International Research Journal of Advanced Engineering and Science
ISSN (Online): 2455-9024

Ransomware Software: Case of WannaCry

Maxwell Mago[1], Farai Fransisco Madyira[2]
[1]Lecturer, UZ School of Technology, University of Zimbabwe
[2]Engineering Instructor, UZ School of Technology, University of Zimbabwe
Phone: +263 773 042 703, +263772 993 276

***Abstract*— *Cybercrime has of late proved to be a major handicap in the maintenance of secure information technology (IT) systems. It is achieved with the use of malware such as ransomware. Examples of such tools that attacked several sectors of the world economy lately are CryptoLocker and WannaCry. This paper attempts to explore different means of protecting IT systems and measures for easy recovery of attacked ones. Additional important suggestions that organizations normally take for granted (human related) are also presented, because security issues in an organization must be taken as everyone's responsibility.*

***Keywords*— *Bitcoins; Cybercrime, CryptoLocker, DoublePulsar, malware, mitigation; Server Message Block; WannaCry.*

I. INTRODUCTION

The rise of the Internet has benefited all and sundry, individuals and business organizations. It led into the transformation of human communication which has become more efficient and effective. This very tool (that is, the Internet) also brought with it a new dimension of problems which is referred to as cybercrime. According to Computer Crime Research Centre (2006), cybercrime is defined as crimes committed on the Internet using the computer as either a tool or a target victim. In the recent past, it has been noted with great concern that there is an increase in the use of Ransomware as a tool to perpetrate cybercriminal activities.

Ransomware present critical risks to both individuals and business organizations, hence the need to craft plans to tackle ransomware assaults. It is a type of malicious software that blocks access to the victim's data and/or threatens to publish or delete it unless a ransom amount is paid. Some simple ransomware may lock the system in a way which is not difficult for a knowledgeable person to reverse, but others are more advanced and encrypt the victim's files and make them inaccessible thereby demanding a ransom payment to decrypt them. Rouse (n.d) says that ransomware is a malicious code that is used by cybercriminals to launch data kidnapping and lockcsreen attacks, under the motivation of monetary gains. Sadly, in spite of all the acknowledgement of an increase in ransomware assaults, a small number has put in place enough artillery to defend themselves against these assaults, Simmonds (2017).

When information has now become recognized as the lifeblood of organizations (Fink, 1994; Reddy *et al*, 2009), the computing systems that handle it have to be structured and maintained with certainty. Attending to and investing in the prevention of malware such as ransomware has therefore become a survival and/or recovery necessity for many individuals, organizations and nations.

II. BACKGROUND

From about 2012 the use of ransomware scams has grown internationally, e.g. CrptoLocker that was particularly successful, securing an estimated $3 million before is was taken down by the authorities. Ransomware is also increasingly becoming a problem in South Africa, Zimbabwe and the entire Sub-Saharan Africa region, although it is still estimated that most affected companies shun reporting incidents for fear of reputational damage. Recently, many South African firms fell victim to the WannaCry ransomware.

Despite the noted tremendous momentum and continued increase in the use and application of computing information systems, security and privacy issues continue to pose serious roadblocks to organizations' dependency on these invaluable systems. This raise the need for the establishment of various approaches to address these challenges, existing solutions and more work that focuses on providing trustworthy environments. Only such efforts will guarantee the perceived benefits that are achievable from these systems.

2.1 Scientific Issues, Objectives and Proposition

Available literature identify a multitude of benefits accruable from the use of safe and stable information technology (IT) systems. These are superior accessing and processing speeds, limitless (broadband) capacities, seamless transition from one system to the other, added confidentiality, capabilities for data recovery and miniaturization of storage space. In the background is a presentation of experiences from organizations that are applying these systems. Contrary to literature however, these firms have had an enormous amount of challenges in achieving the intended benefits from their IT systems.

The employ of IT systems have been mirrored in possible losses, costly, security concerns and uncertain/risky undertaking that threaten the expected benefits and continued use of these systems. Such trends are bound to continue, if firms do not come up with strategies to ensure that their systems become more secure from such malware threats. This paper is focusing on identifying measures necessary to mitigate ransomware such as WannaCry.

The major objective of the paper is to determine measures to mitigate the effects of ransomware attacks, so that IT systems can become more secure. Following are the specific objectives:

- To identify the impact of ransomware on organizations IT systems.
- To explore IT systems vulnerabilities towards ransonware attacks.

- To investigate mitigation practices against ransomware attacks.
- To recommend additional measures necessary for protecting organizations IT systems from ransomware attacks.

