Available online www.jsaer.com

***Journal of Scientific and Engineering Research*, 2018, 5(9):68-74**

Research Article

ISSN: 2394-2630
CODEN(USA): JSERBR

An Approach to Changing Ransomware Threat Landscape

Kelechi G. Eze, Cajetan M. Akujuobi, Matthew N. O. Sadiku, Pankaj Chhetri

Roy G. Perry College of Engineering, Prairie View A&M University, Prairie View, TX 77446

Abstract Ransomware is getting sophisticated as tools and techniques for mitigating them are getting better. New variants with better encryption, obfuscation, and anti-mitigation capabilities are emerging every day. The negative impacts of ransomware such as huge revenue, asset and reputation loss remain a problem and call for attention. In this paper, we study ransomware possible mitigation solutions following the attack continuum. Before the ransomware attack, we studied the attack vectors and how an attack can be prevented. During the attack, we studied the mechanism of attack, static and dynamic analysis methods as well as other machine learning methods for detecting ransomware. After ransomware attack, we studied how we can recover from the attackthrough solutions like a backup. We introduce an object-based backup storage method for recovering from ransomware attack.

Keywords Ransomware, static analysis, dynamic analysis, machine learning, object storage, erasure coding

1. Introduction

Ransomware is a type of malware that works through encryption. There are so many variants or types of ransomware today. However, the major categories are the Cryto Ransomware and the Locker Ransomware. Examples of popular ransomware variants are Cryptowall, Cryptolocker, Cerber, CBT-Locker, Petya, WannaCry and Crysis [1]. These variants use different types of encryption algorithm to encrypt essential system files or lock access to a system, a system resource or a combination of both. What differentiates ransomware from other types of malware is its unique payload and, in some ways, its propagation method [2]. Ransomware attack ranks high among cyber-attacks and may continue to grow due to its success and profitability [3-4]. Other reasons why ransomware may grow even more in the future are Internet of Things, big data and cloud computing. These technologies have contributed to expanding the attack surface and changing the ransomware threat landscape. Also, as new variants of ransomware are being published by malware authors, threat actors will continuously have access to various tools for launching sophisticated ransomware attack, thereby increasing ransomware attack. This growth of ransomware can be estimated using the number of ransomware incidents within a given period and the number of new versions of ransomware discovered over a period [5].

The question is how do we handle the current trend in ransomware attack? Fortunately, there have been efforts from security researchers and the industry to come up with solutions to ransomware attack. In this paper, we review a good number of these efforts towards solving ransomware menace in three categories of prevention, detection and backup. The paper also discusses how object-based storage can be combined with erasure coding to provide reliable backup applicable in the case of a ransomware attack. The rest of the paper is organized as follows. In section 2, we discuss common ransomware attack vectors and some preventive solutions. Section 3 discusses the ransomware attack mechanism while detection techniques are discussed in section 4. Section 5 discusses ransomware recovery solutions. Object-Based Storage, a backup solution that is applicable to recovery from ransomware attack is discussed in section 6. Section 7 is future directions and 8I is the conclusion.

2. Common Ransomware Attack Vectors and Prevention

Threat actors make use of various means or vectors to transport ransomware and obtain unauthorized access to a target host to compromise resources or data. The web browser, the end user, emails and network software vulnerabilities constitute the major ransomware attack vectors [6]. Most of the time ransomware is packaged in form of exploit kits and propagated by means of one or more of the attack vectors. It is important to focus on the attack vectors especially emails while thinking about ways of preventing ransomware attack. According to [6], the attack surface as well as the chances of an attacker taking advantage of human behaviour while using web browsers and email systems can be controlled by means of strong security policies and defence. Security solution such as a strong firewall, IPS and IDS should be properly implemented and managed to detect intrusions and suspicious activities. Static and dynamic analysis of suspicious traffic and emails should be conducted on a routine basis to detect and block ransomware [7-8] before the attack. Vulnerability assessment of the systems and network software are also important.

