Malik et al LGURJCSIT 2019

LGU (IJECI)
ISSN: 2522-3429 (Print)
ISSN: 2616-6003 (Online)

LGU International Journal for
Electronic Crime Investigation

Research Article

Vol. 3 Issue 2, April - June 2019

Ransomware Detection and Defense

Muhammad Shairoze Malik
Lahore Garrison University, Lahore.
shairozemalik@lgu.edu.pk

Abstract:
Like other criminals in world, cyber-criminals are using different illegal and unethical ways to gain their mischievous purposes. Malware known as Ransomware is a new threat to world used by cyber hackers to blackmail individuals and organizations and has been identified as a major threat to network and computer security across the world [1]. Ransomware lock victim's computer by encrypting user files and demands payment often in crypto currency i.e. Bitcoins to give access to files. Research showed that 19,750 victims paid over $16 million as ransom payment in two years [2]. Due to increasing amount of ransomware attacks, different software and hardware level techniques are proposed to detect and mitigate ransomware attacks and to recover user files without ransom payment. Pay Break is a proactive defense mechanism on software level against ransomware that allow victim to recover files without any ransom payment. Furthermore, ransomware variants could get kernel privilege, that let them to shutdown software-based system defense. Considering this, first hardware level defense system is proposed named Flash Guard which is resistant against ransomware that use kernel vulnerabilities.

Keywords: Security, Privacy, Ransomware, Ransomware Detection, Cyber-Defense, Malware, Pay Break, Flash Guard

1. Introduction

Cyber-criminals are using new approaches to make money illegally. Malware known as Ransomware is a new threat to world used by cyber hackers to blackmail individuals and organizations and has been identified as a major threat to network and computer security across the world [1]. Ransomware is a modern approach adopted by cyber hackers to enhance their profit. Ransomware is the most visible growing threat to all users. It comes in different forms and shapes. It holds user files "hostage" until it is paid by victim. Ransomware variants were introduced in late 1980s but modern age of ransomware started in 2013 with Crypto Locker. Ransomware is a malware that attacks user machine by using system vulnerabilities and available methods. It silently encrypts user documents and media and then demands for ransom payment to recover data. Young and Yung were the first to give the idea of file encrypting ransomware in 1996. Their explanation is a perfect picture of current most successful crypto based ransomware families that use encryption to threaten users into paying ransom. Attackers are now more sophisticated and business minded. In start, initial victims were individual systems (regular people) but now they target business sector as ransomware attacks are successful against businesses and they can get more profit from them by halting their productivity. This situation is very torturing for both individuals and businesses. Some of the dangerous forms of ransomware include Crypto locker, Crypto wall, CTB Locker, Tesla Crypt or WanaCry. Digital extortion has increased significantly in last couple of years as the number of online application and smart devices continue to grow [2]. The impact of ransomware is so huge that it is now rated as the biggest cyber threat that hit the market [3].

These attacks are shifting focus to organizations. For example, the Hollywood Presbyterian

Medical Centre in the United States was attacked in February 2016. They were hit by Crypto Ransomware and were forced to shut down. The ransomware encrypted the files, denying hospital access to health records [4].

According to FBI (Federal Bureau of Investigation), due to ransomware attacks estimated losses of about $1 billion US Dollars was incurred in the year 2016. Out the people affected by the attack, nearly 40% of victims paid the ransom. Unfortunately, current preventive methods are not adequate enough to handle the effects of such attacks [7] [10].

Ransomware payloads and malicious binary codes use techniques that make it difficult to detect or analyze. In response to ransomware attacks, it is important to develop tools or techniques that can extract ransomware behavior and improve detection systems. Malwares use almost common evasion methods to evade known detection techniques to attack end user. Techniques to detect, analyze and mitigate ransomware attacks are not different from other methods of identifying malicious attacks. Ransomware use similar approach like other attacks for example opening email attachment or clicking on advertisement can be the cause of attack on user side. Security research groups are working to investigate what particular problems in exposing ransomware attack are similar to other malicious attacks and which are independent in characteristics and need more attention [5]. Several detection and defense systems have been proposed by researchers that use cryptographic algorithms and file access features or patterns to identify and mitigate ransomware attacks.

