Ransomware: A Cyber Security Policy Brief

1st Kelvin Popovic
B.Sc Hons (IT & CS)
North-West University
kelvin.popovic@gmail.com

2nd Joshua Esterhuizen
B.Sc Hons (IT & CS)
North-West University
joshua.esterhuizen27@gmail.com

3rd Jumanah Al-Hazba
B.Sc Hons (IT & CS)
North-West University
jumanah1998@gmail.com

4th Affaan Muhammad
B.Sc Hons (IT & CS)
North-West University
affaanm94@gmail.com

***Abstract*—This is the 2-page analytical policy brief as part of the C3SA Cyber Security 9/12 Strategy Challenge**

***Index Terms*—Ransomware, Policy, Cyber Security, Internal & External Attacks, E-Commerce, Banks,**

I. Introduction

The focus of this discussion is on recommendations for actors to follow, both non-state and state. It discusses the long and short impacts of these recommendations as well as which agencies are responsible for these recommendations. Furthermore, this policy will discuss whether an actor should attribute the threat and how to respond to these Ransomware threats.

II. Collaboration between banks and e-commerce business

As e-commerce services almost always make use of electronic payment methods, such as electronic transfers. Therefore, both the e-commerce industry and the banking sector need to collaborate to ensure that the security surrounding the network communication between them is as sound as possible as well as providing warnings in the event of attacks. There needed to be security measures on both ends to ensure that the data that is being transferred between each other is what was intended to be sent and has not been intercepted and modified or replaced with ransomware – as an example.

III. Addressing these ransomware attacks - Internally and Externally

Internally, these actors need to respond immediately to restore their website capabilities. As such, they need to rollback to an uninfected version of the site if possible – as such, offline back-ups are also a strong recommendation for the actors involved. It is also important that these actors make use of an incident response plan crisis management plan if they have ones already set up and if not should update internal policies to include these types of plans. As the e-commerce sites are infected with ransomware and are functionally defunct, they should be taken offline for the time being until they have been reinstated to a functioning version – which will also protect consumers if it is more than just a ransomware attack. Lastly, it is also important to not actually give in to the attackers' demands.

As for externally responding to the threat, the actors involved have several choices on how to handle the situation. They can either attribute the threat or not as well as publically disclosing this response or not. While attributing what type of attack has happened publically is not vital it should also be noted that the exact type of attack may not be known. However, these actors do have an ethical implication to inform their consumers of any attacks that would affect them in some form – either by disrupting transactions or involving their data.

IV. Long and short term impact of the recommendations

A. Short term impact

The short term impact of implementing the recommendations will be:
The high initial cost to implement the policy and provide appropriate training to employees and users that will ultimately remedy any further significant costs from incidents and reputation loss as a result. The short term impact will also enable the organisation to create a clear and comprehensive incident response plan and backups to recover if any further attacks are initiated. The inclusion of a report plan lets users and employees know exactly how and where to report suspicious activity that technicians can assess faster. Immediately removing/disconnecting the affected system to prevent the attack from propagating within the system will significantly improve the short term outcome. The restructuring of access to a least-privilege principle and segmentation of the network will make internal and external systems more inconvenient to compromise as a whole.

B. Long term impact

The long term impact of the recommendations will, over time, affect the organisational culture surrounding security and the responses to security violations. The shared goals of improving security in the organisation will vastly enhance the identification of attacks, responses, and restoration of systems and reporting incidents. The long term impact from additional security and response will make the system more resilient and inconvenient to attack due to faster and more appropriate reactions.