3. Ransomware Attack Mechanism

Big data and the Internet of Thing have significantly expanded the attack surface for ransomware infection [9-10]. On the other end, cryptocurrency such as the bitcoin, the payment system associated with ransomware attacks is a highly disruptive technology with a high acceptance and staying power [11-12]. Therefore, we are better off knowing how ransomware attack works to be able to detect and mitigate against it. Figure 1 shows the stages in the ransomware attack.

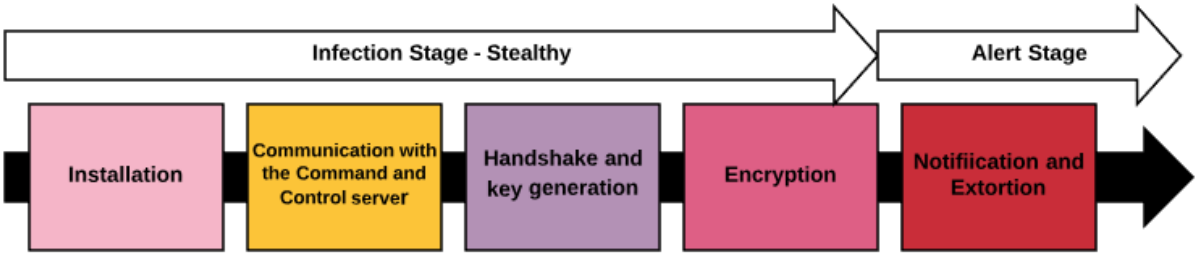

Figure 1: Stages of ransomware attack

- ***Installation***

The infection chain starts with a sequence of installation steps taken by the ransomware payload. A crypto ransomware first finds its way during initial execution into a window process that runs automatically on startup called "explorer.exe" [2]. Explorer.exe is a program manager in Windows-based systems and removing this process will result in the disappearance of the graphical user interface in windows. The second ransomware installation step is the malicious manipulation of the windows registry runkeys. These malicious run keys ensure that the ransomware re-emerges each time the window system is rebooted. In the third step of the installation, the crypto ransomware finds its way into the window service host (svchost.exe), infecting all the shared services handled by this process. The last step in the installation sequence is the removal of the Volume Snapshot Service (VSS) or shadow copy using vssadmin.exe. This destroys the automatic backup process in the window, making backup volumes inaccessible.

- ***Command and Control Server***

Following the installation of malware on the victim's computer is the setting up of a communication channel between the ransomware and the Command and Control server (C&C). The process where a session is established between the C&C server and the ransomware is called handshaking. The command and control server is where the encryption process on the victim's data is activated as well as used to control the generation and distribution of cryptographic keys, payment process and final decryption [2]. The location of the command and control server is usually masked to avoid detection.

- ***Key Generation***

Key generation process takes place to produce encryption keys for encryption and decryption of the victim's data. Modern variants of ransomware use public key encryption mechanism or asymmetric encryption. This has made ransomware attack successful over the recent years. Conversely, private-key cryptography or symmetric encryption method was unsuccessful due to its relative ease of cryptanalysis and subsequent decryption by

security experts. Modern ransomwareuses a combination of AES 256 and RSA 2048/4096 encryption algorithms but some ransomware like CBT locker moves away from this trend [2]. CBT Locker uses a combination of AES 256 and Curve 25519 [2]. AES 256 belongs to the category of encryption algorithm in which the encryption and decryption keys are the same called symmetric encryption. There is key distribution, an essential stage of the symmetric encryption process. Key distribution makes symmetric encryption vulnerable and easy to break due to the possibility of interception and retrieval of the key. On the bright side, AES 256 is comparatively quick and provides good security if the keys are not compromised. RSA 203/4096 is an asymmetric encryption algorithm that uses two different keys, one for encryption and the other for decryption. It is designed such that only the encryption keys are present at the time of encryption thereby making it just impossible to decrypt the data by intercepting the encryption key. However, RSA 203/4096 is relatively slow. A combination of symmetric (AES 256) and asymmetric RSA 203/4096 is also used by ransomware authors to generate an encryption algorithm which is fast and strong. This combination technique can also be referred to as a hybrid solution called Pretty Good Privacy (PGP)

- ***Demand for Ransom***

The final stage of ransomware attack is demand for ransom. Here, the victim machine has been taken hostage. A notification is displayed on the victim's machine with instruction on how to pay a specified amount of ransom in cryptocurrency.