2. Background:

WanaCry hit thousands of users. Many public and private sectors become victim of this ransom attack. This attack utilize kernel vulnerability, encrypts user data and asked for bitcoin payment to unlock files. So concerned increased after large number of high profile ransomware attacks that how to fight against them [5].

PC Cyborg was first ransomware variant reported in 1989. The encryption algorithm used was symmetric cryptography and was easily decrypted [11]. Another ransomware GpCode also employed custom symmetric encryption, first discovered in 2005, and improved over time to become more and more sophisticated [12-13]. Reveton, also known as Police Ransomware, spread through pornographic websites, it changes extensions in win/system32 folder and display notification pages to victims [14][15].

Ransomware authors usually choose between symmetric and asymmetric cryptography. Old ransom versions were based on symmetric encryption, which were quickly reversed by malware engineering and provided decryption instruments. So ransomware attacks were defeated because of their weak cryptology. Malware authors decided to ignore the popular adage “don't roll your own crypto” [8]. Malware authors learned from their past mistakes and started implementing strong hybrid crypto algorithms in their attacks. Besides this, some modern forms of ransomware use kernel privileges for attack. To deal with ransomware attacks and to achieve data recovery capability, it is important to study the behavior of ransomware and its interaction with user data. Research showed that malware locks user data speedily and size of encrypted data is comparatively small. They try to remove any means through which victims could recover from the attack without paying [9]. Proactive detection and defense mechanism is required and for this security research community proposed different tools and techniques like UNVEIL uses the kernel as the module to search for file system activities. CryptoHunt identifies malicious binary code cryptographic functions when attacks use custom cryptographic functions [5]. CryptoDrop detects ransom through the inspection of programs, their activities and user data changes. Redemption implements abstract model that contains behavior or characterization of a large dataset of ransomware attacks to identify malicious process [5]. Pay Break is a new mechanism of protection. It stores cryptographic encryption-keys securely in the key vault and allow victims to recover their ransomed files without paying [8]. Flash Guard, a SSD (Solid-State Drive) has a firmware-level recovery system through which fast, efficient recovery from ransomware encryption can be done without relying on backups [9]. In this paper we will focus on detection and defense techniques particularly Pay Break and Flash Guard.

3. Detection and Defense Techniques:

During the year of 2016 just, a large scale of crypto-ransomware attack occurred on north

American universities, which impacted the university computers & services. Systems were taken offline, as university did not pay the ransom of amount $38000 to release the encrypted file. Recovery took many days to normal the services. Ransomware focuses on controlling system resource's, encrypting data files and holding the decryption keys to demand the ransom. Malware is first distributed to victim`s machine. Once its executed, it encrypts files and notify user by altering that contents are encrypted and they will be lost unless they pay ransom. Ransom note either have unique ransom address or a link on that note for payments to be done against ransomware. They choice Bit coin as their payment method as its decentralized and unregulated. Ransom also includes how to purchase bitcoins and from which exchange [9]. Researchers tracked ransomware end to end by combining multiple data-sources including ransomware binary, victim telemetry, seed ransom payments, and bit coin addresses. Over $16 million US Dollar ransom payments made by 19,750 victims in span of 2 years [9]. Ransomware usually target those users who do not follow good practices [6]. In this response, users are instructed to backups their important data [9]. Back up is reliable defense against ransomware but back up devices had only those data which had last time backup, so this can be prevented by educating people, by proper communication and by upgrading to new technologies in terms of software and Hardware upgrade. To fight against ransomware, it is important to develop methods that can increase evasion costs, upgrade malware detection systems, and help malware analysts to unmask the internal functioning of malicious code [5].

