IJARSCT

ISSN (Online) 2581-9429

International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)

International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal

IJARSCT

Impact Factor: 7.53

Volume 4, Issue 1, May 2024

Ransomware Readiness Assessment Tool

Dr. Nandini S[1], D P Sai Manohar[2], Darshan D[3], G Shivarame Gowda[4], Nisarga S[5]

Associate Professor, Department of Information Science and Engineering[1]

Under Graduate Student, Department of Information Science and Engineering[2,3,4,5]

S J C Institute of Technology, Chikkaballapur, India

Abstract*: Ransomware attacks have been increasingly concerning in times. The situation is only getting worse. They have shed light on a category of software that demands a ransom, for releasing a hostage asset. The majority of ransomware strains rely on encrypting data. Essentially, they lock up files on the victims' devices and network drives before demanding payment to decrypt them. In this study, we first introduce a classification system for ransomware. Then drawing from this taxonomy and identifying a present in highly resilient ransomware during the key exchange process we propose an innovative method for detecting and thwarting these resilient strains to prevent them from encrypting victims' data. Through testing our model shows promising results, in identifying variations of dangerous ransomware strains.*

Keywords: ransomware, crypto virology, prevention; high survivable ransomware

I. INTRODUCTION

Cybercriminals and malware writers have diversified their efforts to make money from their victims, using methods that have been well-established on desktops, laptops, tablets and mobile devices, this includes ransomware. "Ransomware is the name of a so-called phenomenon. It has been built upon the two words ransom and malware" [1]. To define this word, one may give the following general definition: " ransomware is a type of malware which restricts access to the computer system that it infects, and demands a ransom paid to the creator(s) of the malware in order for the restriction to be removed". Some forms of ransomware encrypt files on the system's hard drive (crypto viral extortion, a threat originally envisioned by Adam Young and Moti Yung [2]), while some may simply lock the system and display messages intended to force the user into payment.

Anandrao said in [3] that "It does not appear that a properly designed crypto viral extortion attack has ever been carried out to date immensely." Also Gazet said in [1] that "No ransomware has reached a sufficient complexity level to successfully become a perfect extortion mean. None of the ransomwares we have studied, presents a reliable perfect extortion scheme. An explanation of this may be that ransomwares' writers have a limited knowledge of cryptography." These statements were valid before 2013. But the Crypto Locker ransomware in 2013 showed that the situation has changed and malware developers have increased their cryptology knowledge.

In June 2013, McAfee released data showing that it had collected over 250,000 unique samples of ransomware in the first quarter of 2013, more than double the number it had obtained in the first quarter of 2012[4]. Crypto Locker surfaced in late-2013, had procured an estimated US$3 million before it was taken down [5]. Based on Bitcoin transaction information ZDNet estimated that the operators of Crypto Locker had procured about US$27 million from infected users [6].

In this paper, we present a novel approach for the most dangerous ransomwares to detect their malicious activity and abort their encryption process before it starts. In summary, wemake the following contributions:

- In the beginning we introduce a classification system for ransomware in section 2 drawing from our research, on attacks and various ransomware types. Our taxonomy aims to encompass all known variants of ransomware
- Moving on to section 3 we outline a method for identifying HSRs that utilize domain generation algorithms (DGA).
- Concluding our discussion we propose a strategy named "Connection Monitor & Connection Breaker" (CM&CB) for combating the potent form of ransomware HSR. Our experimental findings from a proof-of-concept implementation validate the effectiveness of this approach, in mitigating the threat posed by the ransomware strains.

DOI: 10.48175/IJARSCT-18062

II. PROPOSED RANSOMWARE TAXONOMY

In this section we describe our proposed comprehensive taxonomy.

A. Non-Cryptographic Ransomware (NCR)

There are ransomware payloads that don't encrypt. Generally, the payload in these scenarios is only an application that locks the screen or even modifies the partition table and/or master boot record to limit user interaction with the system. This kind of ransomware's weak techniques allow for the restoration of its damages without having to pay the ransom.

B. Cryptographic Ransomware (CGR)

Cryptographic Ransomware (CGR) ensnares precious assets and demands a ransom in exchange for its release via cryptographic techniques. In this context, a common occurrence is that the malware may begin covertly encrypting user data (documents, photos, and so forth). The target user is notified that all of his or her data has been encrypted and that the only way to get it decrypted is to pay the ransom. The cryptosystems that these ransomwares employ allow us to subdivide them into three categories.

