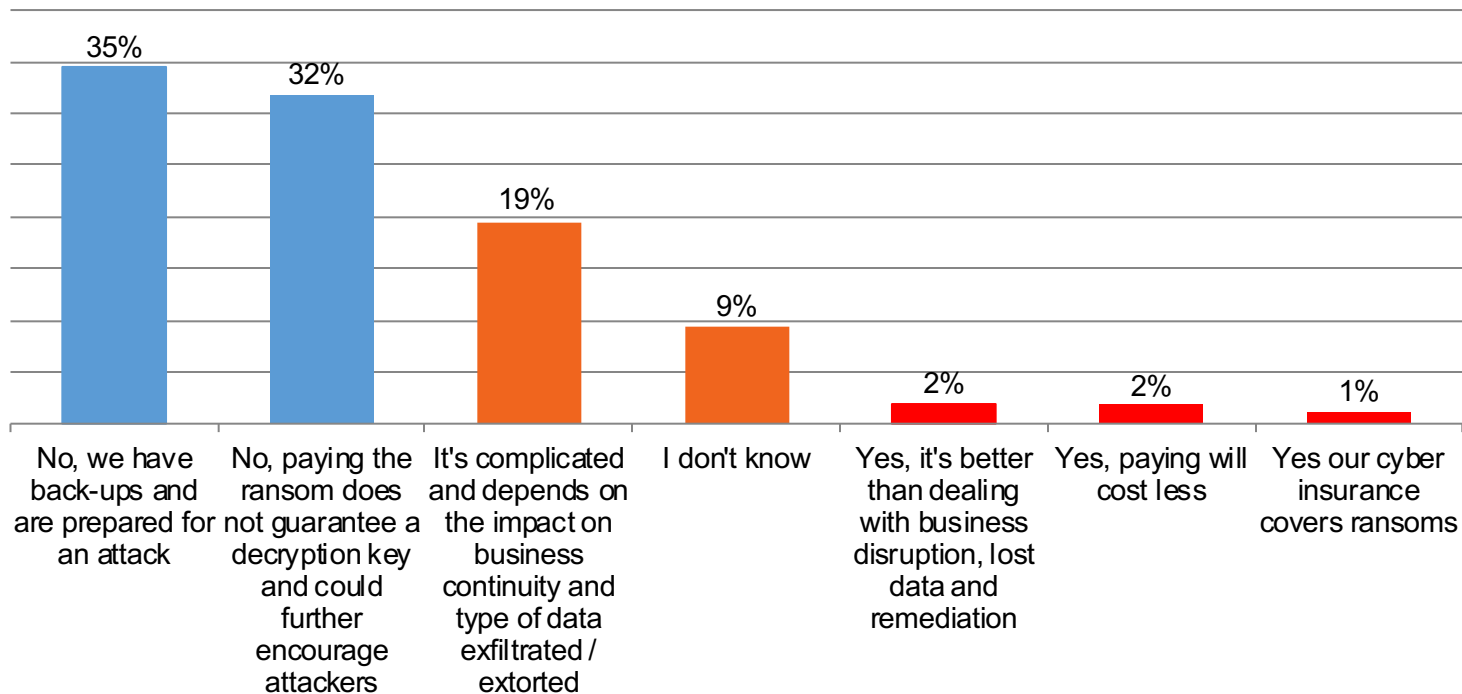
If attacked, would your company pay the ransom?

- No
- It's complicated and depends on the impact on business
- I don't know
- Yes, paying will cost less
- Yes our cyber insurance covers ransoms

All answers are anonymous

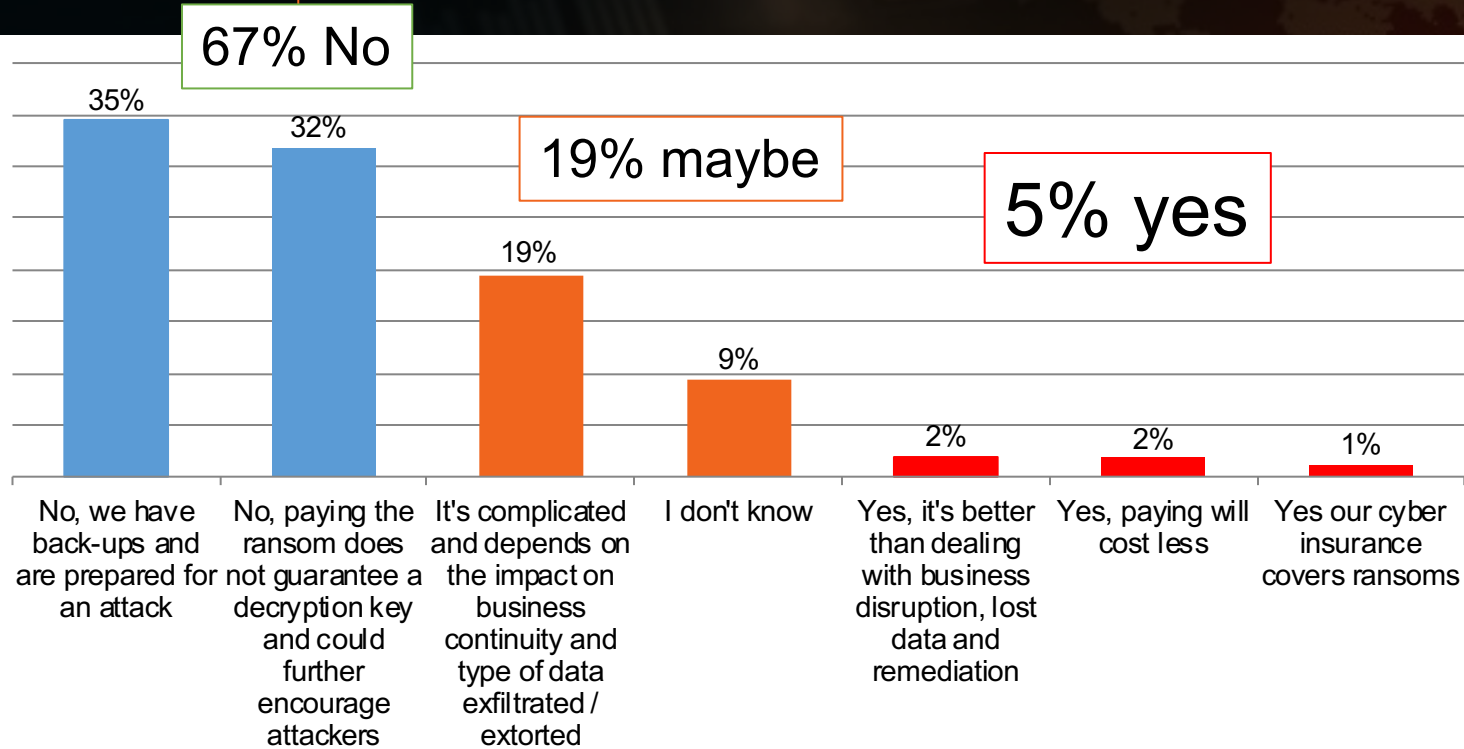
Pay: Yay or Nay?