3.1 Enhancing Detection / Monitoring Techniques:

Dynamic analysis technique is good in analyzing malicious binary code and extracting behaviors or functionalities of malware sample [5]. Bare-metal automated analysis known as Bare Cloud technique is proposed by Kirat and colleagues. It doesn't have any in-guest monitoring component which makes this solution more robust against current bypass techniques [5]. Bare-Cloud extracts the behavioral profile of the malware from its network level and disk level activity. The disk level activity is obtained by comparing the system's state after each execution of malware with the initial clean state. With the understanding of the OS of the analysis host, Bare-Cloud also obtain operating-system-level changes, such as changes to system files and registry keys. Network-level activities are captured as a stream of network packets. For valid monitoring, it is important to know how malware author use cryptosystems, how encryption keys are generated and how attack make user data unreachable. UNVEIL technique use kernel as module to look for system activities [16]. It monitors user processes that have interaction with file system. File monitoring system in UNVEIL gives full view of all file system modifications as it has access to buffers that deals with I/O calls [5]. Another technique named CryptoHunt is introduced by Xu and colleagues. It identifies cryptographic functions in malicious binary code as attacks use customized cryptography functions to bypass detection instead of known crypto functions. Research showed that customized crypto functions are not coded well so recovering encrypted data is easy [5].

3.2. End-Point Protection Systems:

End point solutions are proposed to monitor operating system resource usage to stop attacks once data starts encrypted by ransomware.

Software Level Support

CryptoDrop is an early warning system for ransomware attack [17]. It detects ransomware by inspection of programs, activities and changes to user data. It alerts user and suspends suspicious process. 3 primary (File Types Changes, Similarity Measurement and Shannon Entropy) and 2 secondary indicators (Deletion and File type Funneling) are identified to create strong detector to mitigate ransomware. Hence parameters are set in system for quick detection with low false-positives. This way ransomware can be prevented from completely encrypting a victim`s files and mitigates the amount of victim data loss.

3.3. Pay Break

It is protection tool against hybrid crypto ransomware attacks. In hybrid crypto system, attacker use symmetric key to encrypt each file. This symmetric key is termed as Session Key. The session key is then encrypted with public key of attacker and saved it together with encrypted file contents. So in this case attacker is generating a symmetric key pair on his command and controlling whole game [8]. Malware authors use cryptography into their malware codes by dynamically linking against system provided crypto libraries or statically linking libraries that are embedded into executable application code. It is observed that two famous ransomware families CryptoWall and CryptoLocker are using the same APIs that windows are using for cryptographic functionality and is guaranteed to be present on every windows installation. Practically encryption is doneon the victim`s machine in ransom attack. This characteristic of attack helps in designing Pay Break to fight against modern ransomware. Pay Break consists of three components (Hooking, Key Vault and File recovery) that together make cohesive system to recover encrypted files [8]

4. Hooking Crypto Function:

Pay Break support both linking libraries. It looks for procedures in dynamically linked libraries by their name and address and statically linked procedures by Fuzzy Byte Signature. Pay Break use hooking scheme that helps to export session keys, algorithms and its parameters used for symmetric encryption [8].

Dynamically Linked Libraries Hooking.

In Microsoft, encryption through Crypto API is performed by using Crypt Encrypt Function. Ransomware based on CrytoAPI uses Crypt Encrypt function to do encryption of files. Hooking is done in Crypt Encrypt function to securely export the keys. Moreover, pay break hooks the CryptAcquireContext and CryptSetKeyParam functions to know about the algorithm used for encryption and to obtain cipher mode, initialization vector parameters. Base material that is used to generate session keys and which is used by ransomware by linking libraries dynamically or statically is stored by Pay Break via hooking scheme [8].

4.1. Statically Linked Libraries Hooking:

Statically Linked libraries are placed into the executable code of the application. Pay Break use a slightly different approach when ransomware statically links a cryptographic library. Cryptographic procedures are identified and hooked by Pay Break at runtime in process memory. Pay Break rely on signatures to identify statically linked crypto libraries. Pay Break Prototype is compatible with signatures for Crypto++ statically linked library. Pay Break scans memory of all executed processes for function signatures. Hook is placed when signature is identified at its address. Hook then securely exports the Crypto++ session keys and algorithm details [8].

