Ransomware: Current Trend, Challenges, and Research Directions

Segun I. Popoola, *Member, IAENG*, Ujioghosa B. Iyekekpolo, Samuel O. Ojewande, Faith O. Sweetwilliams, Samuel N. John, Aderemi A. Atayero, *Member, IAENG*

***Abstract*—Ransomware attacks have become a global incidence, with the primary aim of making monetary gains through illicit means. The attack started through e-mails and has expanded through spamming and phishing. Ransomware encrypts targets' files and display notifications, requesting for payment before the data can be unlocked. Ransom demand is usually in form of virtual currency, bitcoin, because it is difficult to track. In this paper, we give a brief overview of the current trend, challenges, and research progress in the bid to finding lasting solutions to the menace of ransomware that currently challenge computer and network security, and data privacy.**

***Index Terms*—ransomware, cyber security, malware, cryptography, data encryption**

I. Introduction

RANSOMWARE is a particular class of malwares that demands payment in exchange for a stolen functionality, mostly data. This class of malware has been identified as a major threat to computer and network security across the globe [1]. Ransomware installs covertly on a victim's device to either mount the cryptoviral extortion attack from cryptovirology that holds the victim's data hostage, or the cryptovirology leakware attack that threatens to publish the victim's data. The real target of this form of attack are critical data that are very important to individuals and enterprises alike. In fact, the attack has spread to mobile devices and mobile malware detection approaches are not so effective because of the subtle nature of the malicious programs [2]. Therefore, billions of mobile device users are susceptible to this attack.

Most of the ransomware variants depend on file encryption as a strategy for extortion. Data stored on victim's device are encrypted while the hacker demands for ransom before the files can be decrypted. Ransomware may encrypt the Computer's Master File Table (MFT) or entire hard drive. It is a denial-of-access attack that prevents computer users from accessing files since it is intractable to decrypt the files without the decryption key. Ransomware attacks are typically carried out using a Trojan that has a payload disguised as a legitimate file. Although advanced encryption algorithms are useful for effective protection of vital enterprise data, they have become tools for malicious attacks in the hand of cyber-criminals. Data protection is, therefore, under serious threat as hackers continue to utilize enhanced algorithms in ransomware attacks.

Digital extortion has significantly increased in the last six years as the number of online applications and services, and smart mobile devices continue to grow exponentially [3]. The impact of ransomware has become so tremendous to the point that it is now rated as the biggest cyber scam to hit businesses [4]. About 80% of ransomware attacks exploit vulnerabilities in Flash that firms should have patched. Destructive ransomware can spread by itself and hold entire networks (i.e. companies) hostage.

Ransomware attacks are shifting focus from individuals to organizations. For instance, the Hollywood Presbyterian Medical Center in the United States was attacked in February 2016. The health care organization was forced to shut down when it was hit by Crypto Ransomware. The malicious program encrypted the files on their databases, denying medical staff the access to patients' health records [5]. In another occasion, the Methodist Hospital in Henderson, Kentucky only managed to recover its patient records with backups after surviving a ransomware attack. Stolen administrative credentials were used to infect servers with ransomware variant dubbed 'SamSam'. Active directory credentials were harvested to break into other servers. Overall, nearly half (46%) of firms have encountered ransomware attacks: 57% of medium-size organizations and; 53% of large organizations. Willingness to pay is surprisingly high. IBM found that 20% of executives would be prepared to pay over $40,000 each; 25% would shell out $20,000-$40,000 and; 11% would pay $10,000-$20,000.

Ransomware are now delivered as Word macros and PowerShell scripts. 'Petya' encrypted hard drive master boot record (MBR), as well as files, rendering computers completely unusable. The MBR is replaced with the malware's own bootloader so that the ransom note can be displayed. The most common method of delivering ransomware is the phishing attack and it is not easily recoverable.

According to the Federal Bureau of Investigation (FBI), estimated losses of about one billion US dollars ($1 billion) was incurred to ransomware attacks in the year 2016. The boom recorded by this crime shows that a good number of victims eventually pay the ransom to have their data

Manuscript received July 15, 2017; revised August 01, 2017.