4. Ransomware Detection

Lesson learned from the ransomware attack vector and attack mechanism can be useful in understanding the behaviour of ransomware and what differentiates ransomware from other malware. The goal of ransomware is to stealthily reach as many targets as possible using various vectors of attack to compromise the system functionality and encrypt data stored in the system or lock access to system resources. Ransomware hence can bypass and subvert all the malware detection solutions at the target such as Firewall and IDS. This behavioural feature is also exhibited by other malware such as rootkit and keyloggers however ransomware notifies the victim at the last stage of the attack. Security experts can use the behavioural characteristics of ransomware to build systems that can detect it. Due to the nature of the current ransomware threat landscape, efficient ransomware detection systems have moved from static analysis and basic dynamic malware analysis which uses emulated or fake malware platform to better solutions like [5, 13]. Machine learning approaches are also used in addition to static and dynamic analysis. The downside of the machine learning method is that it may not be able to detect zero-day attack if the algorithm is not adaptive to the changing threat landscape.

Static Analysis

Static analysis does not make use of artificial user environment but rather runs analysis on files as they exist in the storage of the target systems with the aim of extracting the behavioural profile of malware. Static analysis performs poorly on compressed file formats and because they run inside the host (i.e. in-box) they are vulnerable to subversion by the malware. Some methods used for static analysis are n-Gram, byte sequence, OPCODE, Portable Executable headers, and Malware Target Recognition (MaTR) [14].

Dynamic Analysis

Dynamic analysis has been used widely for detecting ransomware. It works by running the actual malware in sandboxed, emulated, virtual or fake environment to monitor and record its behaviour across the five stages of the attack. A problem with this method is fingerprinting, a method used by malware to detect and evade anti-malware such as fake environment or honeypot. UNVEIL [5] is a dynamic analysis method that overcomes the problem of ransomware fingerprinting by using real files, real file attributes and valid path to make the user environment real. Another approach to overcoming the problem of fingerprinting is to carry out dynamic analysis in different user environments. A variant of this comparison approach is [13], having bare-metal reference system with no in-guest components.

Machine Learning

Machine Learning approach makes use of feature vectors obtained from various malware samples during dynamic analysis, static analysis or other feature extraction methods before running these features on a machine learning algorithm for classification. In [15], Sequential pattern mining algorithm is used to find Maximal Sequential Patterns (MSP) of Locky, Cerber and Tesla Crypt ransomware samples using their activity logs and then fed into a machine learning algorithm for classification. A combination of dynamic analysis and machine learning can also be used as in [16]; EldeRan which uses a sandboxed environment to first extract important ransomware features to be finally run with machine learning algorithm for classification.

5. Recovery from Ransomware

Recovery solution comes after a ransomware attack has occurred. Its main goal is to recover any type of data infected by the ransomware by means of other methods but not paying the ransom demanded. While recovering from locker ransomware is possible through rebooting and other means, recovery from crypto-ransomware is challenging [16]. Various recovery methods have been proposed in the past such as by simply renaming the vssadmin.exe to make it inaccessibleto the ransomware and escape infection [2]. Also, access control in one direction and multiple backup preservationshave been used in [17], implemented on a secure backup system using a highly restricted docker container. We introduce another recovery solution based on object-based storage in the next section. Some advantages of this recovery method are suitability for cloud storage and erasure coding.

6. Object-Based Storage Solution for Recovering from Ransomware Infection

Object-BasedStorage (OBS) uses cryptography (security), object versioning (redundancy) and erasure coding or replication (fault-tolerance/redundancy)to provide a backup solution that can guarantee safe recovery of data after a ransomware attack. Figure 2 is an object storage structure. A data object can be any length and can store data of any type. An object is a combination of data, attributes and metadata. There is a data portion that contains the data. The attributes are user-generated and define the characteristics of an object such as QoS. The metadata are extra information retained by the object storage device for performing management functions [18].

