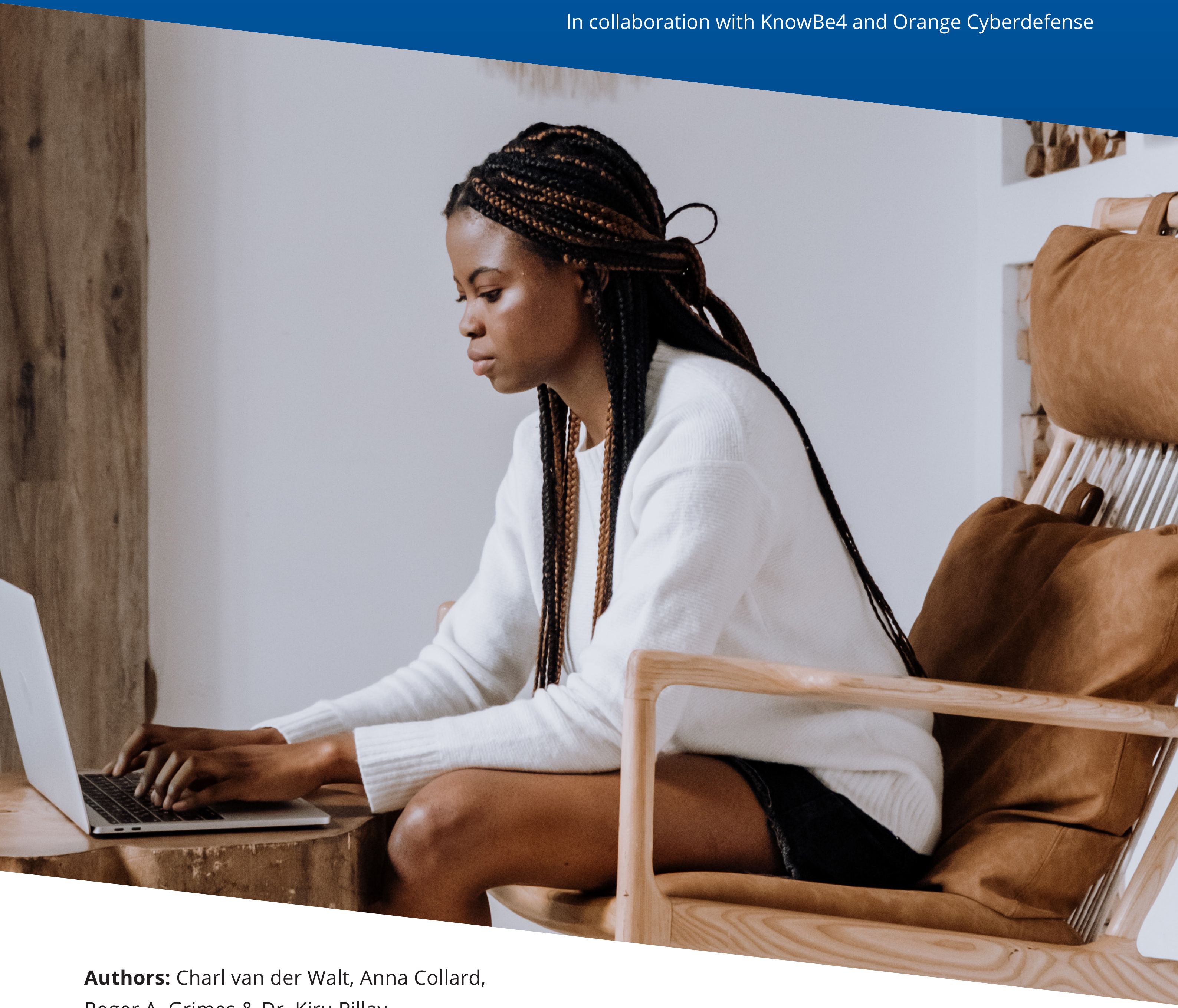
Defending Against Ransomware

An Advisory by the South African Cybersecurity Hub

In collaboration with KnowBe4 and Orange Cyberdefense



Authors: Charl van der Walt, Anna Collard,
Roger A. Grimes & Dr. Kiru Pillay.

Version: 1.0
Date published: September 2021

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

Introduction

You could call it the global wave of cybercrime: Transnet and other South African government departments have joined tens of thousands of victims of ransomware, in which cyber criminals break into computer systems and encrypt and/or steal files in order to demand a ransom payment.

This document will discuss the recommended technical defenses and preparation (including people, processes, technical defenses) organizations should implement to mitigate the threat of ransomware.

Ransomware is listed as the top worry by cybersecurity professionals throughout the world, with good reason. Ransomware has attacked tens of thousands of organizations from small to very large, brought down hospitals, pipelines, food production conglomerates, police stations, ports and even entire cities.

Emsisoft states, in 2020 alone, $18 billion was paid globally in ransom and total costs were in the hundreds of billions of dollars.[1] A recent study by ITWeb and KnowBe4 across 378 South African organizations showed that:

1. Thirty-four (34%) of respondents fell victim to ransomware. Of those, 48% experienced a significant or very significant impact on their business operations

2. Social engineering (27%), unpatched software (16%), misconfiguration (11%) and password issues (8%) were the top reasons for initial foothold.