If attacked, would your company pay the ransom?



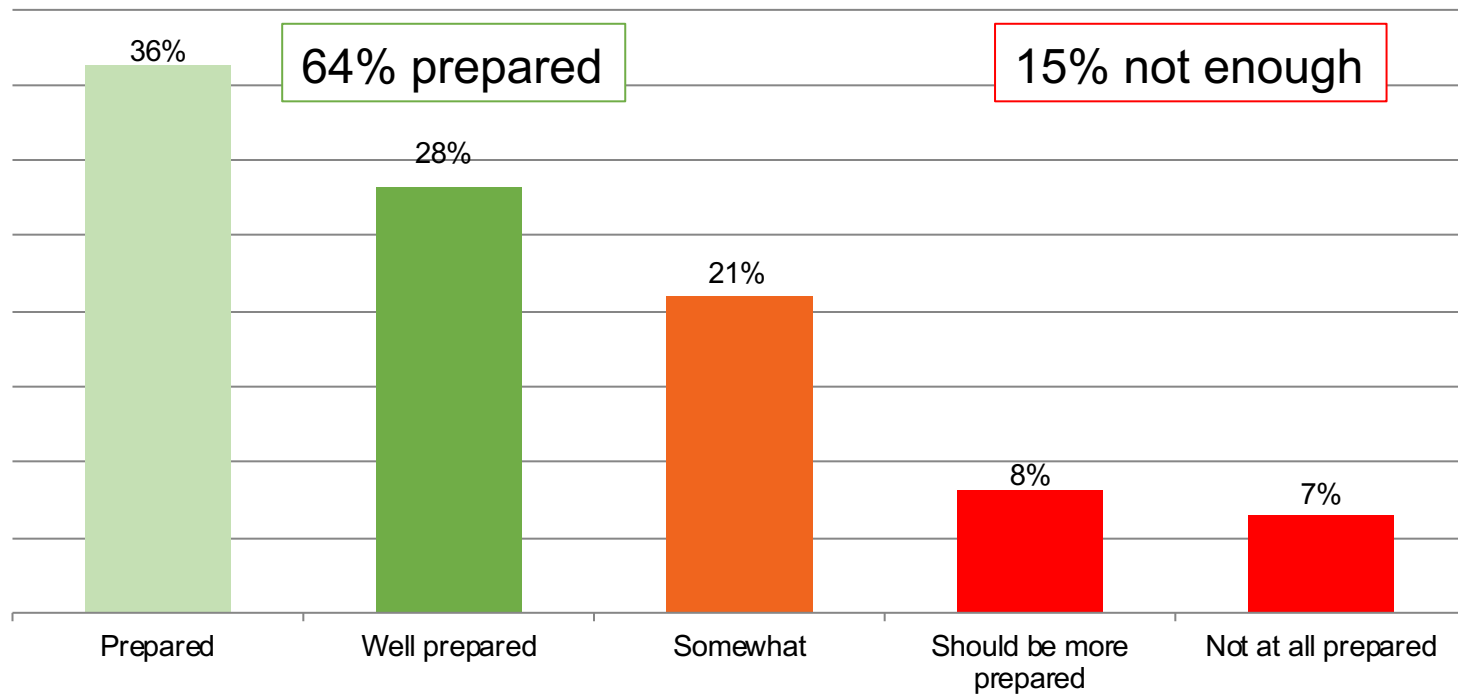
Pay: Yay or Nay?

If attacked, would your company pay the ransom?



Prepared?

How well prepared is your organization for a ransomware attack?



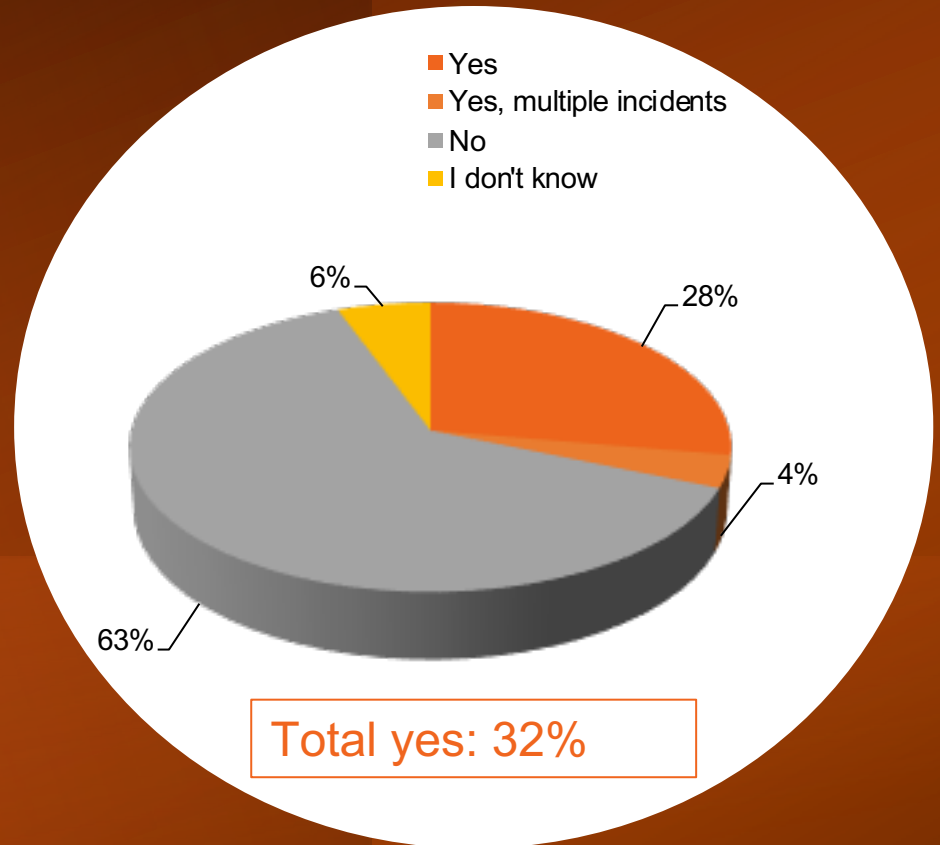
Poll Question

Have you suffered a ransomware attack in the past?