III. CONNECTION-MONITOR & CONNECTION-BREAKER APPROACH

It is evident from outlining the taxonomy of ransomware that hybrid cryptosystem ransomwares, or HCRs, pose the greatest threat. In this work, we present CM&CB, a novel framework designed to identify the most perilous varieties of ransomware and stop them from encrypting the files belonging to the affected party. This section outlines our suggested framework after defining the targeted ransomware kinds.

A. High survivable ransomwares (HSR)

The following outlines the conditions that must be met for a mass extortion method to be effective:

- The ransomware should be regarded as compromised and dangerous since it affects consumers' computers.
- The only person who should be able to remove the infection is the ransomware writer. For malware to be able to demand a ransom, it must have a trustworthy way to extract money. A victim will not pay the ransom if she is able to remove the illness on her own [1]. The decryption key should never be kept on the victim's computer for a flawless extortion, as skilled users or virus analyst possessing basic reverse engineering abilities can easily restore the system to a pristine state.

Based on [2] and the three characteristics of perfect extortion, survival is a problem shared by all ransomwares. A ransomware with a "high survivability property" is defined as follows.

Definition 1: A ransomware is considered to have "high survivability" if it is able to keep control over a critical host resource (RC), allowing access only when necessary. If the ransomware is altered or removed, RC becomes permanently inaccessible, and the only way to decrypt data is to use the Command & Control server (C&C) key while the ransom is being paid.

The HCR subtype comprises the highly survivable ransomwares that have been identified in malware databases during the past ten years. In this study, we present a methodology for detection and prevention of high survivable ransomware (HSR). Furthermore, our system is able to identify any ransomware that operates through a key exchange process.

B. Overview of CM&CB approach

Adleman's research has demonstrated that virus identification is an unsolvable issue, and the efficacy of protection systems based on virus detection is doubtful [11]. Young and Yung have demonstrated that, in the event that asymmetric cryptography is robust, reversing the impact of an HCR on the host system may be an unsolvable computing challenge [2]. Our suggested structure can identify every HSR that is now in use (that has been made public so far) prior to the encryption process beginning, hence totally blocking the operation. To understand this feature we review the HCR attack process in more detail.

Step 1 (Find a Victim): The HCR is initially spread through mail spam and other means. For instance, the CryptoLocker is usually distributed by emails sent to business email accounts posing as FedEx, UPS, or DHS customer support-related queries. When the zip attachment in these emails is opened, the PC becomes infected.

Step 2 (doing): In this phase, social engineering techniques are used to have an unsuspecting user carry out the HCR.For instance, the executables included in the CryptoLocker zip files are essentially PDF files masquerading as executables; they often have the extension FORM_101513.pdf.exe and a PDF icon. Because Microsoft does not display extensions by default, when users open them, they appear to be regular PDF files. In some sophisticated HCR like Cryptolocker in thisstep the HCR tries to delete the victim's volume shadow copies,so the restoration will be disabled.

Step 3 (public key exchange): As per our explanation in PuCR, ransomware authors have numerous restrictions when it comes to integrating pair keys into their malware. Consequently, the HCR will endeavour to locate a live C&C or the user's public directory in order to obtain the unique public key Kpu. For instance, Cryptolocker connects to domains produced by a DGA in an effort to locate a live C&C. The DGA will produce domain names such as jkaeaxjmnxvpv.ru and kjqwymybbdrew.biz. It will communicate with a real C&C server once it is found, obtaining a public encryption key that will be used to encrypt data files.

Step 4 (Encryption): Following the acquisition of the infection-specific public key, the victim's data will first be encrypted with Ks and then chained using CBC as the chaining mechanism. After then, the real data can be replaced or erased. Similar to (1), the symmetric key is attached to The Initialization Vector, and the public key of the virus writer is used to encrypt it.

$$M' = E_{Kpu}(\{IV, Ks\}) \qquad (1)$$

Step 5 (Display message): The victim's screen displays the M' and the anonymous ways to get in touch with the HCR writer after infection.

Step 6(Decryption): Deciphering The victim shall send M' to the HCR writer if he consents under the condition that the ransom be paid. After that, HCR writer delivers the pair back to the victim after decrypting it with the matching private key Kpr. In certain instances, the HCR writer use an executable programme for decryption rather than transmitting the {IV, Ks}.