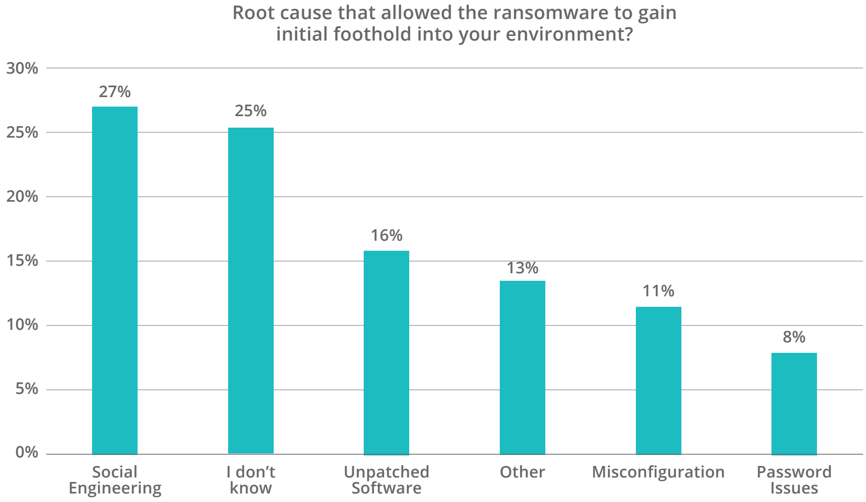


Figure 1: Root causes of ransomware in South Africa - ITWeb & KnowBe4 survey September 2021

According to Sophos, the average cost to rectify a ransomware attack in South Africa is ZAR 6,7M ($0.45 Million) in 2020[2]. Kaspersky saw a 24% increase in ransomware in Q2 2021 in South Africa.

Worse than the actual direct financial costs are long term reputational impacts such as the loss of investor confidence in South Africa. South Africa has a fairly high digital dependency and as developed nations clamp down on cyber criminals, the same criminals will shift their attention towards the emerging economies, making South Africa a more attractive target.

[1] (https://blog.emsisoft.com/en/38426/the-cost-of-ransomware-in-2021-a-country-by-country-analysis/).
[2] sophos-state-of-ransomware-2021-wp.pdf

Motivation or Who Is Behind It?

There are over 100 different "ransomware families" operated by criminals ranging from quasi-corporate, collaborative networks to individual gangs and participants. Ransomware operators call themselves apolitical, they don't particularly care about the impact they are causing to their victims or the citizens of the affected country. But no matter what their form, their objective is to criminally-enrich themselves. Anything that results in a likely payment of the ransom (e.g., the more vulnerable the organization, the higher their cyber dependency, the less prepared, etc.) the more attractive it becomes to the criminals. Ransomware as a Service (RaaS) allows so called affiliate networks to license the technology from operators and split their takings. This allows criminal elements without much technical skill to take advantage of this (underground) market opportunity and makes this such a growing threat on a global scale.

How It Works

At the heart of the ransomware crimewave is the basic idea that if you take something unique and precious from someone, they'll pay to have it back. If you discover someone's secret, they'll pay you to keep it secret. If they consume all your bandwidth so you can't conduct business, you'll pay them to stop. The microcosmic market of one seller and one desperate buyer, with almost zero risk for the ransomware criminal, drives extortion prices and immense profits for the criminal.