The authors wish to appreciate the Center for Research, Innovation, and Discovery (CU-CRID) of Covenant University, Ota, Nigeria, for the partial funding of this research.

This work was supported in part by the Center for Research, Innovation, and Discovery (CU-CRID) of Covenant University, Ota, Nigeria.

S. I. Popoola, U. B. Iyekekpolo, S. O. Ojewande, F. O. Sweetwilliams, S. N. John, and A. A. Atayero are with the Department of Electrical and Information Engineering, Covenant University, Ota, Nigeria. (Corresponding Author: +2348058659008; +2347038049956; e-mail: segunpopoola15@gmail.com; segun.popoola@stu.cu.edu.ng).

unlocked. Nearly 40 percent of ransomware victims paid the ransom. Three out of four ransomware gangs are willing to negotiate prices for decryption. On average, they will give a 29% discount on the fee initially demanded. Unfortunately, traditional preventive and reactive security measures are not adequate to handle the effect of ransomware attacks [6].

In this paper, we provide a brief overview of the current trend, challenges, and research progress in the bid to finding lasting solutions to the menace of ransomware that currently challenge computer and network security, and data privacy.

II. Common Ransomware Variants

PC Cyborg was reported as the first ransomware variant [4]. The malware attack was launched in December, 1989. The victim was deceived with a message display that reads that the user license has expired. However, the encryption algorithm, symmetric cryptography, was not difficult to decrypt [7].

GpCode [8] also employed the custom symmetric encryption but the malware have been improved upon over time. The malware was propagated as job advert through spam e-mail attachment. In its first attack in May 2005, a static key was generated to encrypt all the non-system files. The original data was deleted as soon as the encryption is completed [9]. However, the key was discovered simply by comparing the original data to the encrypted data. A new variant of *GpCode*, called *GpCode.AG* was discovered in June 2016. Its encryption was based on 660-bit RSA public key. In June 2008, another variant, *GpCode.AK*, was identified but it was really difficult to crack owing to the computational demand.

Reveton, which is also known as *Police Ransomware*, is commonly spread through pornographic websites [10]. It changes the extensions in the windows/system32 folder and displays a notification page to its victims [11].

Locker Ransomware was identified in 2007 [8]. It does not tamper with its victims' data but only locks their devices. Therefore, the data on the device can be transferred to another location. Similarly, *ColdBrother Ransomware* locks victims' mobile devices, takes photographs with mobile phone cameras, answers and drops incoming calls, and seeks to defraud victims through mobile banking applications.

Crypto Ransomware encrypts critical files on victims' computer as a payload for extortion. Important files are identified and encrypted with 'hard-to-guess' keys. The choice of encryption keys and coordination of attacks are performed by a command and control server [12]. Crypto Wall, Tesla Crypt, CTB Locker, and Lock are all variants of *Crypto Ransomware*.

CryptoWall was introduced in November 2013. The malware is distributed by e-mail as an attached zip file. The attachment usually consists of a script file and an exploit kit. The malware is injected into explorer.exe and the codes are copied into %APPDATA%. This creates a registry value run key in the local user registry root path. This is done to keep the malware in the victim's computer even after a reboot. The malware also ensure that the system cannot be restored to an earlier point by running processes *vssadmin* and *dcbedit*. Thereafter, a svchost.exe is initiated to encrypt files and communicate with the command and control server. *CryptoWall* is one of the popular ransomware variants; about 31% of ransomware attacks were traced to this malware [13]. However, the encryption of victim's files can be frustrated by the disruption of the connection between the target's computer and the command and control server [14].

In *CryptoWall 2.0*, multiple propagation of e-mail attachments, drive-by download, exploit kits, and malicious portable document formats were added. The Onion Router (TOR) network was also introduced to guarantee anonymous network communication between the target's computer and the command and control server [15]. Some randomized data were introduced into *CryptoWall 3.0 and 4.0* to make malware detection more difficult by using exploit kits for privilege escalation and the Invisible Internet Project (I^2P) network for achieve anonymous peer-to-peer network.

