Prifysgol Cymru
Y Drindod Dewi Sant
University of Wales
Trinity Saint David

Impact of Ransomware Attacks on Business Operations: Mitigation Strategies and Recovery Framework

School of Applied Computing

Chris Thomas 1252344, University of Wales Trinity Saint David

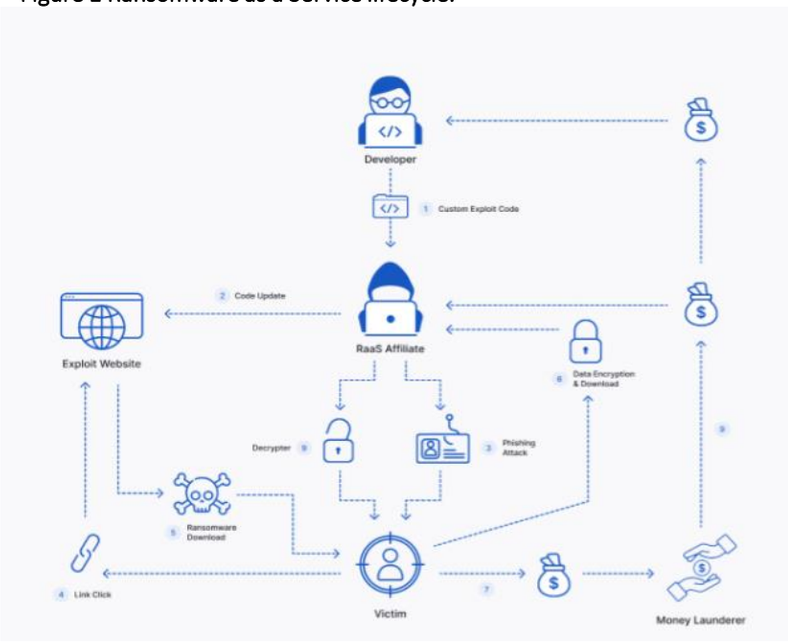
1. Introduction

In June 2023, an end user working in the warehouse in Virginia received an email with an attachment. They recognised who the sender was and opened the attachment. The end user did not realise that the account from the sender was compromised, that the email was from an attacker who had taken control of that users email account and began an email campaign sending malicious attachments attempting to gain access to company networks. This type of attack the end user suffered was a Phishing attack; specifically, this was a Spear Phishing attack. Spear Phishing attacks work when the attackers target an individual or an entire organisation.

2. Objectives

- Conduct an in-depth examination of security vulnerabilities and technologies.
- To enhance and improve the businesses network infrastructure for example new Cisco switch infrastructure and fibre optic backbone.
- To implement further security measures and protocols for the network to prevent further unauthorised access and data loss. For example, Microsoft Multifactor Authentication (MFA) and Duo authentication for server hardening (2FA).
- Procure new Palo Alto firewalls for the business and implement them.
- Implementation of new antivirus and malware protection globally.

Figure 1 Ransomware as a Service lifecycle.



3. Research Overview

Malware is a form of software that has been deliberately created to disrupt the operation of a computer, server or networkand its primary function is to breach the user or organisation's privacy by leaking sensitive information or disrupting the user's ability to operate that device [1].

Polymorphic viruses are part of the malware family; they can dynamically alter their code while retaining their core functionality. This quality makes them particularly elusive to antivirus software (AV) that uses signature-based detection methods, the main aim of polymorphic viruses is to evade being spotted by AV products by changing their appearance each time they infect a new file or system [2].

Metamorphic viruses are more complex in sophistication than their polymorphic counterparts. Metamorphic viruses undergo a complete code transformation, unlike polymorphic viruses, which can alter their appearance while preserving their core functionality[3]. They perform this task each time they propagate; by doing this, they can evade detection from AV software [3]. The metamorphic virus will use many methods to disguise itself; for example, code shrinking, garbage code insertions etc.; each time it performs one or more of these functions, it recompiles itself, and it will look completely different from the one that infected the device to the following [4]. These viruses are crafted to be elusive; metamorphic viruses skilfully avoid AV measures. They actively thwart attempts at heuristic analysis and utilise anti-emulation techniques to impede detection. Engineered for persistence on infected systems [5].

Ransomware is malicious software designed to prevent access to a business or user's computer system files, files and company/user data. Ransomware achieves this by encrypting the data or locking the devices [6]. Ransomware as a Service (RaaS) is a cybercrime business model where ransomware developers create and maintain ransomware tools and infrastructure to be sold on the dark web, these tools can be used by anyone that is willing to pay for this service [7]. An example of a RaaS attack: BitPaymer is an encryption ransomware trojan that became active in August 2017. It targets large organisations and victims' files and encrypts them. Once they have been encrypted, the ransomware demands large ransom payments to decrypt user data; it provides a URL for bitcoin payment, for example, 53 Bitcoin, which equates to $200,000 [8]. One such victim was NHS Lanarkshire, infected with this ransomware on August 25th; it infected their systems by utilising a brute force attack via Remote Desktop Protocol (RDP), encrypted the affected system, and moved to the next [9].

4. Remediation Work

Step One: Replace all End of Life Switches with new Cisco 3850 and brand new Cisco 9300 and new Fibre backbone.

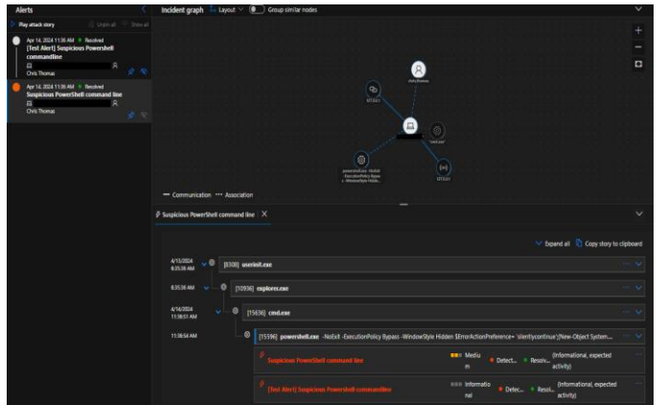
Step Two: Implement Multifactor authentication across all applications and servers. Duo for servers & Microsoft MFA for applications.

Step Three: Windows Defender for endpoint deployment across the entire estate.

Step Four: Password Management implementation. Proof of concepts for 1Password and Keeper.

Step Five: To replace the Global firewall solutions from Cisco ASA and Checkpoints to Palo Alto 3420 and PA 450 devices.

Figure 2 Defender Test Incident



6. Conclusion

This project aimed to discuss how the breach occurred, what type of attack it was, and what steps were taken to strengthen the network. The author focused their research on what security vulnerabilities all businesses suffer from, such as malware and viruses, and what security technologies can be implemented to help mitigate such attacks. The attack showed that the business's security posture should have been better, as the attackers could move around freely and cause significant damage.

References

Further Reading