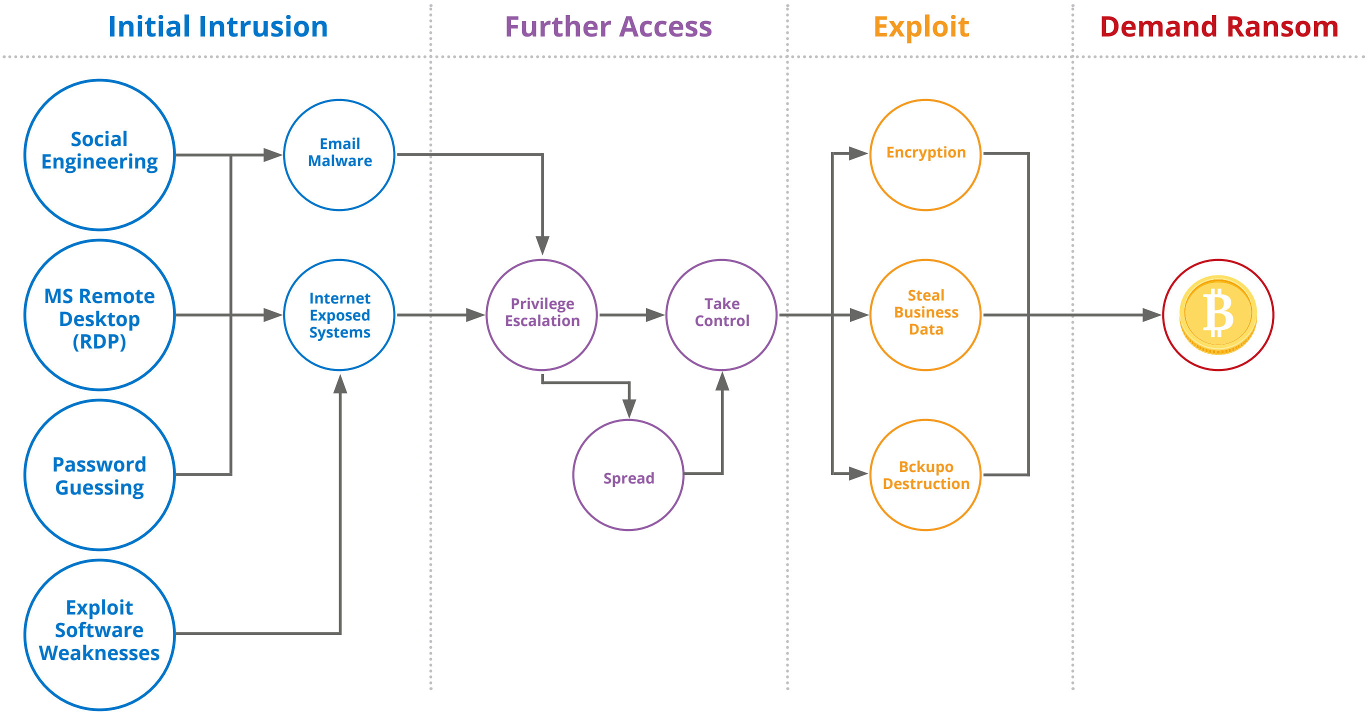


Figure 2: Ransomware kill chain

Top Initial Exploit Causes

The top initial exploit causes that allow ransomware to compromise devices and environments are (in order of popularity):

1. Social Engineering/Phishing
2. Abuse of Microsoft Remote Desktop Protocol (RDP)
3. Unpatched Software
4. Password Attacks

Social engineering is consistently the number one root cause used by ransomware and other malware attacks to gain initial access.[3]

What Is Social Engineering?

Social engineering, also known as "human hacking" is a manipulation technique that exploits human error to deliver malware, steal information or gain unauthorized access.

Phishing emails are one of the most popular forms of **social engineering,** whereby users are tricked into opening a malicious attachment, clicking on a malicious link or giving out sensitive information, such as their username and password.

Other forms of social engineering include **phone calls** or messages sent on **social media and chat applications,** such as SMS or WhatsApp. Social engineering can also take the form of a physical impersonation.

[3] KnowBe4 Root Causes Ransomware: https://info.knowbe4.com/wp-root-causes-ransomware

Take a Risk-Based Approach

The most common initial access vectors are social engineering, Microsoft Remote Desktop Protocol (RDP), unpatched software and password attacks. It makes sense to prioritize controls that address these attack vectors first. Take a look at your environment and focus on addressing the weaknesses related to the above.

We have listed recommended defenses by three broad categories: people, processes, and technical defenses. Following the below should give you a kick start into effectively defending your environment against the threat of ransomware:

People

- **Have a team:** Ensure that your response team is well defined, authorized and equipped with what they may need in a disaster.
- **Plan for reinforcements:** Choose a group of security and IT support vendors and put commercial and contractual frameworks in place ahead of time, in case you need to call on them in a crisis.
- **Train your users!** The most likely entry point for an attacker is often through compromising an end user via phishing or social engineering. So focus on addressing this first. The way to decrease the most risk due to social engineering is end-user training. Well run security awareness training programs provide a quick and dramatic drop in cybersecurity risks.

Processes

1. **Incident response plan:** Your response team should be working from a clear playbook that covers as many eventualities as you can anticipate. See section "Protect" for more. Ensure your incident response plan includes a pre-planned communications strategy designed to reach all your stakeholders.
2. **Keep contact lists updated:** You may need to reach out to a number of people internally and externally, including business leaders, incident responders, insurance, law enforcement, suppliers, your communications teams and more. Ensure that you have their latest contact details readily available. Report the incident to the SSA CSIRT.
3. **Vulnerability & patch management process:** Identify and triage relevant vulnerabilities and test and roll out critical patches timeously, particularly on any internet-facing systems.

Technical Defenses

- **Ensure reliable and secure backups of critical data and resources.** Apply **the 3-2-1 Rule,** which is a recommended best practice to protect critical data assets. Read more in the section Basic Hygiene.
- **Enforce multifactor authentication (MFA)** wherever possible to protect logons with access to valuable and sensitive information, particularly on any internet-facing system.
- **Automate** your user-awareness efforts with a platform that **combines training & phishing simulation campaigns.**
- Use **patch management solutions** to apply in a reliable and timely manner all recommended critical security patches.
- Invest in Detection and prevention technology such as endpoint detection & response **(EDR), Network Threat Monitoring & prevention and mail gateway filters.**
- Embrace the **"Zero Trust " model** as an architecture roadmap and limit access to only what is needed, repeatedly check whether users, devices, services or network components should be trusted, and monitor for malicious or abnormal activity.
- Make sure all internet-facing systems are properly protected by **firewalls and patched.**
- **Limit use privilege.** No one should be logged in as an admin for their normal work. Limit the number of administrators. Generally limit the access of any user to the absolute minimum required.

Plan For the Worst Case Scenario

- A successful extortion incident can cost a lot of money, such as costs to be paid for responders, negotiators and recovery. Do an estimation of these costs and consider how you would pay them in the event of an incident.

- Also check if your cyber insurance policy covers you for ransomware incidents.

You’ve Been Hit – What Now?