- Yes encryption only
- Yes, double extortion (exfiltration of data, encryption)
- Yes exfiltration of data only
- Yes all of the above plus DDOS
- No
- I don't want to answer this

All answers are anonymous

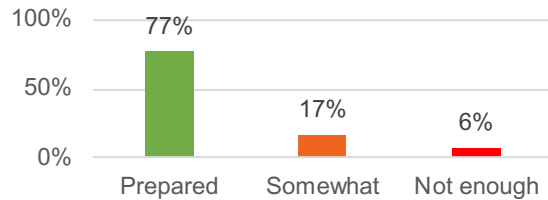
Have you suffered a ransomware attack in the past?



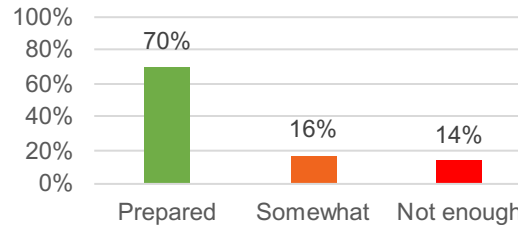
Industry Breakdown

How well prepared is your organization for a ransomware attack?

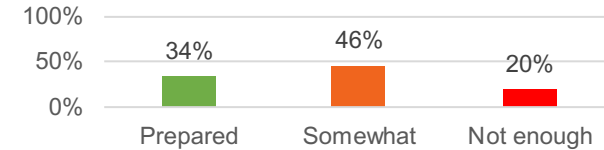
Finance Industry



Telecommunications



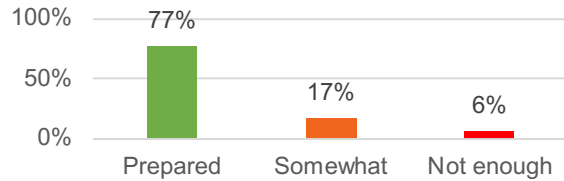
Government & Educations Sector



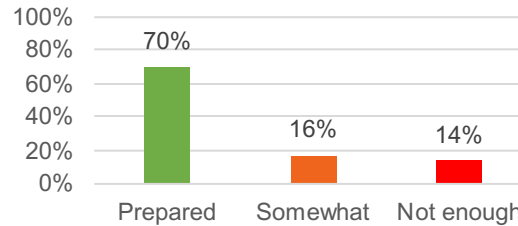
Industry Breakdown

How well prepared is your organization for a ransomware attack?

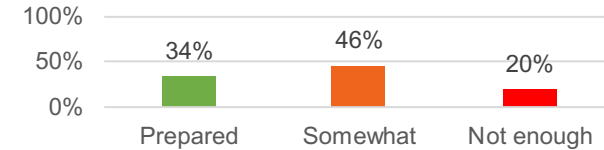
Finance Industry



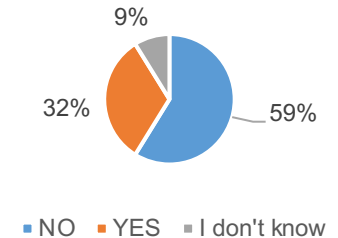
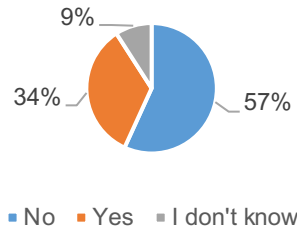
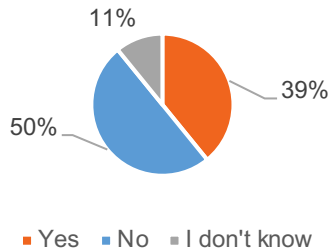
Telecommunications



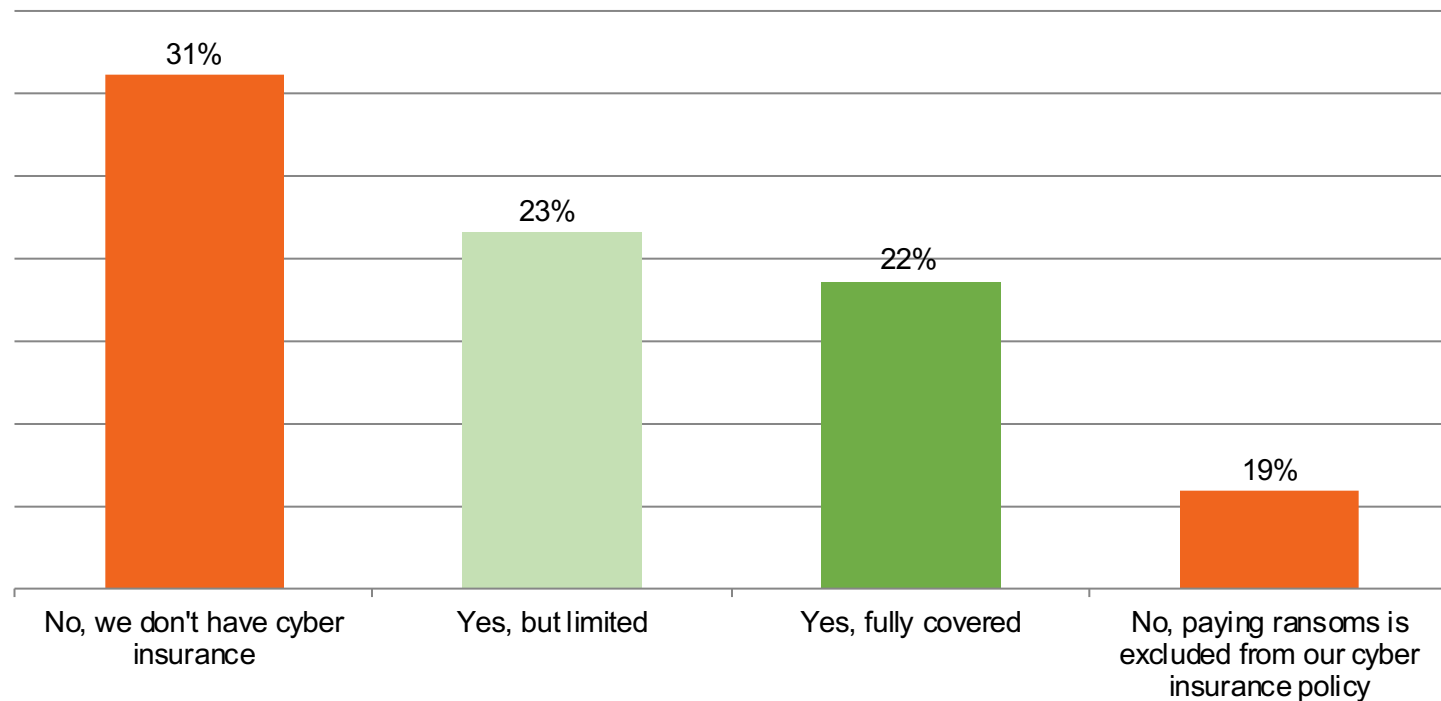
Government & Educations Sector



Have you suffered a ransomware attack in the past?