CryptoLocker creates a set of extensions in the administrator's account which enables it to manipulate the Internet files [11]. Executable files are created in localAppData folder and critical files are detected for subsequent encryption. The malware uses the RSA + AES algorithm for its encryption process. Its exploit kit is known as Angler [16]. On the other hand, *CryptoDefense* uses a low-level cryptographic API that is available in Windows operating systems [17].

Curve Tor Bitcoin (CTB) Locker is also distributed through exploit kits and e-mail. Here, the command and control server is hidden on the Tor network. What is different in *CTB Locker* is its ability to encrypt victim's files without any connection to the Internet. It uses a combination of AES, SHA256, and Curve25519 for its encryption process. This malware essentially targets WordPress-based websites and it unleashes its terror through a PHP script [13].

TeslaCrypt, a recent variant of ransomware, exploits vulnerable websites using AnglerINuclear exploit kits. It has a similar distribution scheme as *CryptoWall* and all shadow copies are deleted using the vssadmin command [12].

Locky had its first attack in February 2016. The malware program was spread by attaching a Microsoft Office document to spam e-mail. The attached document contains a macro that downloads the malicious program to the target's computer. Unlike other ransomware variants, *Locky* extends its encryption to external storage devices, all network resources, database files, and wallet.dat. The wallet.dat is attacked to put the victim under a more intense pressure to pay [18]. Extra efforts were made to prevent easy shut down of the command and control server. This kind of malware employs hardcoded command and control server Internet Protocol (IP) addresses [15].

Cerber leverages the Dridex spam network to distribute the malware via large spam campaigns. The notification of attack is voiced through a text-to-speech module [15]. Devices that run on Windows 10 Enterprise have been attacked with more than 200 cases between December 2016 and January 2017 [18].

PowerWare was launched through a phishing campaign [11]. The operation of the malicious program is similar to

ISBN: 978-988-14047-5-6
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

that of *Locky* but its encryption and hard-coded keys are relatively weak. A decryption tool has been published to evade ransom.

ScareMeNot Ransomware is mainly targeted at Android-based devices and it has attacked over 30,000 devices [19]. *TROJ_CRYZIP.A* was discovered in 2005 [7]. Files on victim's computer are usually zipped and locked, displaying a notification of attack on the screen. It employs an asymmetric cryptography, which is stronger than the symmetric. On the other hand, *KeRanger* is targeted at Apple operating system. The malware is spread as a Trojan on the Transmission Bit Torrent client. As the target installs the program software, a binary file that is covertly embedded in the package is renamed and stored in the library directory as 'Kernel_process' for subsequent execution of the malicious program. All the files on the victim's computer with a particular file extension are encrypted after three days [20].

Seftad launches its attack on Master Boot Record (MBR), which contains the executable boot code and partition table [9]. Replacing the boot code in the active partition with a robust MBR that displays the attack notification prevents the target computer from loading its boot code. However, payment of ransom can be evaded through reverse engineering since the key is not usually hard-coded.

LowLevel04, also known as *Onion Trojan-Ransom*, was spread through the Remote Desktop or Terminal Services using brute force attack. Files were encrypted using AES encryption scheme using the RSA algorithm [21].

Unlike previous variants, *SilentCrypt* looks out for specific artifacts and private files to know if the code is running in an analysis environment or not [22]. *DirCrypt* uses a hybrid approach to encrypt user's files. The first 1024 bytes are encrypted using RSA while the rest are encrypted using the popular RC4 [17].

III. Failed Ransomware Attacks

A. Hitler Ransomware

It claims to have encrypted the victim's files, but in fact simply deletes file extensions for anything found in certain directories. After an hour it crashes the PC and, on reboot, deletes the files. The payment demanded is a cash code for E25 Euro Vodafone Card. Text found in the code suggests it originates in Germany.

B. Fake Windows 10 Lock Screen

It tells the user that their license has expired, turns out to have the decryption key buried in the code. Researchers from Symantec discovered that, while the criminals had gone to considerable effort to set up fake tech support websites for the scam, the phone number they gave out for victims to call was never answered and was soon disconnected. On reverse engineering the code, the researchers found the decryption key (8716098676542789) plainly visible.