The advanced proposition is that the severity of ransomware, insecure IT systems and any mitigation practices have an impact on the security of organizations IT systems from ransomware attacks.

2.2 Significance, Scope and Paper Outline

Considering the impact of IT systems on individual and group entities, this study is going to make significant contribution to the entire magnitude of these user groups through the assurance of secure IT services from different IT systems. Assurance is of importance in the attainment of services that have been recognized as essential for both survival and recovery purposes. The academic fraternity will get an in-depth understanding of the existing puzzle in the determination of secure IT systems, for achieving the expected rewards.

Generally, IT users strive to achieve favorable returns from invested resources. Many studies confirm that ICT occupy a large portion of these resources, especially now when information is considered the life blood of organizations, Fink (1994). The preparation of secure IT systems is one such a measure taken by firms and individuals in improving their performance through embedded IT systems. This makes the paper an interesting and relevant one for the majority of organizations, regardless of size, sector and location.

The remaining part of this paper contains literature review on ransomware and its effects in order to unmask a deeper understanding of the origins of subject under scrutiny.

III. Literature Review

According to Ciampa (2017), malware is a noxious software program that infiltrates into a computer based system while the user is unaware and executes a damaging act. Malware is said to utilize risk vectors to convey a malignant payload that executes the damaging act once it is summoned. One major way of categorizing the different classes of malware is by utilizing the different attributes that malware have. These attributes include how they hide in the system (concealing), how they migrate from one system to another (propagation), how they infect other systems (infection), and the capabilities of the noxious software. One such types of malware is called ransomware.

3.1 Ransonmware in the Context of Malware

Ransomware is a type of malware which scrambles files on a victim's computer system and holds the unscrambling key until a payment is made by the victim, Scaife *et al* (2017). This notion is supported by Bhardwaj *et al* (2016) who say that ransomware is a malware that is categorized under computer based blackmail driven by the use of noxious software programs that contaminates systems through the utilization of several attack vectors which include social engineering, freeware applications, botnets, emails and enticements to draw in a target victim. The method that is sort after by a cyber-attacker is having the victims download the malicious software which contaminates the computer system. This software is then implemented concealed in the victim's computer system. The malicious code then assumes control of the computer system resulting in the scrambling of the victim's data or denial of access.

Ransomware utilises terror strategies to drive victims into paying the demanded amount in Bitcoins (normally untraceable computerized money) or supplying personal information. However, there are instances where files are not decrypted even after a payment has been made. The general consensus is that ransomware insists in two major categories which are crypto and locker. This entails that the hostage holding of the computer system is achieved by either encrypting files or locking the computer system.

WannaCry is a type of ransomware. It is a member of the malware group which scrambles computer system data and requests payment in order for the victim to get the unscrambling key (Vigliarolo, 2017). This expensive digital assault was unleashed on Friday the 12th of May 2017 and it affects individuals and organization in many sectors of the economy. The focal point of the assault were Microsoft Windows framework which resulted in over two hundred and thirty thousand (230 000) computer systems compromised in about one hundred and fifty (150) nations.

Even though the WannaCry assault was avoidable, most business organizations and individuals were caught napping. Microsoft had played its part in developing and discharging a vital fix for the problem before it materialized on the 14th of March 2017. This fix had the capability of correcting the weakness that WannaCry capitalized on. When the ransomware was initialized on the victim's computer system, the malware requested payoff for the victim to be granted access again to the computer system, Ehrenfeld (2017). The requested ransom was payable in Bitcoins with the sum doubling in three days for non-payment. If the ransom is not paid in seven days, the assertion was that the scrambled data would be lost.

3.2 IT Systems Vulnerability to Ransomware Attacks

According to Vigliarolo (2017), WannaCry ransomware preyed on unsuspecting users by capitalizing on an imperfection in the structure of Microsoft Windows operating systems referred to as Server Message Block (SMB) protocol. The purpose of this structure is to oversee data communication elements between network entities on local area networks (LANs). Therefore, the imperfection in the Microsoft Windows operating systems permitted poisonous packets to be transferred from a tainted computer system to a clean computer system on the network. This made an infected computer system ground to zero for WannaCry epidemic. In addition, the transferred packets composed of DoublePulsar. DoublePulsar is a tool that was developed by National Security Agency (NSA) which creates a backdoor on Microsoft Windows operating systems thereby allowing WannaCry code to be installed.