4.2. Key Vault

Key vault stores symmetric session keys and algorithm details with its parameters (i.e. IV and block cipher mode) that are extracted from hook to recover encrypted data. User public key is used to encrypt and export session keys securely to key vault and key vault itself is secured by user`s private key. Public and private keys of user are generated during installation of pay break. Pay Break uses 2040-bit RSA keys for secure encryption of data [8].

4.3. File Recovery

Last component of Pay Break is Recovery of files that are encrypted during ransomware attack. File recovery works in 3 phases.

1. Key vault is decrypted with user`s private key.
2. Data in vault i.e (symmetric keys and their corresponding encryption algorithms with parameters of block cipher mode and IV are analyzed minutely.
3. Finally, victim`s encrypted files are recovered by retrieved session keys.

Each file encrypted with ransomware have meta data such as file length, encryption date, encryption key. Because of this metadata, actual encrypted file data is offset in files held for ransom. Pay Break decrypt file with each possible key and offset until decryption state is reached [8]. See figure below [18]

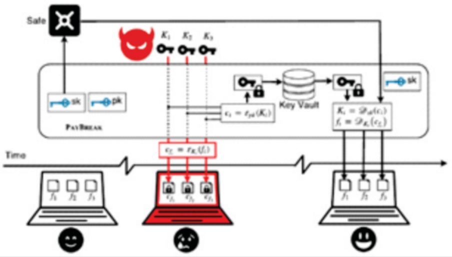
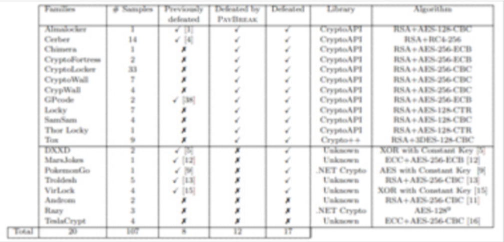


Figure 1: Overview of Pay Break

Research showed that Pay Break defeated 12 of 20 active ransomware families. Files are successfully recovered that are encrypted by CryptoWall and Locky. Locky encrypted 982 files which were recovered in 40s and CryptoWall encrypted 204 files and were recovered in 86s. Pay Break gives the ability to fight against ransomware by using multiple cryptographic libraries including Microsoft Crypto API and Crypto++. To eliminate remaining, respective static / dynamically linked encryption libraries & functions can be hooked with Pay Break [7]. See figure below:



Families	# Samples	Previously defeated	Defeated by PayBreak	Defeated	Library	Algorithm
Almalocker	1	✓ [1]	✓	✓	CryptoAPI	RSA+AES-128-CBC
Cerber	14	✓ [4]	✓	✓	CryptoAPI	RSA+RC4-256
Chimera	1	✗	✓	✓	CryptoAPI	RSA+AES-256-ECB
CryptoFortress	2	✗	✓	✓	CryptoAPI	RSA+AES-256-ECB
CryptoLocker	33	✗	✓	✓	CryptoAPI	RSA+AES-256-CBC
CryptoWall	7	✗	✓	✓	CryptoAPI	RSA+AES-256-CBC
CrypWall	4	✗	✓	✓	CryptoAPI	RSA+AES-256-CBC
GPcode	2	✓ [38]	✓	✓	CryptoAPI	RSA+AES-256-ECB
Locky	7	✗	✓	✓	CryptoAPI	RSA+AES-128-CTR
SamSam	4	✗	✓	✓	CryptoAPI	RSA+AES-128-CBC
Thor Locky	1	✗	✓	✓	CryptoAPI	RSA+AES-128-CTR
Tox	9	✗	✓	✓	Crypto++	RSA+3DES-128-CBC
DXXD	2	✓ [5]	✗	✓	Unknown	XOR with Constant Key [5]
MarsJokes	1	✓ [12]	✗	✓	Unknown	ECC+AES-256-ECB [12]
PokemonGo	1	✓ [9]	✗	✓	.NET Crypto	AES with Constant Key [9]
Troldesh	5	✓ [13]	✗	✓	Unknown	RSA+AES-256-CBC [13]
VirLock	4	✓ [15]	✗	✓	Unknown	XOR with Constant Key [15]
Androm	2	✗	✗	✗	Unknown	RSA+AES-256-CBC [11]
Razy	3	✗	✗	✗	.NET Crypto	AES-128^{9}
TeslaCrypt	4	✗	✗	✗	Unknown	ECC+AES-256-CBC [16]
Total 20	107	8	12	17		