C. 'PowerWare' and 'Bart'

They have been cracked by security researchers who found flaws in the malware. A team at Palo Alto Networks found that PowerWare, while trying to emulate the notorious Locky strain, had weak encryption and hard-coded keys. The company published a decryption tool and AVG created a decryptor for Bart due to the malware's poor encryption algorithm.

D. Chimera Ransomware

The decryption keys of the Chimera ransomware have also been published by a rival ransomware gang known as Janus. Janus aimed at ensuring there are enough victims available for its own malware, dubbed Mischa, which also uses some of the Chimera source code. The Chimera malware was never especially widespread, being aimed mainly at smaller German businesses. But it was notable for the threat from its creators that they would publish victims' private documents and login credentials if they didn't pay up. Security firms had yet to write a decryptor using the published keys. Victims are advised to keep the encrypted versions of their files safe for later decryption once the relevant tool is available.

IV. Current Research Findings and Solutions

The vulnerability of targets to Crypto ransomware attacks was identified in [23]. Easy recovery of users' data is prevented after being encrypted by exploiting the tools available on the victim's computer. However, victims can recover their data after a Crypto ransomware attack by changing the name of the system tool that performs shadow copies [23]. Information on the features of CryptoLockers and the prevention measures against attack can be found in [24].

Ill-preparedness of organizations offers cyber-criminals the ample opportunity of taking advantage of their targets. Therefore, businesses must engage relevant resources, develop strategic plans toward incidence response, educate their staff, and implement policies and regulations that guarantee network security, in order to forestall any attempt of ransomware invasion [25].

It has been established that more than 60% of the ransomware attacks gain access to victim's computer through drive-by downloads [26]. Currently, drive-by downloads are largely controlled by Exploit Kits (EK) and the choice of EK is determined by the control panel based on the vulnerabilities. A framework was proposed in [26] to detect malicious Rig EK communication and protect users' data from being encrypted using a combination of Software Defined Networking and Certificate Authority Checker (CAC).

Two countermeasures that free victims of ransomware attacks from paying the cyber-criminals were presented in [27]. These were achieved by exploiting the weakness of the working operation of the malware, and intercepting calls made to Microsoft's Cryptographic API respectively.

Useful information can be obtained from system API packages. These packages can be used to define applications without any prior knowledge of user-defined content. R-PackDroid was developed in [28] to detect Android-based ransomware and differentiate it from generic malware using machine learning approach.

On data recovery after ransomware attack incidence, a key-backup technique was suggested in [29]. This technique will store copies of the encryption keys in a secure

ISBN: 978-988-14047-5-6
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

repository. Relevant data security laws that borders on ransomware were discussed in [18].

Ganorkar and Kandasamy [30] explained the similarities and the differences among ransomware variants. Detailed knowledge of the working structure of these malwares provides enough information that is needed to develop an efficient defense scheme against the malicious attacks. Important steps to follow in order to avoid ransomware attacks are stated in [31]. Ransomware attacks targeted at Android devices can be prevented based on the method proposed in [32].

Ransomware attack is more prevalent in the health sector. An Electronic Health Record (EHR) system can be secured by using a socio-technical method [33]. Computers and networks that connect health IT professionals should be properly installed and configured to guarantee data security. In addition, system defense strategies adopted by health care organizations should be user-centric. Continuous monitoring of computers and applications must be ensured to promptly discover security vulnerabilities before they are being exploited by cyber-criminals. Quick recovery plans must be in place in case of any attack. Similarly, proactive actions must be taken to prevent a repeat of such occurrence. A dynamic system, which learns new behavior while under attack, was presented in [34].

Scaife et al. [35] presented an early-warning detection system, called *CryptoDrop*, which notifies the target of any suspicious activity. This system stops any process that seems to modify a large amount of data on the target's computer based on certain indicators. Technical solutions are not sufficient to handle ransomware attacks because the malicious programs exploit social engineering approach. In view of this, a honeypot folder can be created and monitored to detect changes. Either of Microsoft File Server Resource Manager characteristics or EventSentry can be chosen to modify the Windows security logs [36].

