Empire Technologies

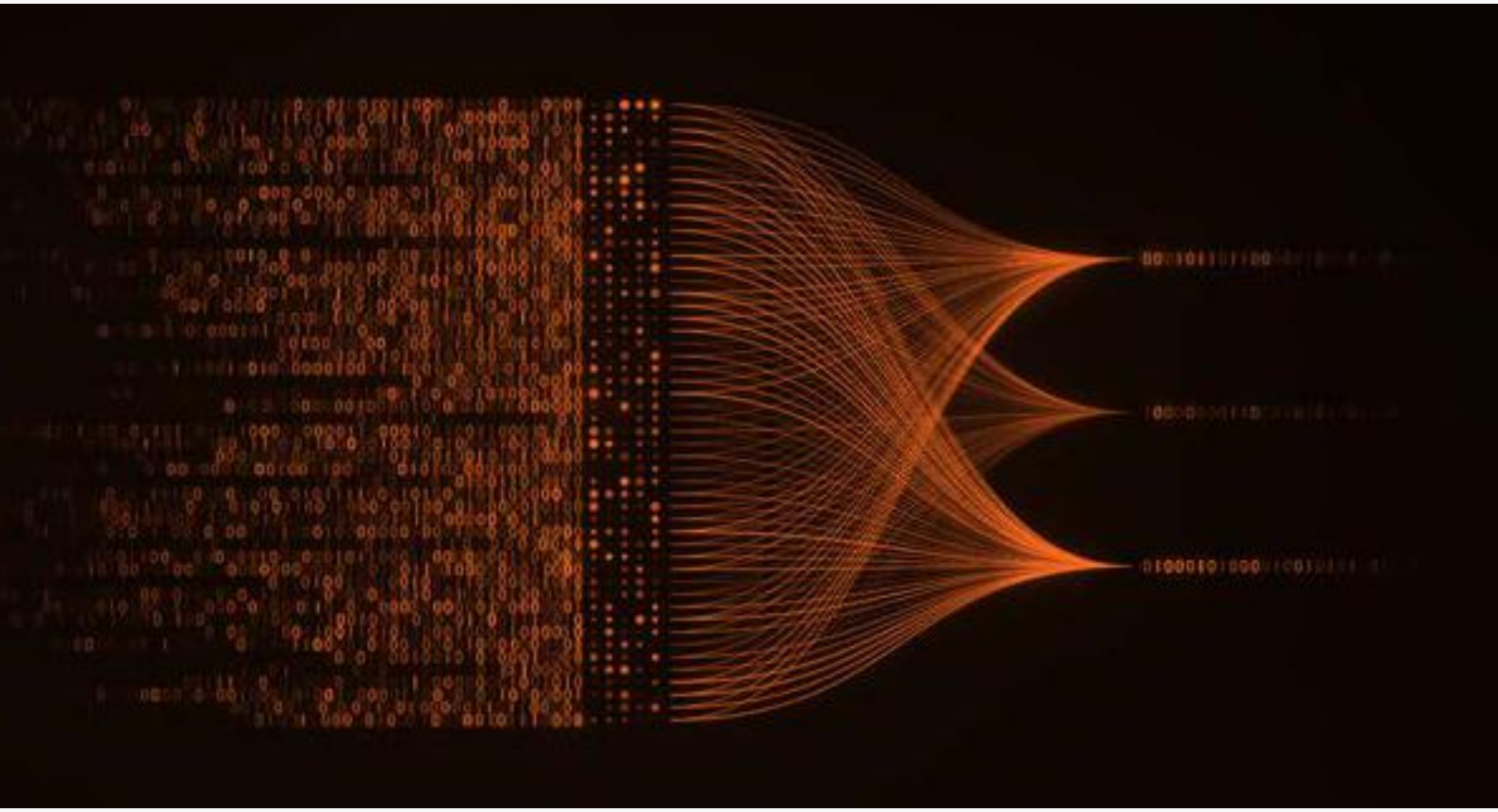
Cyber security • Essential Eight Experts

Case Study

Rapid Response and Recovery from a Ransomware CryptoLocker Attack at a Large Distributor of General Medical Devices and Supplies

Prepared by :

Empire Technologies Cyber Security Engineers



Rapid Response and Recovery from a Ransomware CryptoLocker Attack at a Large Distributor of General Medical Devices and Supplies

INTRODUCTION

In the face of a critical cyber security crisis, a prominent distributor of general medical devices and supplies experienced a significant Ransomware CryptoLocker attack that compromised their entire server infrastructure. At the time of the incident, they were not Empire Technologies clients; however, recognising the urgency of the situation, the company engaged Empire Technologies by reaching out for assistance to manage the attack and restore their operations. This urgent situation prompted an immediate response from Empire Technologies, a leader in cyber security solutions, who promptly intervened to manage the attack and restore the company's operations.

What is Ransomware?

Ransomware is malicious software designed to encrypt files or lock users out of their systems, rendering the data inaccessible. It operates on a simple yet nefarious principle: cybercriminals demand a ransom from the victims to unlock their data or regain access to their systems. Understanding how ransomware works is crucial for individuals and businesses to protect themselves from this growing threat.

BACKGROUND

The distributor operated with a large number of servers, which were essential for its daily operations. The ransomware attack encrypted data across all servers, rendering them inaccessible and threatening to disrupt the entire business process and the company's reputation.