The security process of OBS is shown in figure 3. Before a client gains access to an object storage, a security manager must grant access to the client. The security manager can perform this function by sharing a secret key with the object storage device and authenticating the client using protocols like LDAP, NIS or Kerberos [19] and creating client's capability. The shared secret key is used to hash the elements contained in the capability to generate a capability key. The policy manager instructs the security manager to generate a credential when the authorization check is successful. The credential contains the capability key and the requested capability and is passed from the security manager to the client. The client on receiving the credential issues a command containing the request and the capability and an integrity check. The object storage validates the client's digest by creating a digest of the request using the shared secret key and comparing it with the digest received from the client.

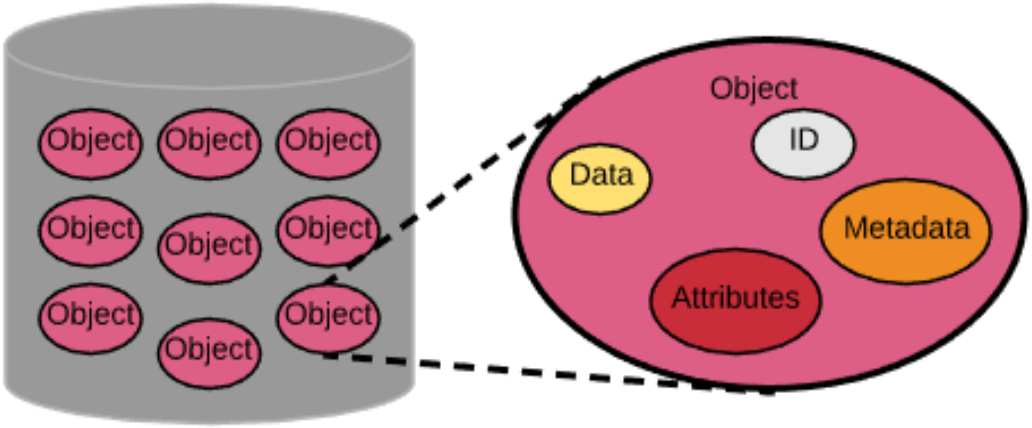

Figure 2: Object storage structure [19].

The object versioning feature of the Object Storage device ensures that once an object is written, it becomes immutable. Updates to the objects are saved as new versions while the previous versions are preserved. Therefore, when ransomware encrypts data, the object storage sees it as new version whereas the original file is not affected [20]. Hence recovery from ransomware is possible from rolling back infected files to their previous versions.