The analysis of selected ransomware variants from existing ransomware families in Windows and Android environments in [37] established that ransomware variants exhibit homogeneous characteristics; their main difference is in the payloads that are used. The encryption techniques employed by these ransomware have significantly improved. However, the malicious programs can be detected in Windows by keeping close watch on abnormal file system and registry activities. On the other, permission request by any Android application should be carefully screened before it is granted.

Formal methods were applied in [38] to detect ransomware and discover the malicious instruction set in the malware's code. Model checking was used in [39] to screen ransomware automatically with the aim of determining whether the characteristics of the program have the same pattern as that of the malicious programs.

Online processes can be screened for ransomware when suspected to be accessing a large amount of data based on the method proposed in [40]. The authors used the Kullback-Liebler divergence to detect a process that transforms structured input files (i.e. JPEG files) into unstructured encrypted files. Similarly, the enhanced ransomware prevention system, CloudRPS, in [41] works based on abnormal behavior analysis and detection in cloud analysis system. It offers more sophisticated attack prevention by monitoring the network, file, and server in real time. A cloud system is installed to gather and analyze different data that originate from user's device.

V. Precautionary Measures

In order to prevent the user's data from getting into unrecoverable state, users should have an incremental online and offline backups of all the important data and images. In addition, all the in-built defense mechanisms and detection tools should be kept up and running all the time. Exposure to threats should be minimized, where possible, with common sense, site or IP address blocking and endpoint protection. Organizations and individuals should ensure that their electronic defense is as impenetrable as possible through the use of anti-virus, firewalls, IPS, web and mail filtering. Policies that prevent penetration should be enforced in organizations by ensuring correct system configuration and device 'hardening'. A robust and incremental back-up system of business and personal-critical details should be implemented.

Also, personnel must ensure that offline back-ups remain offline at all times so they are protected. Backups should be tested regularly to guarantee protection. Organizations should put robust policy and processes and a practical system of educating users on how to best prevent and deal with ransomware attacks in place. Users should enforce a general information policy pertaining to what websites are Safe for Work (SFW) and Not Safe for Work (NSFW) and educate themselves and their team on the risks and the methods by which ransomware is activated and attacks are carried out from beginning to end.

Organizations need a system in place that looks for anomalous behavior such as rapid encryption or malicious non-human activity, to avoid falling prey to rapidly evolving and adapting ransomware attacks. The location where data is stored on file systems should be known, especially in unstructured formats in documents, presentations, and spreadsheets. Access to personal data should be limited on a need-to-know basis or through role-based access controls. The goal is to make it difficult for attackers to access important data after hacking an ordinary user – say, through a phishing email – and launching ransomware based on that user's credentials. Organizations should also remove and/or archive outdated or stale personal data, further reducing the attack surface.

Ordinary users whose credentials the ransomware is leveraging, do not perform a large-scale scans of crawling a file system, navigating through each directory and examining file. Therefore, monitoring software, particularly based on User Behaviour Analytics (UBA), should be able to detect the ransomware and limit the number of files that are encrypted. Companies should perform should regularly perform back-ups of their file systems, especially critical and sensitive data and have in place a recovery plan for restoring the data in the case of cyber-attacks.

In order to handling a ransomware attack: systems must

ISBN: 978-988-14047-5-6
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

be aggressively patched; back-ups must be created and protected; an incidence response plan must be developed; and user awareness training must be conducted. Detection

VI. Conclusion

Ransomware attacks have become a global incidence, with the primary aim of making monetary gains through illicit means. The attack started through e-mails and has expanded through spamming and phishing. Ransomware encrypts targets' files and display notifications, requesting for payment before the data can be unlocked. Ransom demand is usually in form of virtual currency, bitcoin, because it is difficult to track.