Our first version of the framework was created based on an idea connected to the public key exchange stage in the protocol mentioned above, after we analysed over 40 ransomwares in the recent past, took into account the state of anti-malware technologies, and looked towards the future of malware and anti-malware technologies. Because embedding a static list of C&C candidates into ransomwares presents challenges for cybercriminals should the malicious code finally be captured and examined by security vendors and analysts, the majority of sophisticated and evasive ransomwares at this moment use DGA. Most contemporary ransomware has moved away from hard-coded lists and is built to use DGAs in order to get around this weakness. We created a connection monitor in our initial architecture that could identify DNS domain requests made by DGAs

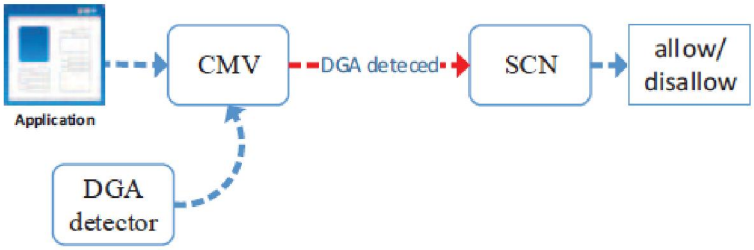

Figure 1: Architecture of DGA detector framework.

DOI: 10.48175/IJARSCT-18062

As demonstrated in Fig. 1, the connection monitor verifier (CMV) uses DGA detector to identify suspicious connections when ransomware attempts to establish a connection to its C&C via DGA. Another crucial aspect of DGA malicious requests is the speed at which these algorithms originate and request connections from numerous sites. The user can then break the connection and report this suspicious connection address to specialists when the suspicious connection notifier (SCN) alerts them to a strange connection. In addition to all the advantages, the DGA detector structure requires great precision in order to reduce false positives. However, certain domains are not nonsense; occasionally, they are written in a different language. As a result, additional work is required for this framework to truly be accepted.

Since the majority of ransomware targets the Microsoft Windows operating system, we have incorporated a connection-monitor in this framework that checks all applications, particularly the new or untrusted executable files in Windows (Fig. 2). To put it simply, a connection monitor approach looks through all of the executables' outgoing communication and prompts the user to accept or reject the connection. We created an enhanced code signing certificate for our advanced mode of operation. In addition to the standard code signing for integrity checks, we advise developers to submit their certificate authority (CA) the connection addresses needed for their applications. Following a quick address check, the CA will confirm that the list has the verified necessary connection addresses (VRCA).

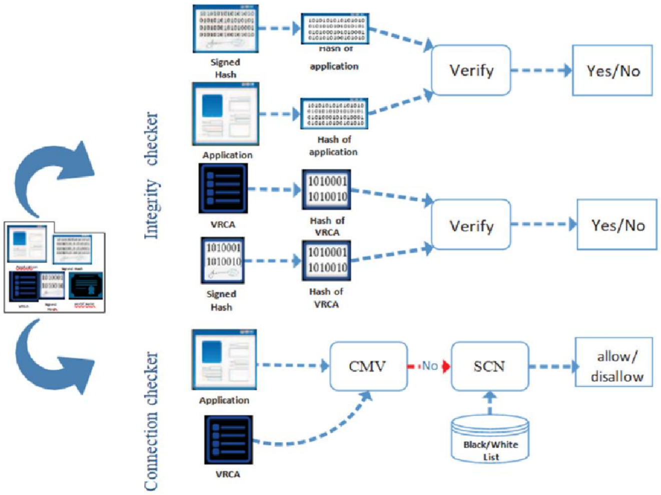

Figure 2: Architecture of proposed framework

A malware analyst can always find the contents of the main HCR body by simply decrypting it using the stored keys. This process will be interrupted if the HCR initially begins encrypting data and then tries to exchange the Kpu with connection breaking. The IV and Ks will be reminded within every instance of the HCR.

IV. EVALUATION

Here, we report the experimental findings and talk about our experiences with this new strategy. Specifically, we evaluate the efficacy of the suggested methodology in identifying and impeding HCRs from using hybrid cryptosystems to encrypt user data. Some ransomware detectors, such BitDefender AntiCryptoWall, Hitman Pro Kickstart, and HitmanPro CryptoGuard, are signature-based and unable to identify newly discovered or unidentified ransomwares. We were unable to compare the results of our framework's detection with those of other tools or frameworks since there is currently no ransomware detector that can identify novel or unidentified ransomwares. We test our concept with over 20 new typical ransomware samples to show that our method is capable of recognising HSRs. With the help of this framework, it was possible to identify every HSR and prevent its encryption before the public key exchange was finished. With regard to HSR detection, the suggested method has a 100% detection rate and 0% false negatives. Table 1 gives an overview of various tests. These examples were chosen because they are extremely complex and widely used (from BleepingComputer.com and malwaretips.com). Table 1 defines detection as defeating the encryption.

