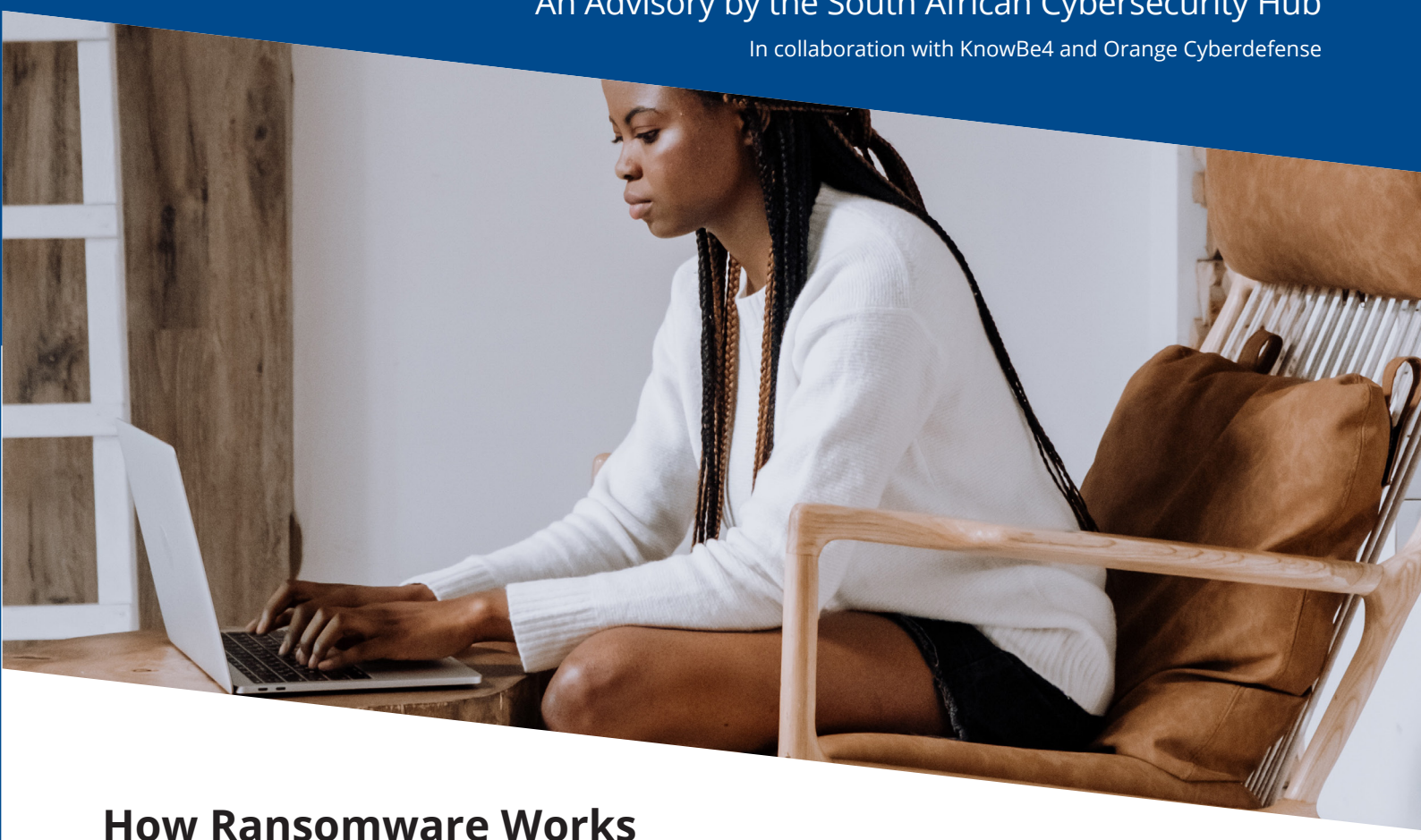
Defending Against Ransomware

An Advisory by the South African Cybersecurity Hub

In collaboration with KnowBe4 and Orange Cyberdefense



How Ransomware 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.

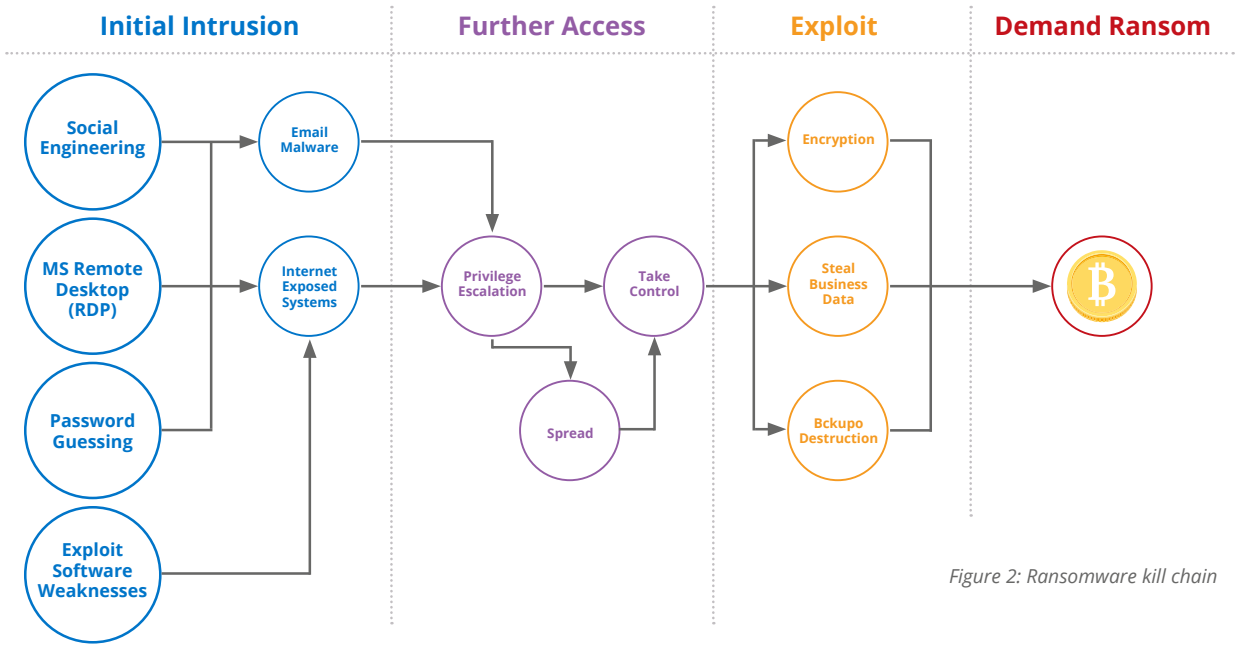


Figure 2: Ransomware kill chain

Take a Risk-Based Approach

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.[1]

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.

Orange Cyberdefense

KnowBe4 Human error. Conquered.

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

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. 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.
- **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 & 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.

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.

Orange Cyberdefense KnowBe4 Human error. Conquered.

Version: 1.0
Date published: September 2021