Stay Calm and Stick To the Plan

- Initiate your incident response plan and don’t make any rash decisions.
- Contact the contracted CSIRT at the earliest opportunity.

Disconnect

- Identify affected systems, isolate them and disconnect from any network. Turn off any wireless capabilities such as Wi-Fi or Bluetooth.
- Unplug any storage devices such as USB or external hard drives.
- Do not erase anything or “clean up” any files.

Determine the Scope

- Determine exactly how much of your file infrastructure is compromised or encrypted **(shared drives or folders, cloud storage or external hard drives etc).**
- Inventory the above and check them for signs of encryption.
- Check what files were backed up and what needs to be restored.

Keep People Informed

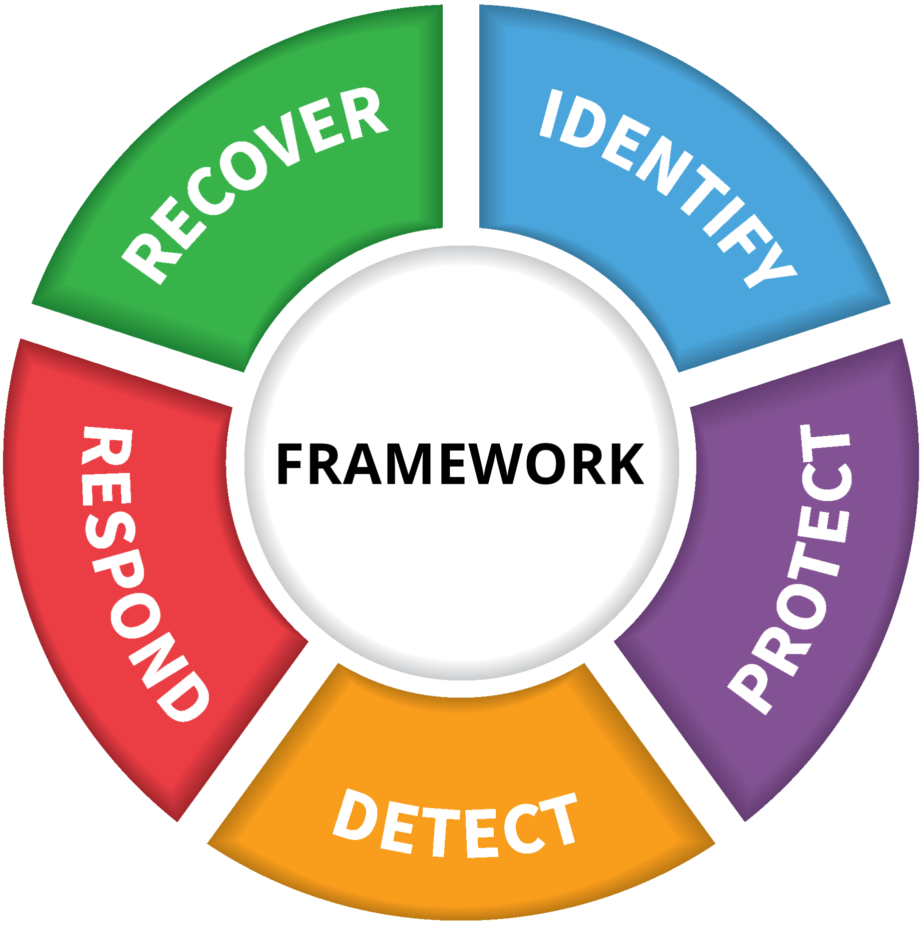
- Clear, open and honest communication is vital, both internally and externally.
- Issue a clear, strong public statement explaining what happened, how much you currently know and what you are doing about it.
- Notify the appropriate regulatory bodies and law enforcement agencies.

Appendix A:

Follow the NIST Cybersecurity Framework

The US National Institute of Science and Technology (NIST) has developed the 'Cybersecurity Framework' [1] as guidance for organizations to better manage and reduce their cybersecurity risk. "It's designed to be a "common language" that spans the entirety of cybersecurity risk management and that can be easily understood by people with all levels of cybersecurity expertise".

The NIST framework is widely referenced and applied. It describes five different 'functions': https://www.nist.gov/cyberframework/online-learning/five-functions



[1] https://www.nist.gov/blogs/taking-measure/identify-protect-detect-respond-and-recover-nist-cybersecurity-framework

RECOVER
IDENTIFY
FRAMEWORK
PROTECT
DETECT
RESPOND

Identify

The Identify function assists in developing an organizational understanding of managing cybersecurity risk to systems, people, assets, data, and capabilities.

Anticipate the Threat

Recent attacks against South African government institutions resulted in severe impacts on our critical infrastructure and it is evident that our public sector is an attractive target for ransomware gangs. By anticipating that you might be a victim and understanding what forms an attack might take, it allows you to assess your readiness and prepare accordingly.

Know Your Adversary

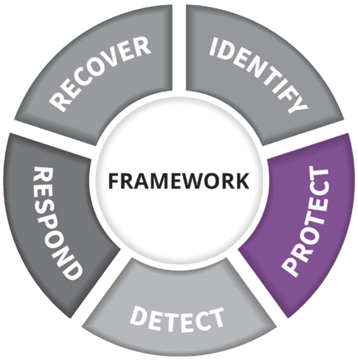
This preparation should therefore include:

- Keep abreast of developments and new techniques used by attackers.
- Become aware of common vulnerabilities and misconfigurations being abused by extortion operators (e.g. social engineering, unpatched software, password guessing against RDP and VPNs), and assess your environment for these issues specifically.
- Be aware that by the time of writing this document, most attacks use social engineering, client-side attacks, attacks against unpatched software, and password attacks, which bypass firewall protections.