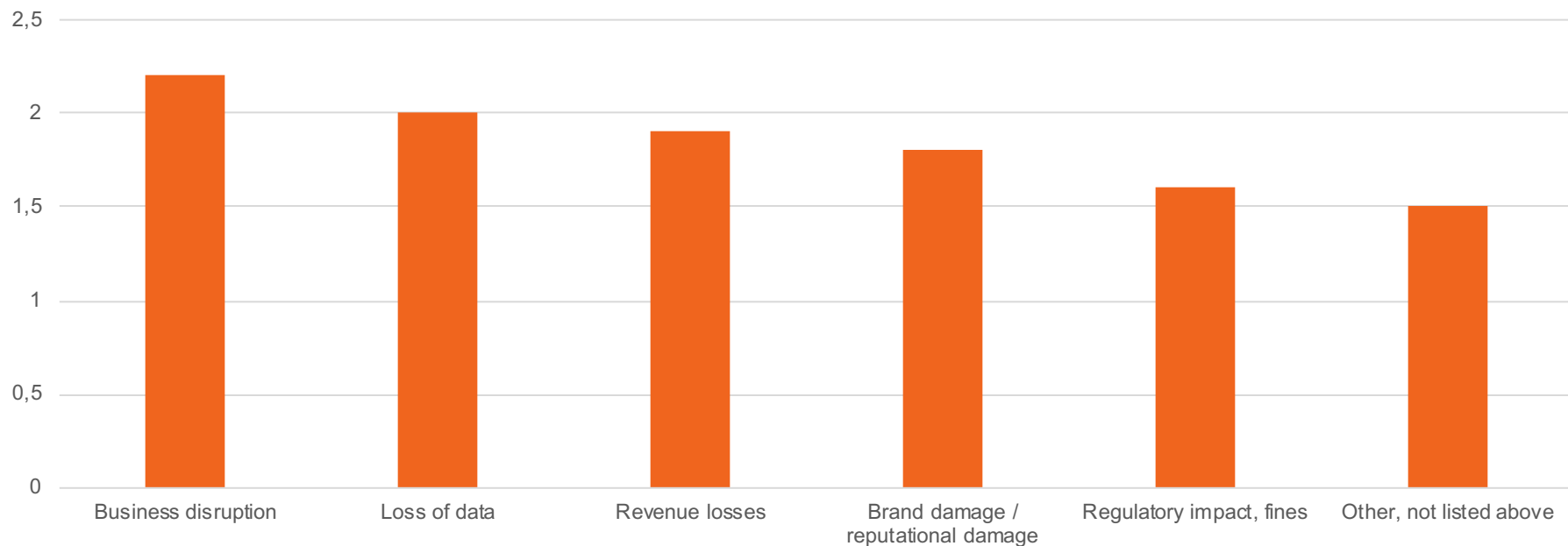


Does your cyber insurance cover your organisation against ransomware?

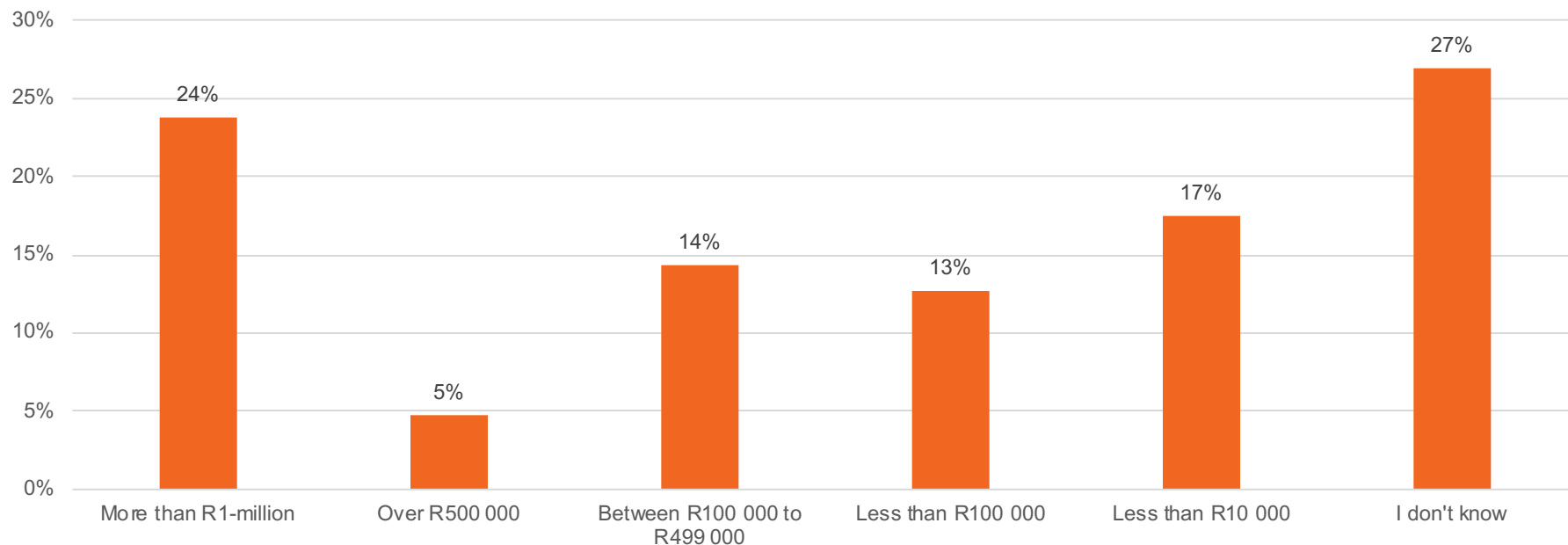


Business Impact

On a scale of 1-5 how drastic was the impact to your business?