The variants of ransomware has continue to increase because of the profitability of the illicit act. However, there is a growing effort to curb the spread of this malware. A good understanding of the behavior of ransomware will help individuals and enterprises to tidy up their vulnerabilities to this kind of attack. State-of-the-art research findings, proposed solutions, and precautionary measures are provided in this study. With the recent spread of ransomware attacks on Linux and Mac operating systems, the analysis of ransomware on these platforms is needful. Kaspersky Lab and Intel have joined forces with Interpol and the Dutch National Police to set up a website (www.nomoreransom.org) aimed at helping people to avoid falling victim to ransomware. The website will host decryption keys and tools for those ransomware strains that have been cracked by security researchers.

To avoid data theft and undue extortion of ransomware, individuals and organization needs robust network security platform. This topic is an emerging field of study in academic research. Therefore, more research effort is needed to stop the growing trend of ransomware attacks.

Acknowledgment

The authors wish to appreciate the Center for Research, Innovation, and Discovery (CU-CRID) of Covenant University, Ota, Nigeria, for the partial funding of this research.

References

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

[2] N. Andronio, S. Zanero, and F. Maggi, "HELDROID: Dissecting and detecting mobile ransomware," in *18th International Symposium on Research in Attacks, Intrusions, and Defenses, RAID 2015* vol. 9404, H. Bos, G. Blanc, and F. Monrose, Eds., ed: Springer Verlag, 2015, pp. 382-404.

[3] 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.

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

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

[6] 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.

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

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

[9] 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.

[10] 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.

[11] 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.

[12] M. Weckstén, J. Frick, A. Sjöström, and E. Järpe, "A novel method for recovery from Crypto Ransomware infections," in *Computer and Communications (ICCC), 2016 2nd IEEE International Conference on*, 2016, pp. 1354-1358.

[13] H. Haughey, G. Epiphaniou, and H. M. Al-Khateeb, "Anonymity networks and the fragile cyber ecosystem," *Network Security*, vol. 2016, pp. 10-18, 2016.

[14] K. Cabaj and W. Mazurczyk, "Using software-defined networking for ransomware mitigation: the case of cryptowall," *IEEE Network*, vol. 30, pp. 14-20, 2016.

[15] E. Kalaimannan, S. K. John, T. DuBose, and A. Pinto, "Influences on ransomware's evolution and predictions for the future challenges," *Journal of Cyber Security Technology*, vol. 1, pp. 23-31, 2017.

[16] K. K. Gagneja, "Knowing the ransomware and building defense against it-specific to healthcare institutes," in *Mobile and Secure Services (MobiSecServ), 2017 Third International Conference on*, 2017, pp. 1-5.

[17] B. Herzog and Y. Balmas, "Great Crypto Failures," 2016.

[18] A. Green, "Ransomware and the GDPR," *Network Security*, vol. 2017, pp. 18-19, 2017.

[19] T. C. Back, "Intel's Core M Chip could let manufacturers build ultraslim laptops."

[20] B. Kim, "AN ANALYSIS OF VULNERABILITY EXPLOITATION TECHNIQUES USED BY OSX MALWARE AND THEIR DEFENSES."

[21] M. H. U. Salvi and M. R. V. Kerkar, "Ransomware: A cyber extortion," *Asian Journal of Convergence in Technology*, 2016.

[22] A. Kharraz, S. Arshad, C. Mulliner, W. K. Robertson, and E. Kirda, "UNVEIL: A Large-Scale, Automated Approach to Detecting Ransomware," in *USENIX Security Symposium*, 2016, pp. 757-772.

[23] M. Wecksten, J. Frick, A. Sjostrom, and E. Jarpe, "A novel method for recovery from Crypto Ransomware infections," in *2nd IEEE International Conference on Computer and Communications, ICCC 2016*, 2017, pp. 1354-1358.

[24] L. Usman, Y. Prayudi, and I. Riadi, "Ransomware analysis based on the surface, runtime and static code method," *Journal of Theoretical and Applied Information Technology*, vol. 95, pp. 2426-2433, 2017.

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

[26] P. Raunak and P. Krishnan, "Network detection of ransomware delivered by exploit kit," *ARPN Journal of Engineering and Applied Sciences*, vol. 12, pp. 3885-3889, 2017.