3.3 Mitigation Practices Against Ransomware Attacks

Mitigation involves putting in place certain particular practices to avoid the occurrence of some function or process. FEMA (2017) says that mitigation is the effort to reduce loss of life and property by lessening the impact of disasters. In protecting computer systems from ransomware such as WannaCry, such measures include the following:

3.3.1 Updating operating systems

The WannaCry attack was based on flaws that are in the Microsoft Windows operating systems which has since had a security patch developed to curb the weakness. Therefore, the first crucial step towards mitigating WannaCry entails updating or patching Microsoft operating systems with patches that are discharged from time to time to curb discovered system vulnerabilities. On the 12th May 2017 attack there are indications that the infected computer systems had their operating system last updated sometime before the 14th of March 2017, Vigliarolo (2017).

3.3.2 Upgrading operating systems

The continued usage of products that will have reached the end of their lifespan is dangerous as they lack technical support. This has been the case of Microsoft Windows XP as system patches were no longer developed for it and on the 12th of May 2017 attack this operating system was tainted at a higher rate than its counterparts. Therefore, another way of mitigating WannaCry attack is by migrating to newer operating systems that still have full technical support, Warner (2017).

3.3.3 User training

Vigliarolo (2017) insists on training computer system users as a way of curbing current and future cyber-attacks. This entails educating users on how they are expected to behave with regards to cyber security. It ensures that users are made aware of security risks and in a better position to screen these risks, since issues of security have since become everyone’s concern in an organization. Awareness and appreciation are important tenets for practicing such requirements by all and sundry in an organization.

3.3.4 Electronic mails

Electronic mail (email) is one of the primary tools that cyber attackers use to contaminate unsuspecting system users. It is therefore crucial that users do not respond to unsolicited emails as well as not taking action on links and attachments that are embedded into emails as these may result in the downloading of malicious payload onto the system, Ciampa (2017).

3.4 IT Systems Security Measures

These are the necessary measures that can be taken by users and the responsible maintenance personnel in order to control and manage seamless recoveries of the systems from attacks whenever they occur. They include the following:

3.4.1 Data back-up

Properly laid down and frequently tested recovery procedures are the panacea of reliable business continuity processes (BCP). They are the attacks aftermaths measures that enable victims of attacks to restore their core business and other information after the attacked computer system has been disinfected. It is recommended that frequent back-ups are performed and securely stored offline in preparation for disaster recovery processes. Symantec Security Response (2017) says that one of the effective ways of fighting ransomware and ensure non-strenuous recovery from an attack is by creating regular system back-ups.

3.4.2 Cloud services engagement

Cloud computing is a new approach to securing information and communication services on-demand, eliminating the costly requirement to install and own the necessary infrastructure and/or facilities, Mago *et al* (2016). The use of cloud facilities help in the alleviation of ransomware problems as these are used as repositories for data handling and back-ups. The back-ups can then be used to restore system stature and/or data to the previous last known good state. However, it is crucial that this security measure be associated with a reliable cloud vendor with a strong security structure for it to be effective, considering the idea of outsourcing the storage of important/essential organizational information.

3.4.3 Effectiveness of any such measures

Arguments and counter-arguments have been raised on the magnitude and effectiveness of many of these and other IT systems security measures. Miller (2012) says that some of these approaches are not only expensive but precarious. On cloud computing, Choubey *et al* (2011) note that it has associated risks and threats which include security, data linkage, insecure interface and sharing of resources and inside attacks. Anderson (2004) believes that in some ways the digital data sets and information are more fragile than paper-based or physical specimen collections and archives.

3.5 Summary

The literature analysis has reviewed that ransomware is an attack tool that is based on the malware architecture. This attack has been around for a while although the recent past has seen an escalation in its use, tearing down security thresholds of both individuals and business organizations’ IT systems. It is a worrying phenomenon as the ransomware attacks are launched at an alarmingly gigantic scale, leading into several hundreds of thousands of computer systems infected across the globe. These attacks have resulted in huge data destructions of several victims. Furthermore, the attacks are being aided by the use of Bitcoins, an encrypted digital currency that makes it difficult to trace the perpetrators.

It has also been noted with great concern that the success of ransomware, specifically WannaCry owes to the negligence and/or complacency of both individuals and business organizations as their operating systems were either not up to date or they were using old versions of operating systems that were no longer supported by their vendors for example Windows XP. It brings to light the importance for operating systems to be constantly updated and upgraded.

In addition, it has also been noted that the primary tool that attackers use to infiltrate systems is email. This entails that there is greater need for educating users on the dangers of downloading email attachments and action links embedded in the emails that they receive. Educating users make them more security aware that result in the reduction of ransomware attack instances, especially considering the current widespread use of office IT systems in accessing social media platforms and online games.