Know Yourself

- Conduct end-user **education** along with **simulated phishing attacks** to assess how susceptible end users are to social engineering and to identify those who need more education. Assess your organization’s security culture on an annual basis.
- Conduct **table-top and technical simulation exercises** based on an understanding of how attacks and extortions play out.
- Perform an **asset discovery** to identify systems deployed in your environment and maintain an accurate inventory.
- **Discover your Internet Attack Surface,** including those systems that are hosted, in the cloud, in reserve or apparently depreciated as well as remote workers’ PCs, and ensure these are patched. Pay **particular attention to firewalls and VPN gateways,** as these have been specifically targeted since their increased use due to the pandemic.

- Routinely check for issues with **weak passwords** and password reuse.
- Identify and **patch local privilege escalation vulnerabilities.**
- Build the ability to rapidly **perform scans or (preferably) searches** across your IT inventory to identify systems or services that are most vulnerable to current attack vectors.
- Perform **ad-hoc searches** for systems with specific vulnerabilities or attributes that are being exploited by attackers.
- Engage **regular penetration tests** or Red Team exercises that emulate the tools and tactics that actual cyber criminals are deploying.
- **Involve SOC and response teams** in penetration testing exercises so that they can acquire proper 'battlefield' experience and practice identifying and responding to a skilled and determined adversary.



Protect

Document and Test Your Incident Response Plan

A well thought out incident response plan with detailed recovery procedures offers the best chance for surviving a ransomware attack and minimizing damage. According to the National Institute of Standards and Technology (NIST), an incident response plan should include four sections.

- **Preparation** Ensure everyone understands his or her role in the event of an incident. Develop scenarios to ensure that the plan works as intended.
- **Detection & Analysis** Determine if an incident occurred, the type of incident involved and its severity.
- **Containment, Eradication & Recovery** Stop what is causing the incident before any further damage is done and restore affected systems.
- **Post-Incident Activity** Conduct a lessons learned exercise identifying whether documented procedures were followed and if they were adequate. This also includes steps to potentially avoid this scenario in the future.

For more information on these recommendations, review NIST's Computer Security Incident Handling Guide.

- Test it regularly (at least bi-annually) against real-world case studies with tabletop exercises and targeted red team exercises.

Security Awareness and Culture

Follow the below for running a successful security awareness & culture program.

1. **Get executive (active) involvement:** This goes beyond just sponsorship or budget approval for the campaign, but requires leaders to be the face of the campaign.
2. **Measure your baseline:** Create a baseline view of your current status quo by running a proficiency or security culture assessment and track this at least every 12 months to showcase improvements. Phish-prone ™ Percentage (PPP), which refers to the percentage of employees who can be tricked into clicking on a phishing attack, can also help as a tracking metric.
3. **Avoid cognitive overload:** Focus on 2-3 key 'behaviors' and/or messages at a time and repeat these throughout your 'campaign'. Don't throw the whole security book at your people, as nothing will stick then.
4. **Don't do it alone:** Work with your marketing, internal comms, HR, compliance, etc.
5. **Make it beautiful:** This is the visible face of your department – make sure your comms are beautiful, simple and impactful. Choose content that is personally relevant and interesting to people (protect your kids, your home, etc.)

6. **The rod and the carrot:** Combine positive with negative incentives: reward desired 'behavior' such as a public shout out for someone reporting a nasty phish; bonus payments for anyone not falling for a simulated phish in 12 months. Negative incentives can include automatic remedial training for clickers or line manager escalations.
7. **Combine training with frequent phishing simulations:** Performing quarterly phishing simulations is not enough... everyone in the organization should get a randomly assigned phish every week – this gamifies the experience as every email needs to be scrutinized.
8. **Be human:** Emotions are powerful engagement techniques, so use them in your content. Tell stories, use humour.

Endpoint Protection, Detection and Response (EDR)

The most obvious place to detect and disrupt malware and ransomware activities is on the endpoint. Endpoint detection typically takes the form of antivirus or Endpoint Protection, Detection and Response (EDR), also known as 'Next Generation' anti-virus.

Choose the right EDR

- Ensure the solution uses multiple detection techniques including signature based, static indicators of com promise (IOC's) and behavioural analysis capabilities.
- It should be cloud-based, allowing for continuous monitoring and centralised collection of activity data.
- Ability to perform remote remediation actions, whether the endpoint is on the corporate network or outside of the office.

EDR success lies in the details of the implementation

- Determine whether you have the in-house capabilities and workload availability to effectively deploy, manage and tune the solution, if not, you should consider using a service provider to ensure optimum protection.
- Ensure it has coverage for all the major operating systems in use in your environment.
- Go with a single solution which provides the benefits of standardised reporting, easier data correlation and one place to go to manage alerts.

Strong Authentication, Everywhere That Matters

Strong or multi-factor authentication restricts other primary attack vectors, namely password spraying and credential stuffing.