CHALLENGE

The company faced several immediate challenges:

- The entire server network was infected, jeopardising critical data and operational continuity.
- There was an urgent need to restore essential services before the start of the next business week to minimise downtime and financial impact.
- Compliance with cyber insurance policies requires a thorough forensic analysis to understand the breach and secure potential claims.

Empire Technologies

IT Support and Cyber Security

https://www.empiretechnologies.com.au/

Sydney, NSW | Melbourne, VIC | Brisbane, QLD | Adeleide, SA | Perth, WA

SOLUTION

Empire Technologies implemented a multi-step recovery process:

1

Initial Assessment and Response:

Upon receiving the distress call on a Friday afternoon, a specialised response team from Empire Technologies was promptly deployed to the affected site. The engineers' immediate action was to sever the network connections of all compromised computers to halt further dissemination of the malware. Subsequently, they initiated the installation of an advanced XDR (Extended Detection and Response) agent on each computer, fortifying their defences against additional malware activities.

To pinpoint the origin of the security breach, the team conducted a meticulous forensic analysis. This investigation was performed offline to ensure the utmost security and integrity of the data. The objective was to accurately determine the exact date and time the malware infiltrated the system, which was critical for understanding the attack vector and preventing future incidents. This approach not only contained the immediate threat but also provided crucial insights into the recovery point, thereby facilitating a strategic roadmap for a comprehensive recovery and robust system fortification process.

2

Server Recovery and Data Restoration:

The engineers prioritised recovering critical virtual machines by utilising Pure Storage's Snapshot and Safe Mode. They were able to successfully restore the VM by using a Snapshot that was taken one hour before the attack. During the recovery process, they kept the systems isolated from any network to prevent the possibility of recontamination.

3

Systematic Verification and Network Reintegration:

Each virtual machine was methodically cleaned, updated with the latest security patches, and scanned for vulnerabilities. The first machine to be reconnected was a critical domain controller, ensuring it was completely secure before reintegrating it into the network.

RESULTS

Empire Technologies implemented a multi-step recovery process:

4

Extended Recovery Process:

Following the same recovery process, the remaining 90 virtual machines were restored, prioritising from the most to least critical. By Monday, all essential services were back online, with minimal disruption to the company's operations.

5

Communication and Compliance with Insurance Requirements:

Despite initial challenges in communicating with the insurance team, persistent efforts by Empire Technologies ensured that by Monday, the affected infrastructure was successfully isolated for the insurance forensic analysis. This critical step was in compliance with cyber insurance requirements, helping to facilitate the claims process and ensure thorough documentation of the incident.

Responsive Action Plan

Creating an incident response plan involves outlining a detailed strategy for how an organisation will identify, address, and bounce back from cyber security incidents. These incidents may include data breaches, ransomware attacks, insider threats, and denial-of-service (DoS) attacks. A well-prepared incident response plan offers a structured method to minimise the effects of cyber incidents and promptly restore regular operations.

Empire Technologies

RESULTS

Empire Technologies' efficient crisis management led to the complete recovery of all affected servers by the following Monday, effectively minimizing potential operational and financial consequences. The rapid recovery not only ensured the uninterrupted functioning of the Large Distributor of General Medical Devices and Supplies but also met all insurance and regulatory obligations.

LESSONS LEARNED

This incident highlighted the critical importance of robust security measures and a responsive action plan. Post-incident, the large distributor of general medical devices and supplies has enhanced its cyber security protocols, including regular updates, more frequent backups, and comprehensive disaster recovery strategies.

Rapid Response and Recovery from a Ransomware CryptoLocker Attack at a Large Distributor of General Medical Devices and Supplies

The perfect balance to do it all on your terms and make an impact.

CONCLUSION

Empire Technologies' rapid and effective response to this severe ransomware attack demonstrates our cyber security and crisis management expertise. Our proactive measures and strategic recovery plans are designed to ensure that businesses can quickly rebound from cyber threats with minimal impact.

Call to Action

Protect your business from unexpected cyber security threats. Contact Empire Technologies today to learn how our expert services can safeguard your operations and ensure you are prepared for any incident.

We take pride in our ability to provide tailored solutions that meet the unique needs of each client, ensuring their success in an ever-evolving digital landscape.

Find us.

https://www.empiretechnologies.com.au/
1300 754 718

Empire Technologies

IT Support and Cyber Security
https://www.empiretechnologies.com.au/
Sydney, NSW | Melbourne, VIC | Brisbane, QLD | Adeleide, SA | Perth, WA

Empire Technologies

IT Support and Cyber Security

https://www.empiretechnologies.com.au/

Sydney, NSW | Melbourne, VIC | Brisbane, QLD | Adeleide, SA | Perth, WA

Cyber security • Essential Eight Experts

TRUSTED BY SOME OF THE WORLD'S LEADING ORGANISATIONS.

Microsoft veeam SentinelOne PURESTORAGE VOCUS vmware DELL FORTINET cisco SOPHOS

Empire Technologies started as a team of passionate individuals with a common goal: to empower businesses through technology. Today, we are a trusted partner offering technology solutions to businesses across Australia. Our experienced team understands the intricate needs of businesses and provides seamless operations. We take complete ownership of maintaining and supporting the solutions we deploy, ensuring our clients achieve their business objectives.

Thank You

FOR YOUR TIME

We are here to help you, count on us.