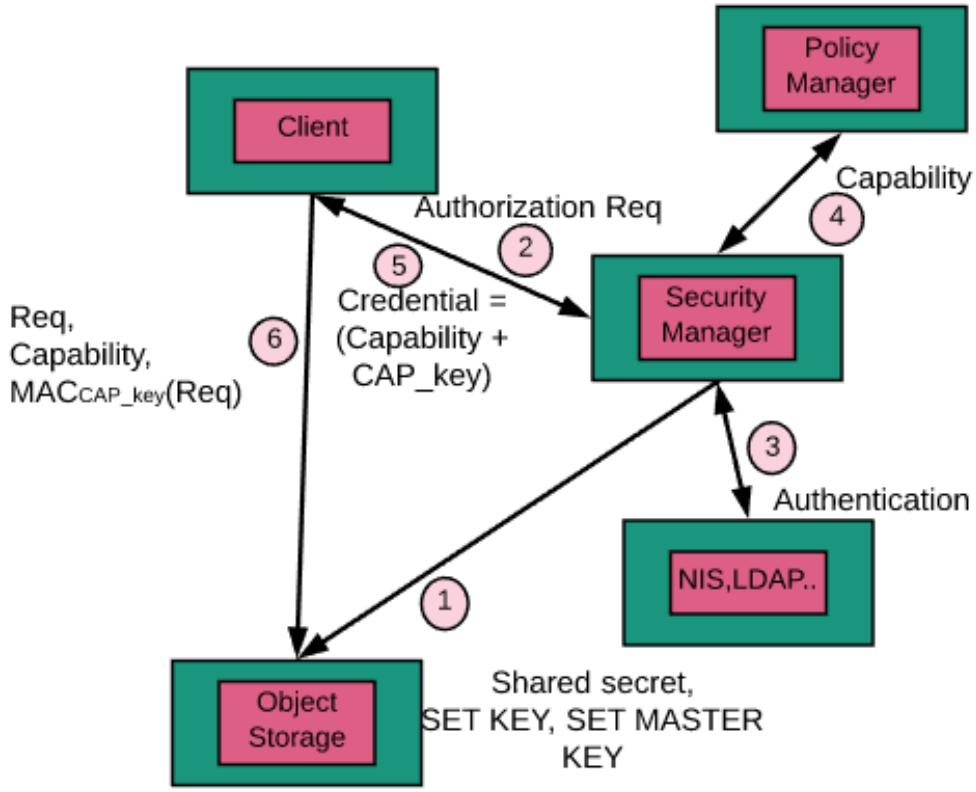

Figure 3: Security process of OBS [19].

Erasure coding can be used to enhance the reliability of object-based storage systems [21]. They offer data protection to object-based storage systems. Object storage support is suitable for large unstructured data in the cloud [21]. Erasure coding works by fragmenting data and encoding these fragments to be stored in a separate location. You can, therefore, get the original data back from a combination of the fragment. Using simple equation, erasure coding can be represented as z = y + x, where y is the original data, x is the redundant data fragments that provide protection from failure, and z is the total number of fragments reconstructed after the erasure. An alternative to erasure coding is replication however replication is suitable for data protection where less CPU power and speed are required such as for smaller datasets.

7. Future Direction

Object-based storage has been in use for cloud storage by Google, Amazon and Microsoft [21] as well as erasure coding and replication for data protection, so these technologies are not new. We have explained how these technologies can be applied to recover from ransomware. The next direction will be to demonstrate how this would work using appropriate tools and data.

8. Conclusion

In this paper, we carried out a study of ransomware with focus on mitigation. Breakthroughs have been made in the past for detecting and preventing ransomware attack but new variants with sophisticated attack process that defeats these efforts are in the wild today. The changing ransomware threat landscape must be understood to guide present and future research effort in the field of security. It is from the behavioural profile of ransomware that we design analysis system such as dynamic and static analysis systems that can extract the behavioural

features of ransomware. In turn, the behavioural characteristics of ransomware are learned through studying the whole attack continuum of ransomware. In this paper, we have done just that. We studied that ransomware attack mechanism and vectors of attack and reviewed various analysis method used for detecting ransomware. We also reviewed other solutions that use a machine learning approach. We introduced a backup solution for a ransomware attack using object-based storage with erasure coding or replication. The proposed solution can be applied to a wide range of use cases, most importantly those involving huge emission-critical data.

References

[1]. C. Brunau, "Common types of Ransomware," https://www.datto.com/blog/common-types-of-ransomware

[2]. M. Wecksten et al, " Novel Method for Recovery from Crypto Ransomware Infection," *Proceedings of the 2nd International Conference on Computer and Communication*, 2016, pp. 1354-1358

[3]. N Scaife et al., "CrytoLock (and Drop It): Stopping Ransomware Attack on User Data," *Proceedings of the 36thInternation Conference on Distributed Computing Systems*, 2016, pp.303-312

[4]. Nick Ismail, "The ransomware business model" https://www.information-age.com/ransomware-business-model-123465658/

[5]. E. Kirda, "UNVEIL: A Large-Scale, Automated Approach to Detecting Ransomware," *Proceedings of the 24thInternation Conference on Software Analysis, Evolution and Reengineering (SANER)*, 2017, pp. 1-1.

[6]. R. Hummel, "*Securing Against the Most Common Vectors of Cyber Attacks*," https://www.sans.org/reading-room/whitepapers/riskmanagement/securing-common-vectors-cyber-attacks-37995

[7]. M Hasan and M. Rahman, "RansHunt: A support vector machines-based ransomware analysis framework with integrated feature set," *Proceedings of the 20th International Conference of Computer and Information Technology*, 2017 pp. 1-7

[8]. A Bhardwaj et al., "Ransomware Digital Extortion: A Rising New Age Threat," *Indian Journal of Science and Technology*, 2016, vol. 9 (14), pp. 1-5.