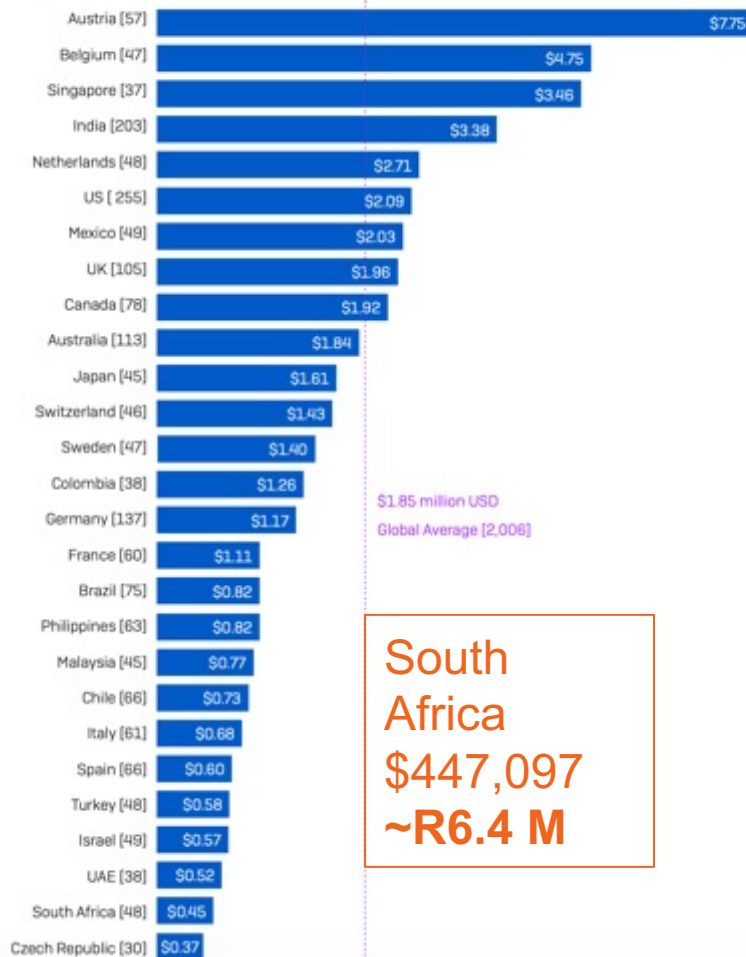
Financial Impact



Remediation Costs

Remediation costs vary based on your location

Looking at the ransomware remediation costs at a country level, we see considerable variations.



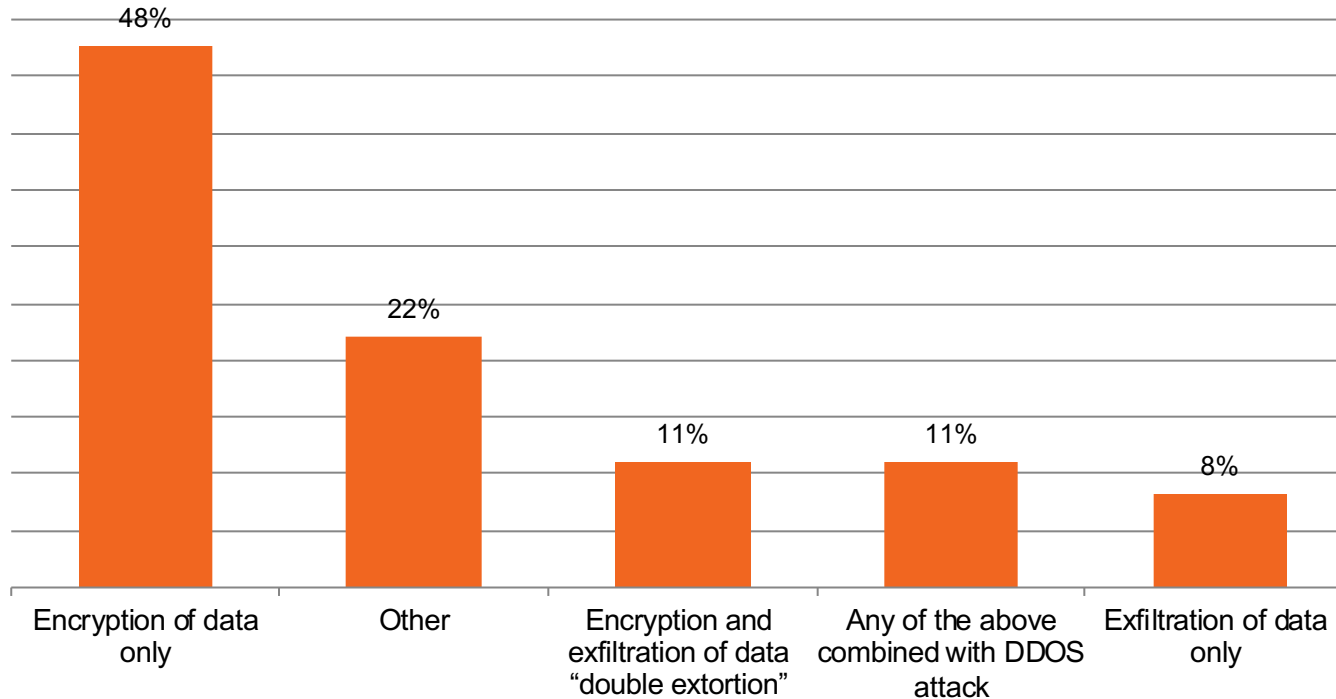
South
Africa
\$447,097
~R6.4 M





Attack Type

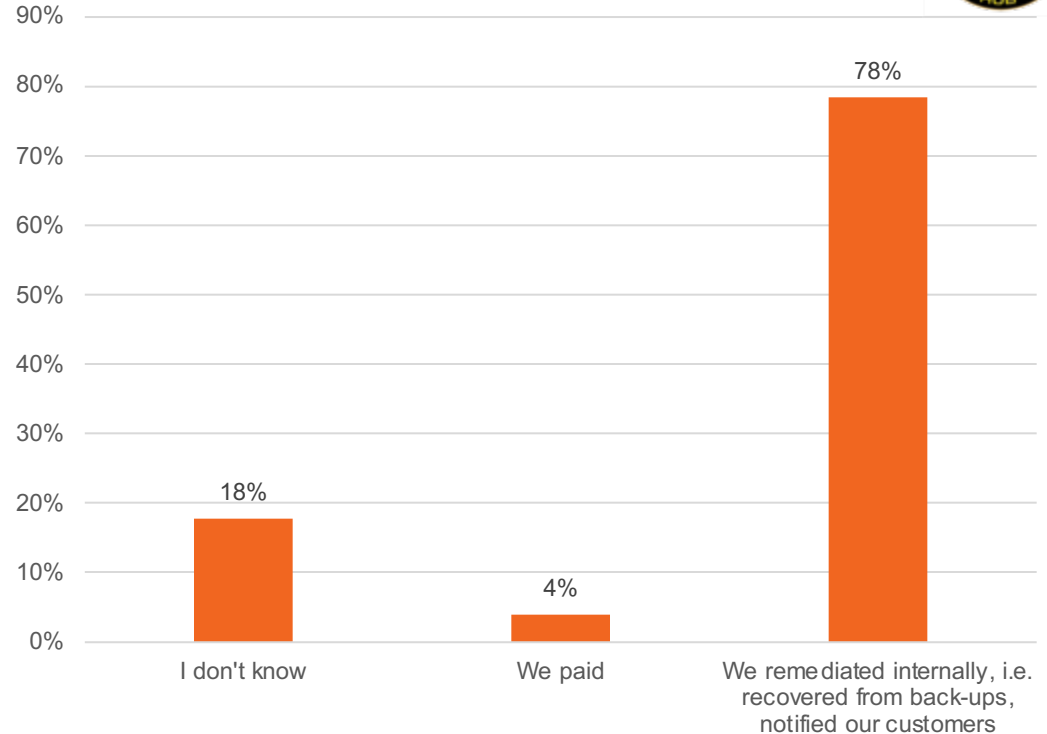
What kind of attack(s) did you experience?