- Enable multi-factor authentication (MFA) to protect valuable and confidential data, where it can be done.
- At the very least, enable it on email, VPN and exposed RDP services.

Getting the Basics Right: Security Hygiene Practices

There are a couple of “basic” security hygiene practices that should be implemented:

Enforce least privilege

- Minimize the number of privileged users and groups.
- Minimize the number of permanent members of elevated groups.
- All users should use the least privilege set of permissions and privileges necessary to do their task at hand.
- Ensure that a user’s standard domain account does not have administrative privileges anywhere, this includes locally on a device or at domain admin level.
- Consider a Privileged Access Management (PAM) solution where passwords can be checked out, then checked back in once used and changed.

Embrace the “Zero Trust” Model

Network segmentation is basically the principle of least privilege but aimed at only allowing the minimum necessary network traffic that needs to get to and from a system.

Software-defined segmentation offers a new, more agile approach to isolate and segment networks and applications that is faster and easier to manage than internal firewalls and VLANs.

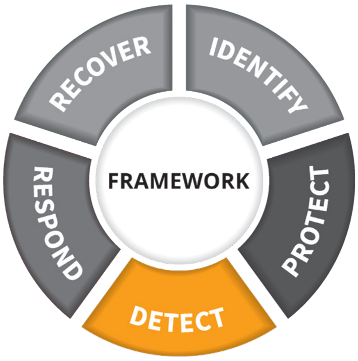
It is more flexible across on premises and hybrid cloud environments and enables more rapid implementation of a Zero Trust Security model to protect your most critical applications and data.

Zero Trust is a security model based on a set of design principles that assumes that a breach is inevitable or has likely already occurred. Zero Trust architectures limit access to only what is needed, repeatedly check whether users, devices, services or network components should be trusted, and monitor for malicious or abnormal activity.

It is more than just a technology architecture though, it’s a long-term philosophy and requires a mindset change amongst everyone involved. To succeed, it is essential to create a security culture that embraces Zero Trust. This means broadening the conversation and explaining Zero Trust principles to business leaders, IT administrators and general users.

Backup & Backup Retention Policy

- The 3-2-1 Rule for backups is a recommended best practice to protect critical data assets. It stipulates:
- Have three timely, secure, copies of critical data (i.e., the original data, plus two more copies), store those copies on at least two different media types and keep one backup copy offsite (where it cannot be accessed online).
- Define a backup retention policy to have backups completed once an hour or once a day.
- Offsite backups may be limited to just once a week or even monthly.



Detect

EDR

- Include your endpoint solutions in the security monitoring efforts.
- Ensure they can detect signatures of malicious files or processes, or even suspicious traffic or other behaviours.
- Block the processes from executing and quarantine the suspicious files.

Network Threat Detection

Complimentary to EDR, deploy a Network Threat Detection solution.

- Analyse the network traffic at certain choke points and identify threats.
- Using behavioural analysis and in some cases AI capabilities, suspicious, malicious or anomalous traffic flows and patterns can be identified and alerted on.
- Some solutions also have the capability to perform automated remediation actions such as terminating connections, quarantining a device or cutting off a subnet to prevent lateral movement.
- Consider solutions that can be deployed in on-premises, virtual and cloud network environments to provide total coverage and protection.

Detect and Prevent Phishing Campaigns

Phishing attacks are a key vector for an attacker to gain a foothold in a network.

- Deploy a solid email security system to detect and prevent phishing campaigns along with other email-borne threats.
- An optimal solution is cloud-based service for centralised monitoring and control and scalability.
- Ensure they offer real-time intelligence and protection based on telemetry from the vendor's customer base.

Deception Technology

Deception technology utilises the creation of traps (decoys) which are mixed within existing IT resources designed to tempt an attacker to interact with them. These traps or lures, often referred to as canaries, can be in the form of specific files, user accounts or even a host system on the network.

- Pair deception technology with effective detection and response capabilities.
- Deception alerts are infrequent by design, but of very high fidelity. Accordingly, systems and processes must be put in place to ensure that alerts from deception systems are noted and responded to with appropriate urgency.

RECOVER
IDENTIFY
FRAMEWORK
RESPOND
PROTECT
DETECT

Respond

Stay Calm and Keep To the Plan

If the worst should happen and you do fall for an extortion attack, the first key thing is to try and remain calm and not panic or make rash decisions.

- Initiate the incident response plan and get control.
- Contact the contracted CSIRT to help coordinate and provide much needed additional manpower on a 24x7 basis.
- Engage them at the earliest opportunity.

Disconnect

- Identify affected systems and isolate them or the subnets they are on to prevent any further spread.
- Disconnect the infected devices from any network it is on. Turn off any wireless capabilities such as Wi-Fi or Bluetooth.
- Unplug any storage devices such as USB or external hard drives.
- Do not erase anything or "clean up" any files or anti-virus. To find out which computer it is, check the properties of any infected (encrypted) file.

Determine the Scope

- Determine exactly how much of your file infrastructure is compromised or encrypted. **Did the infected machine have access to any of the following?**
  - Shared drives or folders
  - Network storage of any kind
  - External Hard Drives or USB memory sticks with valuable files
  - Cloud-based storage (DropBox, Google Drive, Microsoft OneDrive/Skydrive etc...)
- Inventory the above and check them for signs of encryption.
- In the case of cloud storage devices such as DropBox or Google drive, you may be able to revert to older, unencrypted versions of your files.
- Check what files were backed up and what needs to be restored versus what may not be backed up.