Table 1: Active Ransomware Samples

Redemption another ransomware protection tool is introduced besides PayBreak and Cryptodrop. This detection technique is based on abstract model that holds behavior or characterization of large class of ransomware attacks is implemented. A process is marked as malicious if its behavior matches with the behavior recorded in abstract model [5].

5. Hardware Level Support:

5.1. Flash Guard:

Modern ransomware now using approach to run with administration privilege to load kernel code and carry out attacks on kernel level. They obtain kernel privileges to terminate software-based defense systems such as anti-virus or to destroy backups. To defend ransomware without depending on software-based solutions and backups, idea of Flash Guard-Solid State Drive (SSD) is proposed which has light weight hardware-assisted data recovery system and is resistant against ransomware. It has firm-level recovery system that provides efficient recovery from encryption ransomware without relying on backups. It is based on the out-of-place characteristic of an SSD. SSD keeps old copies of pages that are updated or deleted until they are reclaimed by the garbage collection process [9].

5.2. Design and Implementation:

Flash Translation layer (FTL) in new SSDs consists of four data structures. Flash Guard technique is based on Solid State Drive data structure. It modifies garbage collection process of SSD to keep copies of data encrypted by ransomware and to ensure data recovery. It consists of two major components, a tool for data recovery and (RFTL) Ransomware Flash Transition layer. SSD data structure works with other components of Flash Guard. It is very hard to track the pages that are encrypted. RFTL is proposed to track invalid pages resulted from ransomware attack.

RFTL use existing FTL structure with additional Data Structure RTT (Read Tracker Table). Ransomware encrypt data by reading from disk and then overwrite/delete original copy. RTT is used to track pages that has been read and to check if it is valid or not. Each entry is a read bit map indexed by a block address [9].

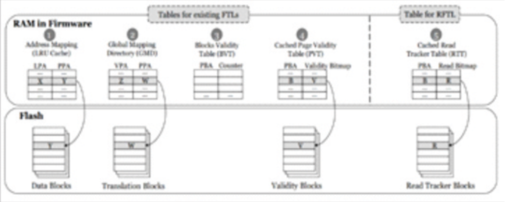


Figure 2: Overview of RFTL in Flash Guard.

5.3. Garbage-Collection in Flash Guard:

Garbage-collection is key component in SSDs, it provides free blocks for future use. It plays important role in keeping invalid pages (old copies) of the data exploited. A new garbage collection (GC) scheme in RFTL is proposed to make Solid State Drive capable of keeping data for recovery. Traditional GC looks for number of valid pages in each block by using Block Validity table (BVT) and to ensure whether block is garbage-collected or not. Once block is highlighted as GC candidate, PVT (Page Validity table) is accessed to verify which pages are valid and should be moved to new free block. The GC in RFTL follows the basic procedures of FTL including block selection and valid page movement. Invalid pages whose RIP bit is not set, and has been read as indicated by RTT, are treated as pages to be kept. RFTL copy retained invalid pages kept in flash device for a certain time or all encrypted writes which means all invalid pages that have been read will be kept in

SSD. It will keep retained invalid page until it is expired. Old copies (invalid pages) are collected by garbage collector (GC). RFTL takes retained invalid pages as valid pages and the blocks carrying these retained invalid pages will have their GC delayed. RFTL will delete those that have never been read and garbage collect it. The idea behind this is that before encryption data is read by ransomware from SSD, so pages that have never been read are not damaged data [9].