These observations put under the spotlight human efficiencies over and above the identified technical approaches and capabilities. The strengths and ability of the technical systems alone will leave a lot to be desired.

REFERENCES

[1] W. L. Anderson, "Some challenges and issues in managing, and preserving access to, long-lived collections of digital scientific and technical data," *Data Science Journal*, vol. 3, pp. 191-201, 2004.

[2] A. Bhardwaj, V. Avasthi, H. Sastray, and G. V. B. Subrahmanyam, "Ransomware digital extortion: A rising new age threat," *Indian Journal of Science and Technology*, April, vol. 9, issue 14, pp. 1-5, 2016.

[3] R. Choubey, R. Dubey, and J. Bhattacharjee, "A survey on cloud computing security, challenges and threats," *International Journal on Computer Science and Engineering (IJCSE)*, vol. 3, issue 3, pp. 1227-1231, 2011.

[4] M. Ciampa, Security Awareness: Applying Practical Security in your World, 5th ed. Boston: Cengage Learning, 2017.

[5] Computer Crime Research Centre, Cybercrime definition, 2006. Available at http://www.crime-research.org/articles/joseph06/ *(*Accessed 01/09/2017).

[6] J. M. Ehrenfeld, "WannaCry, cybersecurity and health information technology: A time to act," *Journal of Medical Systems*, vol. 41, issue 7, 2017.

[7] FEMA (2017). What is Mitigation? Available at https://www.fema.gov/what-mitigation (Accessed 01/09/2017).

[8] D. Fink, "A security framework for information systems outsourcing," *Information Management & Computer Security*, vol. 2, issue 4, pp. 3-8, 1994.

[9] M. Mago, T. Matekenya, and D. Madzikanda, "Dertemining Firms Preparedness for Adoption of Cloud Computing," *Imperial Journal of Interdisciplinary Research*, vol. 2, issue 7, 2016.

[10] C. Miller, Real time, *Hobart Mercury*, 2012.

[11] Rouse, M. (n.d) What is ransomware? - Definition from WhatIs.com – SearchSecurity, available at http://searchsecurity.techtarget.com/definition/ransomware (Accessed 01/09/2017).

[12] G. S. Reddy, R. Srinivasu, S. R. Rikkula, and V. S. Rao, "Management Information System to help managers for providing decision making in an organization," *International Journal of Reviews in Computing*, 2009.

[13] N. Scaife, H. Carter, P. Traynor, and K. R. B. Butler, *CryptoLock (and Drop It) Stopping Ransomware Attacks on User Data*. Nara, Japan, IEEE, pp. 303-312, 2017.

[14] M. Simmonds, "How businesses can navigate the growing tide of ransomware attacks," *Computer Fraud & Security*, March, pp. 9-12, 2017.

[15] A. Bhardwaj, V. Avasthi, H. Sastray, and G. V. B. Subrahmanyam, "Ransomware digital extortion: A rising new age threat," *Indian Journal of Science and Technology*, vol. 9, issue 14, pp. 1-5, 2016.

[16] M. Ciampa, *Security Awareness: Applying Practical Security in your World*, 5th ed. Boston: Cengage Learning, 2017.

[17] J. M. Ehrenfeld, "WannaCry, cybersecurity and health information technology: A time to act," *Journal of Medical Systems*, vol. 41, issue 7, 2017.

[18] N. Scaife, H. Carter, P. Traynor, and K. R. B. Butler, *CryptoLock (and Drop It) Stopping Ransomware Attacks on User Data*, Nara, Japan, IEEE, pp. 303-312, 2017.

[19] M. Simmonds, "How businesses can navigate the growing tide of ransomware attacks," *Computer Fraud & Security*, March, pp. 9-12, 2017.

[20] Symantec Security Response, *What you need to know about the WannaCry Ransomware*, 2017. [online] Symantec Security Response. Available at: https://www.symantec.com/connect/blogs/what-you-need-know-about-wannacry-ransomware [Accessed 24 Jul. 2017].

[21] B. Vigliarolo, *WannaCry: The smart person's guide – TechRepublic*, 2017. [online]TechRepublic. Available at: http://www.techrepublic.com/article/wannacry-the-smart-persons-guide/ [Accessed 24 Jul. 2017].

[22] G. Warner, *WannaCry: Ransomware Catastrophe or Failure?*, 2017. [online] Dark Reading. Available at: https://www.darkreading.com/attacks-breaches/wannacry-ransomware-catastrophe-or-failure/a/d-id/1328900?ngAction=register&ngAsset=389473# [Accessed 25 Jul. 2017].