IN THIS PAPER

Ransomware – how to better protect your organisation.

PUBLISHED

1st APRIL 2022

WRITTEN FOR

Cyber security professionals

This paper looks at Ransomware and how to implement processes and technologies to achieve better protection.

FORWARD

Credo Of the Cybercriminal:

"ATTACK HIM WHERE HE IS UNPREPARED, APPEAR WHERE YOU ARE NOT EXPECTED."

SUN TZU, THE ART OF WAR C. 544-496 BCE

This paper outlines an approach using Rebasoft as part of an integrated cyber security defence system that can significantly reduce the risk of Ransomware infecting your organisation. It helps you identify those unexpected/unknown areas where your organisation might be susceptible to a Ransomware attack and helps respond quickly to reduce the impact should there be an infection.

WHAT IS RANSOMWARE?

To fight it effectively, we must first understand our adversary. Ransomware is simply a class of Malware that combines damage to IT systems with a ransom demand.

Since the dawn of networked computers, Malware has been around and is constantly evolving. It is a program installed on a target system designed to compromise, gain control, or steal data (exfiltrate data, as security professionals call it).

There are three main categories and infection mechanisms of Malware:

- VIRUSES—These applications spread by replicating themselves, like biological viruses infect host cells. When a new device encounters an infected one, it too can become infected, further propagating the virus.

- TROJANS - Trojans masquerade as real programs, and they trick users into opening them through phishing emails or downloads from the internet. Trojans are some of the most common malware applications.

- WORMS—Worms can spread between systems on the network on their own without user involvement

Ransomware uses Malware with the "dangled" option of putting things back the way they were through ransom payment. The advent of cryptocurrencies allows cybercriminals to use Bitcoin and other "un-trackable" denominations. After payment, they then promise to provide the antidote (decryption key or return stolen data).

Ah, if only life were as simple. Like in real-life, cybercriminals cannot be trusted; payment may not result in the restored system(s). Cybercriminals will also often re-target organisations that were previously compromised.

WHY IS RANSOMWARE IN THE NEWS SO MUCH?

The answer is simple – cybercriminals can make cheap and easy money. The chances of being caught are low, and the opportunity to make serious money is relatively high.

Ransomware distribution can be easily automated using an array of inexpensive equipment. It allows a single cybercriminal to target many organisations simultaneously.

Cybercriminals have mainly targeted large companies, but now any sized organisation is "fair game". Perhaps "easy game" is a better phrase, as cybercriminals will often go for the easy rather than the big.

Smaller organisations are less likely to have large businesses' multi-layered, sophisticated defences. Systems like Rebasoft now cost-effectively offer protection. Companies of all sizes can now stand up a more effective guard, reducing their risk of infection.

How do you best defend against Ransomware?

Studies have shown that leading organisations that invest in the right technology and processes are four times more likely to prevent a ransomware infection. Such organisations also implement and maintain compliance with security standards such as Cyber Essentials, ISO27001, NIST, and CIS. Following the standards mean organisations can focus on effective defences.

The most effective organisations invest in great value "cybersecurity basics". The basics deliver improved security and avoid "uncontained" costs that can result from the arms race against cybercrime. Such organisations get protection in place more quickly and sustain value over time.

Cybersecurity basics focussed on Ransomware defences, beyond running regular and off-line backups of critical data, are:

1) IDENTIFY AND CLASSIFY ALL THE ASSETS in the organisation

Assets change over time. You need constant discovery and classification to allow you to set and measure security policy for each class of system in the organisation. The resulting real-time asset database ensures that you can find and prioritise a resolution should you have an incident. Rebasoft builds this real-time view.

1. Maintain a VULNERABILITY PROGRAM that can identify, prioritise, and quickly fix issues

   - A ransomware attack happens every 11 seconds. 20,000 vulnerabilities are found each year. Rebasoft implements real-time, scan-less vulnerability checks that help ensure vulnerable systems are identified and quickly updated

2. Ensure SECURE CONFIGURATIONS are implemented, including the first line of defence against Malware – Antivirus systems - on all systems

   - Systems without Anti-virus and other misconfigured settings are likely to be found by cybercriminals. Rebasoft helps find and fix security gaps before Ransomware is planted

2) RESPOND quickly to reduce the impact of any infection

   - Rebasoft can help monitor the network for signs of infection and quickly isolate infected devices before they can spread their disease. This reduces the recovery costs and allows fast restoration of systems to minimise business interruption.

CAN YOU EVER BE 100% SAFE FROM RANSOMWARE?

There are three reasons that you can never be 100% safe from Ransomware:

1) Malware often exploits user behaviour. People make mistakes and can be duped by sophisticated, socially engineered attacks. While better training helps, it can never eliminate the human factor.

2) Vulnerabilities are constantly announced, but perhaps, many more are found and not disclosed and kept as "tools of the trade". This means that cybercriminals can use unknown vectors to attack.

3) The first line of defence - Antivirus systems - relies on signature patterns and heuristics. There is often a time lag between a new malware item being discovered and analysed and a "fix" available in your antivirus system.

Even against these odds, you can reduce the impact of infection through quick identification and changing network access to prevent the spread of an attack.

SHOULD YOU PAY THE RANSOM?

If you are unfortunate enough to be hit with Ransomware, while it might seem cheaper to pay a ransom than go to the expense of re-building the IT systems from scratch, payment is not advised. The authorities state that paying the cybercriminals "feeds the beast". If criminals can make it pay, they will continue their nefarious activities.

To change behaviour, authorities such as the US Treasury department are now starting to make it an offence to pay ransoms. This will, in the future, mean that ransoms may not be insurable, and payment of a ransom could become a criminal offence for the organisation and its senior management.

CALL TO ACTION

Contact Rebasoft or your partner to understand better how we can be part of your Cyber resilience program.

FOR MORE INFORMATION:

Rebasoft's all-in-one security system helps with Network Security, Asset Security, Vulnerability Management, Network Access Control. It can also save you money through retiring point monitoring solutions.

For more information, visit us at: https://www.rebasoft.net/.