[27] A. Palisse, H. Le Bouder, J. L. Lanet, C. Le Guernic, and A. Legay, "Ransomware and the legacy crypto API," in *11th International Conference on Risks and Security of Internet and Systems, CRISIS 2016* vol. 10158 LNCS, N. Cuppens, F. Cuppens, J. L. Lanet, and A. Legay, Eds., ed: Springer Verlag, 2017, pp. 11-28.

[28] D. Maiorca, F. Mercaldo, G. Giacinto, C. A. Visaggio, and F. Martinelli, "R-PackDroid: API package-based characterization and detection of mobile ransomware," in *32nd Annual ACM Symposium on Applied Computing, SAC 2017*, 2017, pp. 1718-1723.

[29] K. Lee, I. Oh, and K. Yim, "Ransomware-prevention technique using key backup," in *7th International Conference on Big Data Technologies and Applications, BDTA 2016* vol. 194 LNICST, J. J. Jung and P. Kim, Eds., ed: Springer Verlag, 2017, pp. 105-114.

[30] S. S. Ganorkar and K. Kandasamy, "Understanding and defending crypto-ransomware," *ARPN Journal of Engineering and Applied Sciences*, vol. 12, pp. 3920-3925, 2017.

[31] K. K. Gagneja, "Knowing the ransomware and building defense against it-Specific to healthcare institutes," in *3rd Conference on Mobile and Secure Services, MOBISECSERV 2017*, 2017.

[32] S. Song, B. Kim, and S. Lee, "The Effective Ransomware Prevention Technique Using Process Monitoring on Android Platform," *Mobile Information Systems*, vol. 2016, 2016.
[33] D. F. Sittig and H. Singh, "A socio-technical approach to preventing, Mitigating, and recovering from Ransomware attacks," *Applied Clinical Informatics*, vol. 7, pp. 624-632, 2016.
[34] M. Shukla, S. Mondal, and S. Lodha, "POSTER: Locally virtualized environment for mitigating ransomware threat," in *23rd ACM Conference on Computer and Communications Security, CCS 2016*, 2016, pp. 1784-1786.
[35] N. Scaife, H. Carter, P. Traynor, and K. R. B. Butler, "CryptoLock (and Drop It): Stopping Ransomware Attacks on User Data," in *36th IEEE International Conference on Distributed Computing Systems, ICDCS 2016*, 2016, pp. 303-312.
[36] C. Moore, "Detecting ransomware with honeypot techniques," in *1st Cybersecurity and Cyberforensics Conference, CCC 2016*, 2016, pp. 77-81.
[37] Monika, P. Zavarsky, and D. Lindskog, "Experimental Analysis of Ransomware on Windows and Android Platforms: Evolution and Characterization," in *11th International Conference on Future Networks and Communications, FNC 2016 / 13th International Conference on Mobile Systems and Pervasive Computing, MobiSPC 2016*, 2016, pp. 465-472.
[38] F. Mercaldo, V. Nardone, A. Santone, and C. A. Visaggio, "Ransomware steals your phone. Formal methods rescue it," in *36th IFIP WG 6.1 International Conference on Formal Techniques for Distributed Objects, Components, and Systems, FORTE 2016 and Held as Part of the 11th International Federated Conference on Distributed Computing Techniques, DisCoTec 2016* vol. 9688, E. Albert and I. Lanese, Eds., ed: Springer Verlag, 2016, pp. 212-221.
[39] F. Mercaldo, V. Nardone, and A. Santone, "Ransomware inside out," in *11th International Conference on Availability, Reliability and Security, ARES 2016*, 2016, pp. 628-637.
[40] F. Mbol, J. M. Robert, and A. Sadighian, "An efficient approach to detect torrentlocker ransomware in computer systems," in *15th International Conference on Cryptology and Network Security, CANS 2016* vol. 10052 LNCS, G. Persiano and S. Foresti, Eds., ed: Springer Verlag, 2016, pp. 532-541.
[41] J. K. Lee, S. Y. Moon, and J. H. Park, "CloudRPS: a cloud analysis based enhanced ransomware prevention system," *Journal of Supercomputing*, pp. 1-20, 2016.

ISBN: 978-988-14047-5-6
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)