5.4. Data Recovery:

Flash Guard use its OOB meta data to reconstruct user files. It uses previous physical page address stored in metadata to reverse invalid page to its previous version. Recovery tool in Flash guard sort invalid pages with their LPAs and time stamp to recover original file. Flash guard keep all versions of invalid pages in flash device which helps recovery tool to reverse invalid pages and allow users to verify content [9].

5.6. Performance:

Flash Guard efficiently recovers encrypted user data. The execution time to restore encrypted data is from 4.2 to 49.6 seconds. According to statistically studies, flash guard have impact on storage performance. Only small portion of storage operations have similar I/O patterns. So flash guard will keep small amount of invalid pages for regular applications. Second, RFTL retained invalid pages by counting them as valid pages which delays GC execution on flash blocks. Third, FTL allows GC to run during idle time of flash controller which reduces performance. Finally, when all pages on flash block are invalid, flash block will be erased without any additional page movement. This gives boost to performance [9].

7. Discussions:

Pay Break is a system that hold keys on user behalf. Government mandated key escrow systems but this approach is criticized. Pay Break if different from Government proposed Key escrow system as only one entity is involved to access keys-user herself. To bypass ransomware approach, malware authors are considering to implement their own cryptographic libraries or to use secure third-party libraries but Pay Break working experience with different libraries shows that it is supportive against other libraries as well. For this, malware analyst needs to identify encryption scheme once and add it to Pay Break to add support [8]. Malware authors can use another strategy to bypass Pay Break by detecting that Pay Break is running on user machine and accordingly jump over the hooks. This approach of malware authors can be mitigated by inserting hooks at arbitrary points in the function [8]. Ransomware that have knowledge of Pay Break mechanism can bypass Pay Break by using denial of service attack either by corrupting the public key that is used to encrypt vault data or by putting garbage values into vault. Pay Break can be modified to have a dedicated process that appends to vault to protect public key. The privileged process mentioned above alerts user of ongoing attack and terminate malicious process. So Pay Break is a strong defense mechanism in fighting against modern ransomware and in recovering encrypted user files without paying ransom [8]. Considering SSD characteristics, few encryption ransomwares was developed. Flash gives support to data recovery by holding data encrypted by ransomware and prevents it from being removed by garbage collector [9]. Institutions suggest that attacker can exploit storage capacity by writing content to occupy available space in SSD which in turn forcing flash guard to leave control. Second attack would be that ransomware keep reading and overwriting data to SSD so that flash guard retains large amount of garbage data. Such attacks are not useful. Flash guard do not release data hold until data is expired, even though SSD is full. In this case, flash guard will stop taking I/O requests that result into failure of OS file system [9]. The longer the flash guard contains old data, the more overhead it imposes to I/O operations so time factor is important for both security and performance of flash Guard. For this, user needs to set expiry of holding data relatively short. Flash guard have negligible overhead to I/O operations even life span of data is set to 20 days [9]. Flash Guard can protect user against encryption ransomware on multiple platforms. Its approach can be applied to any kind of flash-based storage devices. Flash devices are used on mobiles as well. This idea can be deployed on mobiles to protect them from ransomware attack [9].

8. Conclusion:

Ransomware is new threat to modern world especially to small business owners and organizations. Cyber criminals attack user system, encrypts user data files and demand for ransom for files access. They are increasingly using bitcoins for their payments as Bit coin crypto currency is unregulated. Security research community proposed different tools and techniques by analyzing ransomware behavior and techniques that malware authors are using to by pass defense mechanism. Successful ransomware families are using hybrid crypto approach or exploiting kernel privileges. Pay Break is a protection tool that defeats threat of hybrid crypto ransomware by using key vault technique. It is very efficient in recovering encrypted files. Moreover, researchers explored possibility of using hardware to provide security against ransomware attack. They introduce flash guard as first firmware solution that is resistant against ransomware. This hardware level anti ransomware technique helps in providing resistance against kernel level ransomware attacks.