Table 1. PROPOSED FRAMEWORK EXPERIMENTAL RESULTS

Ransomware Name	Ransomware Type				**HSR**	**Detection**
	HCR	***PuCR***	***PrCR***	***NCR***		
Cryptolocker	**1**	×	×	×	**1**	**1**
Cryptolocker 2	**1**	×	×	×	**1**	**1**
Cryptolocker 3	**1**	×	×	×	**1**	**1**
Cryptowall	**1**	×	×	×	×	**1**
Cryptowall 2	**1**	×	×	×	**1**	**1**
Cryptowall 3	**1**	×	×	×	**1**	**1**
CoinVault	**1**	×	×	×	**1**	**1**
CryptoGraphic Locker	**1**	×	×	×	×	**1**
CryptoDefense	**1**	×	×	×	×	×
CryptoDefense 2	**1**	×	×	×	**1**	**1**
CryptorBit	×	×	**1**	×	×	×
TorrentLocker (original)	×	×	**1**	×	×	×
TorrentLocker	**1**	×	×	×	**1**	**1**
ACCDFISA	×	×	**1**	×	×	×
BuyUnlockCode	**1**	×	×	×	×	×
CryptoFortress	**1**	×	×	×	×	×
PClock2	×	×	**1**	×	×	×
Critroni(CTB Locker)	**1**	×	×	×	×	×
Computer Crime & Intellectual Property Section	×	×	×	**1**	×	×
Harasom	×	×	**1**	×	×	×

V. CONCLUSION

We discussed a number of methods in this research to mitigate the threat posed by malicious ransomware. To identify and stop harm caused by the most deadly ransomware, new monitoring approaches dubbed CM&CB and a DGA-detector are suggested. The crucial realisation that this strategy needs to succeed is that a key-exchange stage is necessary for HSR operation. The entire HSR process is impeded by monitoring and obstructing this phase. The following succinctly describes the primary benefits of the suggested concept. Initially, this framework is the first of its kind created specifically to address the problem of ransomwares. It does this by keeping an eye on questionable connections and stopping them before they can encrypt the data of the victim. The results of the experimental assessments demonstrate that the suggested framework can effectively block the most potent HSRs, which was previously an unresolved issue in the malware mitigation community. More study is now being conducted on creating a more thorough review. Furthermore, botnets, drive-by download malware, malware that mines bitcoin, and other malicious software can all be detected with the use of this framework. The concept of granting this type of enhanced certificate is not unique to HSRs, hence it can be a helpful defence system against numerous more dangers. Our long-term goal is to expand this framework by incorporating an additional 17 HSR traits in order to identify novel and unidentified advanced HSRs.

REFERENCES

[1] Gazet, Alexandre. "Comparative analysis of various ransomware virii." Journal in computer virology 6.1 (2010): 77-90.

[2] Young, Adam, and Moti Yung. "Cryptovirology: Extortion-based security threats and countermeasures." Security and Privacy, 1996. Proceedings., 1996 IEEE Symposium on. IEEE, 1996.

[3] Shivale, Saurabh Anandrao. "Cryptovirology: Virus Approach." arXiv preprint arXiv:1108.2482 (2011).

[4] "Update: McAfee: Cyber criminals using Android malware and ransomware the most". InfoWorld. Retrieved 16 September 2013.

[5] "Cryptolocker victims to get files back for free". BBC News. 6 August 2014. Retrieved 18 August 2014.

[6] Violet Blue (December 22, 2013). "CryptoLocker's crimewave: A trail of millions in laundered Bitcoin". ZDNet. Retrieved 2013-12-23.

[7] McAfee Threats Report: February 2015, By McAfee Labs,Page 38,2015.

[8] McAfee Threats Report: Third Quarter 2013, By McAfee Labs,Page 19,2013.

[9] McAfee Threats Report: Second Quarter 2014, By McAfee Labs,Page 21 ,2014

[10] Young, Adam, and Moti Yung. Malicious cryptography: Exposing cryptovirology. John Wiley & Sons, 2004.

[11] Adleman, Leonard M. "An abstract theory of computer viruses." Proceedings on Advances in cryptology. Springer-Verlag New York, Inc., 1990

[12] Abidin, Shafiqul, Rajeev Kumar, and Varun Tiwari. "A Review Report on Cryptovirology and Cryptography." International Journal of Scientific & Engineering Research 3.11 (2012): 1.

[13] Stone-Gross, Brett, et al. "Your botnet is my botnet: analysis of a botnet takeover." Proceedings of the 16th ACM conference on Computer and communications security. ACM, 2009.

[14] Yadav, S., Ashwath K. K. R., and Supranamaya R. . "Detecting algorithmically generated domain-flux attacks with DNS traffic analysis." Networking, IEEE/ACM Transactions on 20.5 (2012): 1663- 1677

DOI: 10.48175/IJARSCT-18062