Keep People Informed

- Clear, open and honest communication is vital, both internally and externally.
- Make internal staff aware of what has happened, what is being done about it and how they can help.
- Externally, issue a clear, strong public statement explaining what happened, how much you currently know and what you are doing about it.
- Notify the appropriate regulatory bodies and law enforcement agencies.

Don't Fuel The Fire (If You Can)

- Paying the ransom encourages criminals to continue waging ransomware attacks, so it should really be avoided. They are criminals after all and there is no guarantee that all your data can be recovered.
- Be careful how you select your advisors. Not all ransomware "negotiators" are worth their fee.

RECOVER
IDENTIFY
PROTECT
DETECT
RESPOND
FRAMEWORK

Recover

Establish a Trustworthy Beachhead

While it's feasible to detect and remove specific malware or hacking tools from a computer, it's almost impossible to assert that a network is 'clean' after it has been infected or compromised. To fully recover from the attack, and completely evict the attackers from your environment:

- Seriously consider scrapping everything and rebuilding the affected devices and software from scratch.
- Recreate your Active Directory domain if domain controllers were compromised.
- Whilst this can clearly be a daunting undertaking, it is the only way to 100% know that the attacker has been removed from your networks as often it is not possible to fully know where an attacker has been and what they have done.
- This is where your secured backups become a critical component as they should allow you to get mission critical systems up and running quickly, providing they have not been compromised.

Recovery Is a Marathon, Not a Sprint

Full recovery from a serious incident can take a long time, and the response effort will claim a huge toll on your team.

- Consider the wellbeing of any staff involved in the recovery process.
- Ensure they get adequate rest and time off to avoid burnout.
- Work with an external CSIRT that can provide the additional efforts needed to allow the rotation of key staff needed in the recovery process.

Appendix B:

Helpful Tools & Resources

Documents:

Beating ransomware – Orange Cyber Defense whitepaper and practical guidelines
https://orangecyberdefense.com/global/white-papers/beating-ransomware/

NIST Tips and Tactics for Dealing With Ransomware
https://csrc.nist.gov/projects/ransomware-protection-and-response

CISA Ransomware Guide
https://www.cisa.gov/stopransomware/ransomware-guide

Ransomware Taskforce
https://www.ncsc.gov.uk/blog-post/ransomware-taskforce-rtf-announce-framework-to-combat-ransomware

Free tools:

Free phishing simulation test up to 100 users
https://www.knowbe4.com/phishing-security-test-offer

Ransomware simulator tool
https://www.knowbe4.com/ransomware-simulator

Breached password test
https://www.knowbe4.com/breached-password-test

Orange Cyberdefense KnowBe4 Human error. Conquered.

Appendix C:

Examples for End-User Awareness Communication

Imagine a message appears on your screen that says “We have your files – pay us to get them back – if not we’ll publish all of it”. It could and does happen frequently.

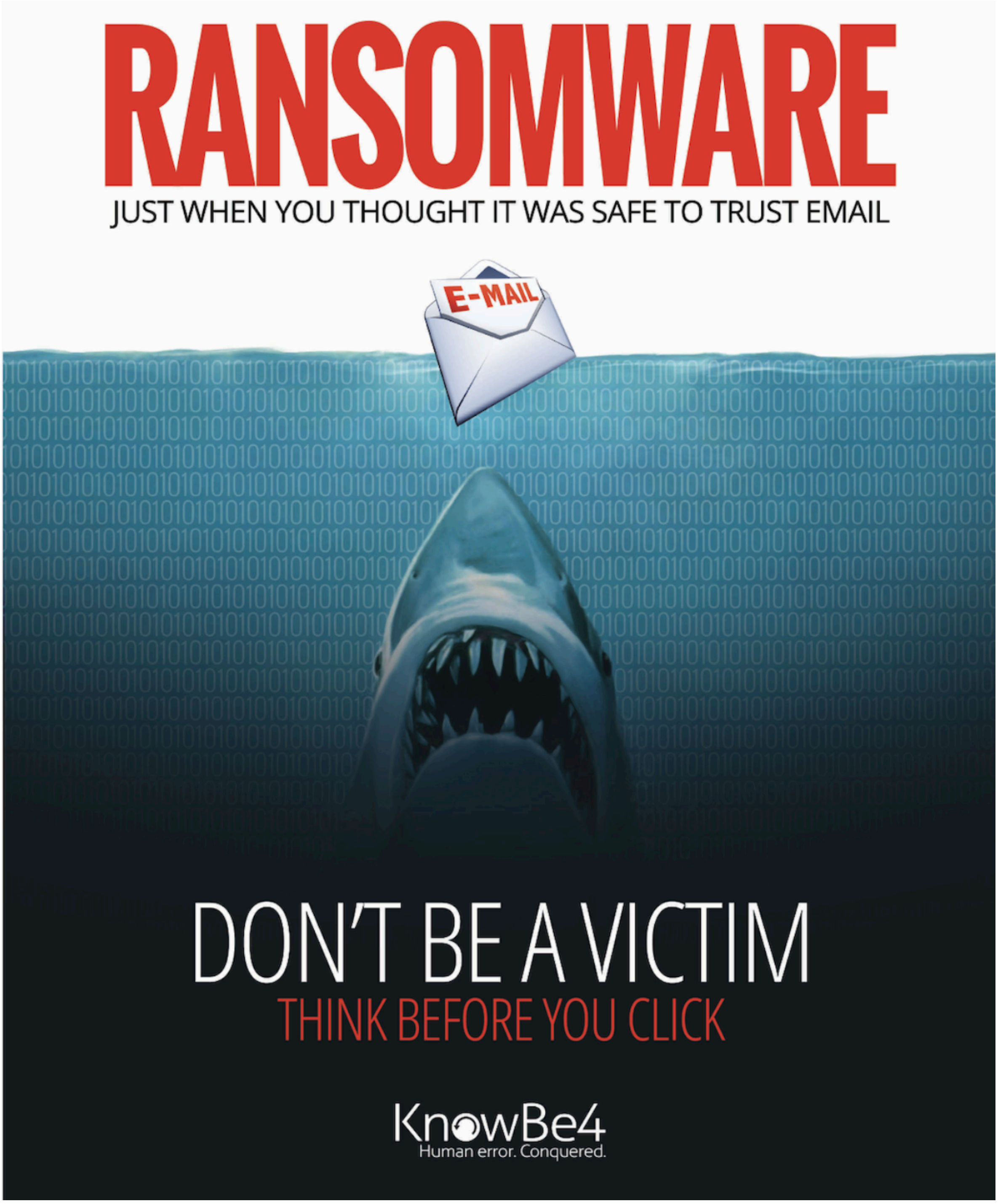
It’s a nasty extortion threat called ransomware. It starts with malicious software that gains access through malicious email attachments or links, infected websites, unpatched software or stolen passwords.