How did you respond?

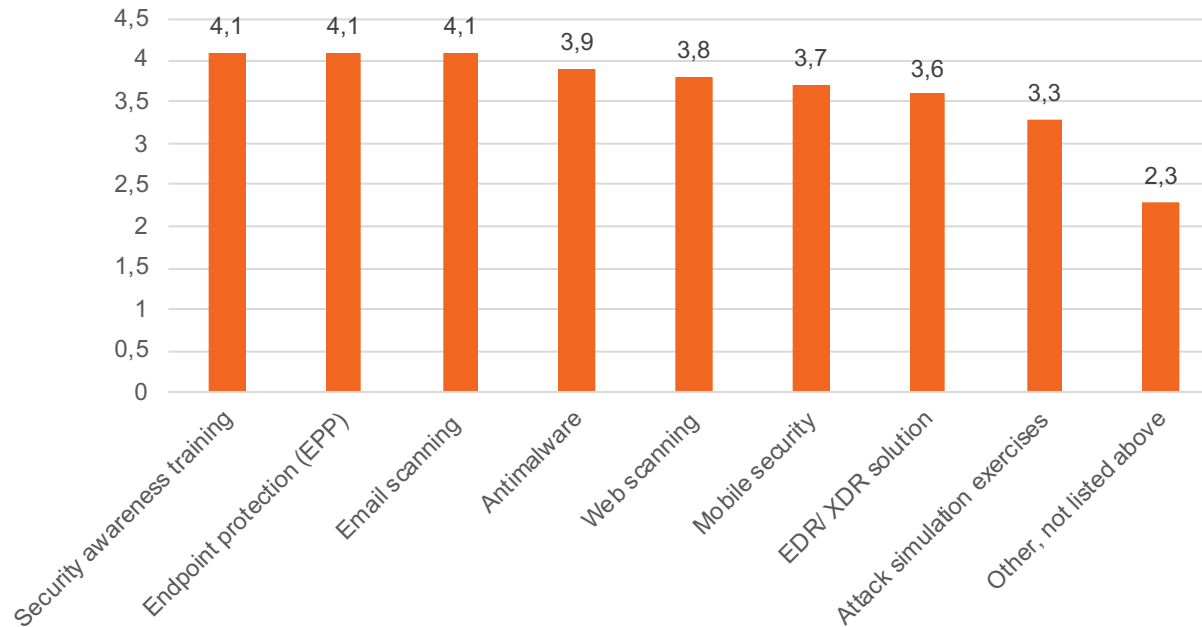
ITWeb and KnowBe4 Ransomware Survey –
September 2021

How did you respond?



Counter-measures

On a scale of 1-5, what countermeasures do you feel are most effective in stopping ransomware?

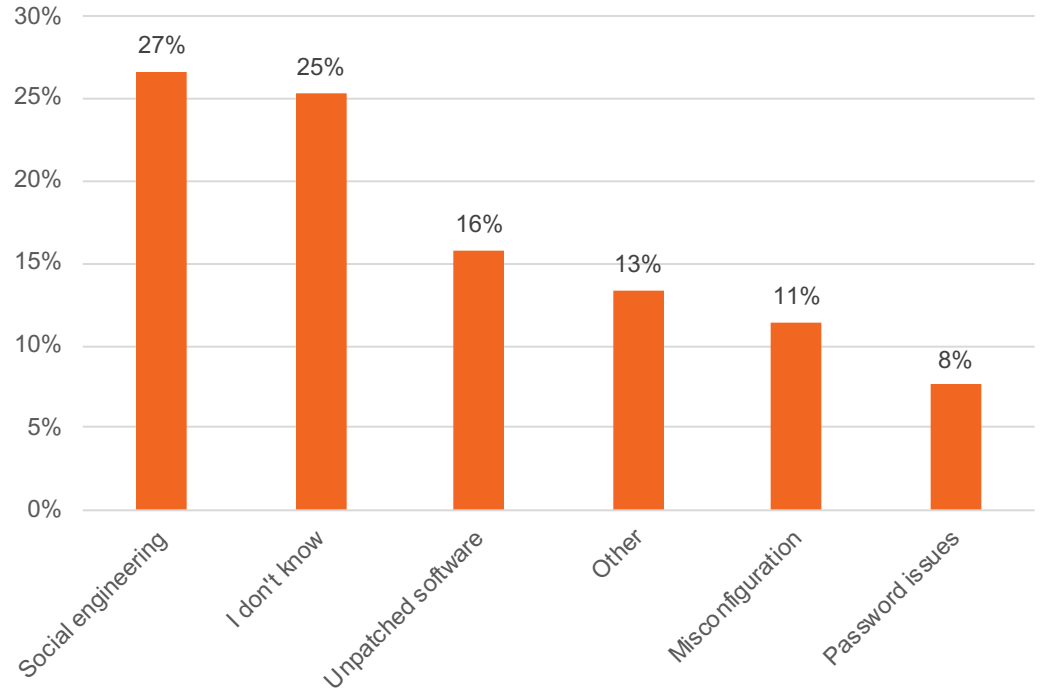


Root causes

ITWeb and KnowBe4 Ransomware Survey –
September 2021



Root cause that allowed the ransomware to gain initial foothold access into your environment?