9. References

[1] A. Gazet, “Comparative analysis of various ransomware virii,” Journal in Computer Virology, vol. 6, pp. 77-90, 2010.

[2] A. Bhardwaj, “Ransomware: A rising threat of new age digital extortion,” in Online Banking Security Measures and Data Protection, ed: IGI Global, 2016, pp. 189-221.

[3] R. Brewer, "Ransomware attacks: detection, prevention and cure, "Network Security, vol. 2016, pp. 5-9, 2016.

[4] C. Everett, "Ransomware: To pay or not to pay?," Computer Fraud and Security, vol. 2016, pp. 8-12, 2016.

[5] A. Kharraz, W. Robertson and E. Kirda, "Protecting against Ransomware: A New Line of Research or Restating Classic Ideas?," in IEEE Security & Privacy, 2018.

[6] L. Zhang-Kennedy and J. R. R. M. K. B. a. S. C. Hala Assal, "The aftermath of a crypto-ransomware attack at a large academic institution," in 27th USENIX Security Symposium, 2018.

[7] D. Y. Huang, M. M. Aliapoulios, V. G. Li, L. Invernizzi, E. Bursztein, K. McRoberts, J. Levin, K. Levchenko, A. C. Snoeren and D. McCoy, "Tracking ransomware end-to-end," in IEEE Symposium on Security and Privacy, 2018.

[8] E. Kolodenker, W. Koch, G. Stringhini and M. Egele, "PayBreak: Defense Against Cryptographic Ransomware," in Conference on Computer and Communications Security, 2017

[9] J. Huang, J. Xu, X. Xing, P. Liu and M. K. Qureshi, "FlashGuard: Leveraging Intrinsic Flash Properties to Defend Against Encryption Ransomware," in Conference on Computer and Communications Security, 2017.

[10] A. Continella, A. Guagnelli, G. Zingaro, G. De Pasquale, A. Barenghi, S. Zanero, et al., "ShieldFS: A self-healing, ransomware-aware file system," in 32nd Annual Computer Security Applications Conference, ACSAC 2016, 2016, pp. 336-347.

[11] D. Kansagra, M. Kuhmar, and D. Jha, "Ransomware: A threat to Cyber-Security," CS Journals, vol. 7, 2016.

[12] R. Richardson and M. North, "Ransomware: Evolution, Mitigation and Prevention," International Management Review, vol. 13, p. 10, 2017.

[13] A. Kharraz, W. Robertson, D. Balzarotti, L. Bilge, and E. Kirda, "Cutting the gordian knot: A look under the hood of ransomware attacks," in International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment, 2015, pp. 3-24.

[14] D. P. Pathak and Y. M. Nanded, "A dangerous trend of cybercrime: ransomware growing challenge," International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume, vol. 5, 2016.

[15] P. Zavarsky and D. Lindskog, "Experimental Analysis of Ransomware on Windows and Android Platforms: Evolution and Characterization," Procedia Computer

Science, vol. 94, pp. 465-472,2016.

[16] KHARRAZ, A., ARSHAD, S., MULLINER, C., ROBERTSON, W. K., AND KIRDA, E. Unveil: A large-scale, automated approach to detecting ransomware. In USENIX Security Symposium (2016), pp. 757–772.

[17] SCAIFE, N., CARTER, H., TRAYNOR, P., AND BUTLER, K. Cryptolock (and drop it): stopping ransomware attacks on user data. In 36th International Conference on Distributed Computing Systems (ICDCS) (2016), IEEE, pp. 303–312.

[18] Eugene Kolodenker, William Koch, Gianluca Stringhini, and Manuel Egele, “PayBreak : Defense Against Cryptographic Ransomware” Conference Paper 2017 ACM.