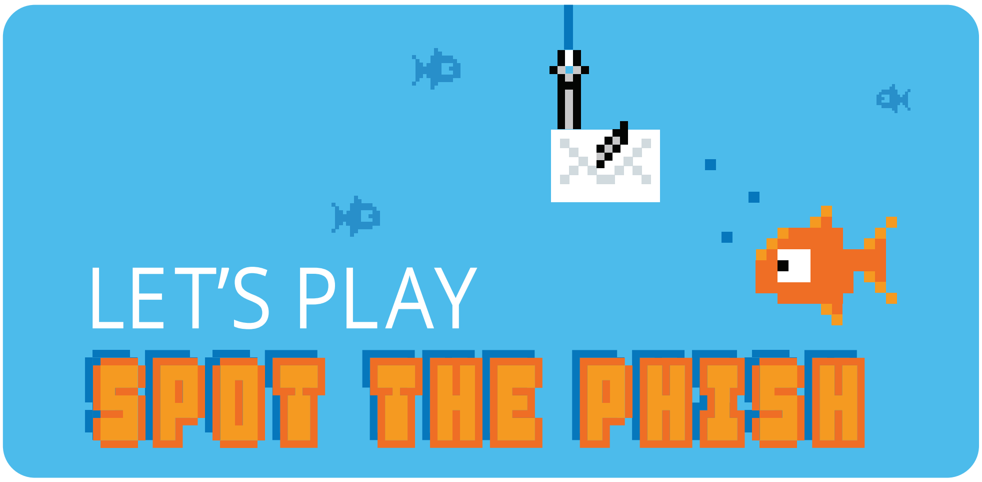
Once the ransomware is installed, it blocks access to all data until a ransom of up to millions of Rands is paid for its release. Often the criminals exfiltrate sensitive and personal data first. This means that if the victim refuses to pay up, information can be leaked online or sold to the highest bidder.

Be Ransomware Aware:

- Don’t trust unexpected attachments or links in emails (even if you know the sender).
- Watch out for browser security warnings (i.e. “this site cannot be trusted”).
- Use multi-factor authentication wherever possible.

If you see something, say something. Notify your IT / Security team immediately should you suspect having fallen for a phishing attack or experience anything suspicious.


RANSOMWARE
JUST WHEN YOU THOUGHT IT WAS SAFE TO TRUST EMAIL
E-MAIL
DON'T BE A VICTIM
THINK BEFORE YOU CLICK
KnowBe4
Human error. Conquered.



LET'S PLAY SPOT THE PHISH

Tips to Spot a FAKE message:

- **F** **Feeling:** Does the message trigger an emotion?
- **A** **Action:** Does it ask you to do something?
- **K** **Know:** Do you really know who it's from?
- **E** **Expect:** Were you expecting this email?

DON'T BE HELD RAnsOm!

WATCH OUT FOR THESE POPULAR PHISHING MAILS:

- Invoice attached
- Proof of Payment
- Resume / CV
- You have voice mail
- Your delivery

Orange Cyberdefense

KnowBe4
Human error. Conquered.

Thank you

Cybersecurity Hub:

www.cybersecurityhub.gov.za

cshubcsirt@cybersecurityhub.gov.za

KnowBe4
Human error. Conquered.

KnowBe4 Africa:

www.knowbe4.com/contact-us

Telephone +27 (80) 0014860

Orange Cyberdefense

Orange Cyberdefense:

www.orangecyberdefense.com/za/contact/

Telephone +27 (0)12 460 0880