Top Initial Root causes



Report Name	Social Engineering	RDP	Unpatched Software	Password Guessing	Credential Theft	Remote Server Attack	Third Party	USB	Other
Coveware Report	30%	45%	18%	-	-	-	-	-	5%
Statista	54%	20%	-	-	10%	-	-	-	-
Forbes Magazine Article	1st	3rd	2nd	-	-	-	-	-	-
Datto's Report	54%	20%	-	21%	10%	-	-	-	-
Hiscox Cyber Readiness	65%	-	28%	19%	39%	-	34%	-	-
Sophos Report	45%	9%	-	-	-	21%	9%	7%	9%
Averages	50%	24%	23%	20%	20%	21%	22%	7%	7%

1. Social Engineering
2. RDP
3. Unpatched Software
4. Password / Credentials

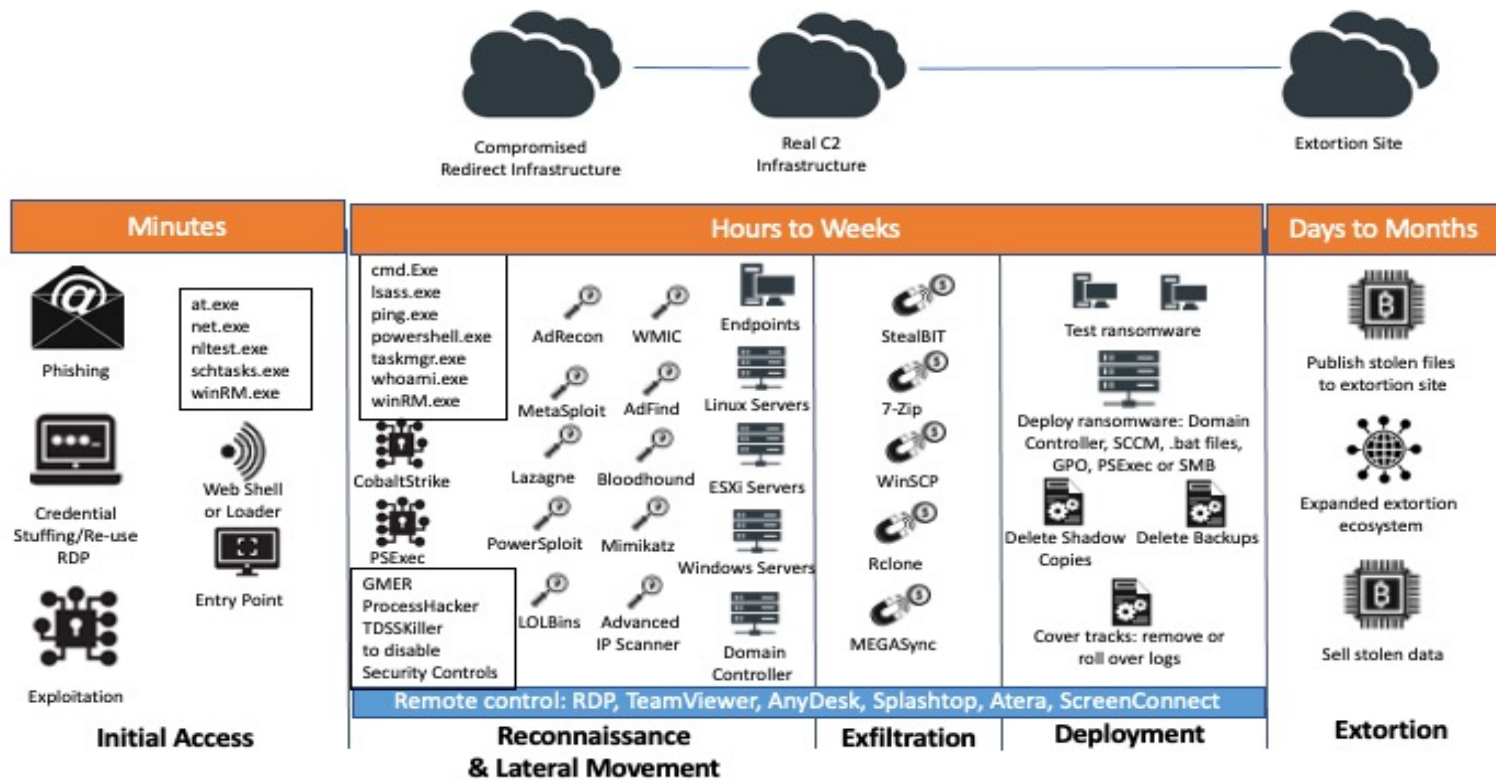
Source: Root causes of Ransomware by Roger Grimes 2021



Agenda

- Ransomware Trends
- Survey Results
- Prevent & Mitigate
- Systemic & criminology response

Know your enemy..



Defending Against Ransomware Advisory


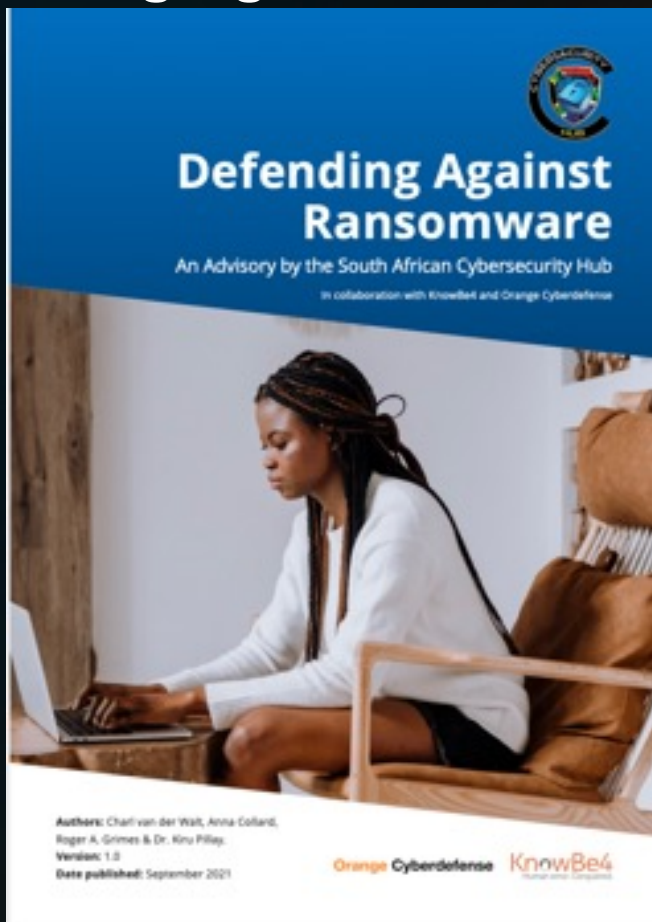


Table of Contents

Introduction	3
Motivation or Who Is Behind It?	4
How It Works	4
Top Initial Exploit Causes	5
Take a Risk-Based Approach	6
People	6
Processes	6
Technical Defenses	7
Plan For the Worst Case Scenario	7
You've Been Hit - What Now?	8
Appendix A: Follow the NIST Cybersecurity Framework	9
Identify	10
Protect	12
Detect	15
Respond	16
Recover	18
Appendix B: Helpful Tools & Resources	19
Appendix C: Examples for End-User Awareness Communication	20
Thank You & Contact Details	23

Orange Cyberdefense KnowBe4
Human error. Conquered.