[9]. A. Zahra and M. Shaf , "IoT Based Ransomware Growth Rate Evaluation and Detection using Command and Control Blacklisting," *Proceedings of the 23rd International Conference on Automation and Computing*, 2017, pp. 1-6.

[10]. A. Zimba, Z. Wang and H. Chen, "Reasoning crypto ransomware infection vectors with Bayesian networks," *Proceedings of the IEEE International Conference on Intelligence and Security Informatics (ISI)*, Beijing, 2017, pp. 149-151.

[11]. N. Kshetri and J. Voas, "Do Crypto-Currencies Fuel Ransomware?," *IT Professional*, vol. 19, no. 5, 2017, pp.11-15.

[12]. G. HurlBurt and I. Bojanova, "Bitcoin: Benefit or Curse," *IEEE IT Professional*, 2014, vol. 16, no. 3, pp. 10-15

[13]. D. Kirat, G. Vigna, and C. Kruegel, "BareCloud: Bare-metal Analysis-based Evasive Malware Detection," *Proceedings of the 23rd USENIX Security Symposium*, 2014, pp. 287-301.

[14]. HV Nath and BM Mehtre, "Static malware analysis using machine learning methods" *Proceedings of the International Conference on Security in Computer Networks and Distributed Systems*, 2014, pp. 440-450.

[15]. S. Homayoun, A. Dehghantanha, M. Ahmadzadeh, S. Hashemi and R. Khayami, "Know Abnormal, Find Evil: Frequent Pattern Mining for Ransomware Threat Hunting and Intelligence," *IEEE Transactions on Emerging Topics in Computing*, 2017, pp. 1-11

[16]. D. Sgandurra et al, "Automated dynamic analysis of ransomware: Benefits, limitations and use for detection," *arXiv preprint arXiv:1609.03020 (preprint)*, 2016, pp.1-12

[17]. Y. Jin, M. Tomoishi, S. Matsuura and Y. Kitaguchi, "A Secure Container-based Backup Mechanism to Survive Destructive Ransomware Attacks," *Proceeding of the IEEE International Conference on Computing, Networking and Communications (ICNC)*, Maui, HI, 2018, pp. 1-6.

[18]. M. Mesnier, GR. Ganger and E. Riedel, "Object-based Storage," *IEEE Communications Magazine*, 2003, vol.41, no. 5, pp. 84-90
[19]. C. Bandulet, " Object-Based Storage Devices," http://www.oracle.com/technetwork/server-storage/solaris/osd-142183.html
[20]. E. Ottem, "Object Storage and Ransomware – How to Better Protect Your Business,"https://blog.westerndigital.com/object-storage-ransomware-better-protect-business/
[21]. S. Samundiswary and N. M. Dongre, "Object storage architecture in cloud for unstructured data," *Proceedings of the International Conference on Inventive Systems and Control*, 2017, pp. 1-6

Authors

Kelechi G. Eze (keze@student.pvamu.edu) is a doctoral student at Prairie View A&M University, Texas. He is a student member of IEEE. His research interests include Internet of things security, data security and privacy, blockchain technology, wireless sensor networks, and machine learning.

Cajetan M. Akujuobi (cmakujuobi@pvamu.edu) is the vice-president for Research, Innovation and Sponsored Programs at Prairie View A&M University, Texas. He is the author of two books and several papers.

Matthew N.O. Sadiku (sadiku@iee.org) is a professor at Prairie View A&M University, Texas. He is the author of several books and papers. He is an IEEE fellow. His research interests include computational electromagnetics and computer networks.

Pankaj Chhetri (pachhetri@pvamu.edu) is an IT Professional and a doctoral student at Prairie View A&M University, Texas. He is a student member of IEEE. His research interests include: Cloud and IoT Security, Access Control Models on IoT devices and IT Management and security