ADDRESSING RISING CASES OF RANSOMWARE ATTACKS

Student’s Name

Course

Date

Cyber systems are increasingly becoming a primary resource for successful engagement in business activities. In particular, organizations and individuals have increasingly become dependent on the internet of things as a means of integrating different factors of communication. Improvements in the technology available and consequent development of various device applications has led to innovation in means of gathering user data for various cyber systems, leading to some individuals engaging in activities that significantly compromise the integrity of the systems. In particular, ransomware forms one of the most significant threats to cyber security in contemporary society, with the consequent exploitation of user data leading to hackers using the information to make changes on the users’ hardware, and seek compensation to restore the devices to functionality.

Ransomware primarily involves the use of a computer software to compel other users whom a particular individual would have gained information about to provide a fee for the restoration of the device to complete functionality. Most as recent as 2017, the WannaCry attack made headlines following the use of a cruptoworm to encrypt data on Microsoft Windows devices, and proceeded to demand payment for systems restoration to functionality.[[1]](#footnote-1) The attack on a system as large as Microsoft, in addition to the ease of access to the payments demanded, which was to be in the form of bitcoin, exposed the vulnerability of society to ransomware. Such issues necessitate a significant research on how best to deal with similar attacks, and in effect control the extent to which technology makes users vulnerable.

Notably, cyber security has been a subject of significant discussion in contemporary society, but much of the attention given to the issue relates to cyber attacks and exploitation. However, reports on recent cases of unauthorized access to cyber systems reveal that the risks of ransomware are ever increasing.[[2]](#footnote-2) The primary challenge associated with this form of cyber insecurity is the damage caused to society through the activities that the attacks end up hindering, some of which are critical to human welfare.[[3]](#footnote-3) Society does not have to suffer a catastrophic case such s an attack on a hospital to pay much more attention to the problem. As long as the trends in the nature and frequency of attacks indicate increased complexity, then an effort to control the issue is of much importance. However, society can only institute control measures based on an understanding of the potential implications of investing in some of the suggestions made by individuals with an exceptional command of cyber systems security.

One of the most common solutions to most issues in the workplace has often been straining the employees, and such would also be helpful in helping mitigate cases of ransomware attacks. In particular, phishing forms one of the primary means using which the attackers gather information that they end up using to conduct the attack. It includes sending a link to the target system within a particular network, with the hope that the user would then open the link, thereby giving the source of the said ransomware access to the computer systems, and by extension, the network to which it is connected. Ultimately, the employee would have ended up giving an opportunity to the attackers, unconscious of the implications of his or her actions to the network’s integrity.

One of the primary advantages of this approach lies in the normalcy of its application. Notably, if an organization decided to train its employees on ransomware and the phishing concept, then the training process would be relatively similar to those which the workers have experienced in the past for other purposes related to their productivity at the company. Therefore, it would be relatively easy to implement a training program in response to the issue. However, this solution is only applicable to organizational settings, but the attacks are not limited to such environments. Just as the organizations, individual cyber users could be vulnerable to ransomware attacks, which necessitates that the measure developed as a possible solution be inclusive of individuals not working within organizational contexts. Although various software developers could provide some insight on the best use of the platforms and in effect protect them from potential phishing vulnerabilities, this solution may not be as effective for individual use.

Alternatively, constant updates to the security system used by particular user to protect the IoT could be a solution effectively addressing the chances of a ransomware attack. Constant efforts to determine the ability of the security framework to counter the existing threats could be a solution, if only one is capable enough of making the necessary updates to the security software as and when improvements are made to the system. In any case, different firms make extensive investment in research and development of potential security software, which in turn increase the ability of the organizations and individuals to remain safe, knowing that they have an application in place to provide an alert in the event of any suspicious activity in their system. On the other hand, making an effort to constantly review the devices connected to a particular user’s cloud would be integral to understanding the potential for attacks and taking the necessary measures to prevent such an outcome.

Notably, the efforts to maintain the integrity of the cyber system present an advantage to the user, by ensuring that one has absolute control of the security of his or her devices. Additionally, individuals as well as organizations could easily implement this measure, using security products from some of the renowned security services providers available in the market. After all, their investment in ensuring that the cyber space is secure enough, and prevention of cases of ransomware attacks or other forms of cyber space challenges increases their appeal to the market, ultimately influencing the quality of their security products. The only disadvantage with these systems lies in the cost of investment in the systems, which in turn implies that they may not be as cheap to procure, particularly where the ultimate impact of the security framework is highly guaranteed.

In conclusion, developing and implementing solutions to mitigate cyber security issues is paramount to future success in the cyber environment. Ransomware attacks currently indicate an upward trajectory, including an increase in the costs incurred by organizations and individuals who fall victims to the attacks. Notably, improved technology through factors that include blockchain currencies such as bitcoin adds on the challenges in recovering finances lost through ransomware, due to difficulties tracing the money once disbursed. Based on the two solutions herein analyzed, constant updates to the security system and management of the features therein is one of the most effective solutions, with a high chance of deterring cases of attacks in the future for both individuals and organizations.

Bibliography

Kate O’Flaherty. “How To Survive A Ransomware Attack -- And Not Get Hit Again.” *Forbes,* August 17, 2018. <https://www.forbes.com/sites/kateoflahertyuk/2018/08/17/how-to-survive-a-ransomware-attack-and-not-get-hit-again/#4661d18c6cd3>

Yaqoob, Ibrar, Ejaz Ahmed, Muhammad Habib ur Rehman, Abdelmuttlib Ibrahim Abdalla Ahmed, Mohammed Ali Al-garadi, Muhammad Imran, and Mohsen Guizani. "The rise of Ransomware and Emerging Security Challenges in the Internet of Things." *Computer Networks,* 129 (2017), 444-458.

1. . Kate O’Flaherty, “How To Survive A Ransomware Attack -- And Not Get Hit Again,” *Forbes,* August 17, 2018, <https://www.forbes.com/sites/kateoflahertyuk/2018/08/17/how-to-survive-a-ransomware-attack-and-not-get-hit-again/#4661d18c6cd3>

   [↑](#footnote-ref-1)
2. . Yaqoob, Ibrar, Ejaz Ahmed, Muhammad Habib ur Rehman, Abdelmuttlib Ibrahim Abdalla Ahmed, Mohammed Ali Al-garadi, Muhammad Imran, and Mohsen Guizani, "The rise of Ransomware and Emerging Security Challenges in the Internet of Things," *Computer Networks* 129 (2017) 445. [↑](#footnote-ref-2)
3. O’Flanherty, How to Survive a Ransomware Attack, 2018 [↑](#footnote-ref-3)