NIST 5 Functions



Anticipate & Identify



- **Anticipate** the threat
- Know Your **Adversary**
- Know **Yourself**
 - Table-top and technical **simulation exercises**
 - **Asset discovery**
 - Internet **attack surface**
 - Check for **weak passwords**
 - Patch local **privilege escalation** vulnerabilities
 - Perform scans / searches on **relevant vulnerabilities**
 - Regular **pen tests**



Protect



- Document & **test** IRP
- Security Awareness & **Culture**
- Endpoint Detection & Response (**EDR**)
- **Strong authentication**
- Security **Hygiene Practices**
 - Enforce least privilege
 - Backup & Retention Policy (3-2-1 Rule)



Detect



- **EDR**
- Network Threat Detection
- Detect & **prevent phishing**
- **Deception** technology (Canaries)



Respond



- Stay calm
- **Disconnect**
- Determine **scope**
- Keep people **informed**
- Don't pay (if you can)



Recover

- Establish a trustworthy beachhead
- Recovery is a marathon



Good Resources



<https://orangecyberdefense.com/global/white-papers/beating-ransomware/>

<https://info.knowbe4.com/ransomware-hostage-rescue-manual-0>



Key Take Aways

- Extortion Attacks are here to stay
- It's a crime not a technology
- Defense in Depth
- Plan for the worst...

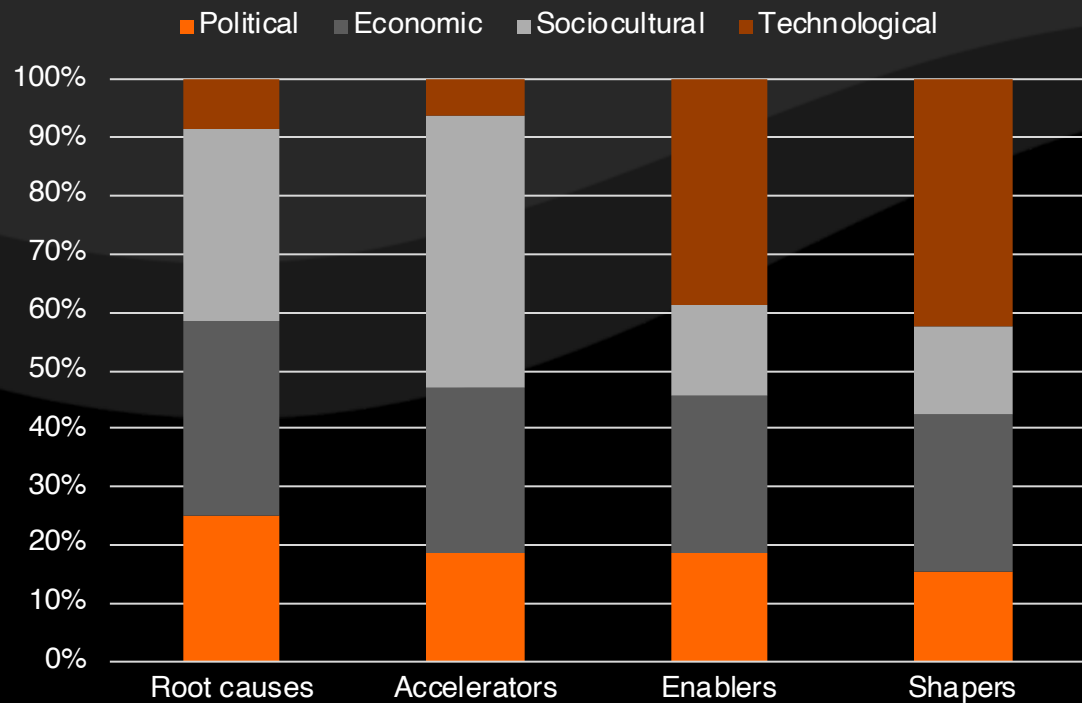


Agenda

- Why extortion happens
- A systemic response
- A criminological response

**If you think
technology can
solve your security
problems, then you
don't understand the
problems and you
don't understand the
technology.**

BRUCE SCHNEIER



It could be argued that the elements of our model broadly pit the real-life context of the criminal against the deep-rooted security debt that has accumulated in our technology stacks as we have rushed over the past three decades towards an everything digital / everything online society. All of this perpetuated by skewed economic drivers and political ambivalence



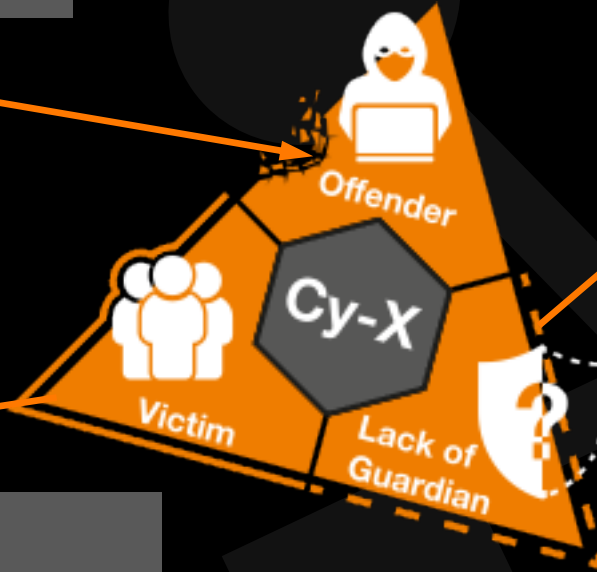
Reducing the Ransomware threat – Comprehensive Response

Demotivate offenders:

- Coordinated law enforcement effort
- Reducing the flow of funds from victims
- Targeted efforts to reduce criminals' neutralization techniques

Get suitable guardians in place:

- Appreciate the limited potential of security technologies in the complexity of cyberspace
- Use the power of community in partnership with security service providers and law enforcement



Decrease attractiveness as victim:

- Decreasing vulnerability
- Decreasing the value of digital assets
- Create inertia with Encryption, DRM and honeytokens
- Decreasing visibility & reducing attack surface
- Agile detection and response

Thank you & Questions?

Please get in touch:



Anna Collard



@annaCollard3

Charl van der Walt

@charlvdwalt

KnowBe4
Human error. Conquered.