Modern Ransomware Attacks and Countermeasures(Cyber Crime)

Jeyaradnam Tharjalan
Undergraduate–department of information system
Faculty of computing
Srilanka Institute of Information Technology
Malabe,Srilanka
Tharjalan@icloud.com

Udagedara C.L
Undergraduate–department of information system
Faculty of computing
Srilanka Institute of Information Technology
Malabe,Srilanka
lakshikauda@gmail.com

***Abstract*— Cybercrimes have started to become one of the most difficult and deadly sort of crimes in the present world. Instead of simply hacking in real time, cyber criminals have come to start using malwares, a kind of software that infects victims through popular social services site as well as download clients. Ransomware, a type of a malware that demands ransom for the data it locks out from users, is one of the leading contenders in all the types of malwares used by various offenders. This research mainly stayed on how these ransomware infects and then goes on to spreading more widely through the internet as well as the repercussions that come with the infection in a victim's machine by reviewing other works related to the topic. It should be noted on how these malware are spreading and how they are expected to start spreading in future as well, since they are a main factor in creating countermeasure to such attacks at the current as well as in future. Once a machine is infected it is nearly impossible to recover from the damage even when the ransom demand has been met, so it is wise to create counters before even the threat appears as per research.**

***Index Terms*—cybercrime, cyber criminal, ransomware, ransom, malware, infection, contremesure**

I. Introduction

Nowadays, number of digital platforms are very high and still increasing. And every user has interconnected their personal or unique information with these digital devices. Having the important details without the proper security mechanism is the very high amount of risk. In this case, cybercriminals are using malware to the targeted host and demand victims to pay the huge amount through this malware called ransomware. Then, the attacker will send the payload to the targeted host using spam emails, social engineering or via torrent download. Then attacker will activate the payload remotely. Then the ransomware will encrypt all of the target's important files and pop up the payment methods to decrypt it. Usually, attackers demand payment in bit coins because it cannot be traced.

In the past ransomware has targeted most of the field in the different sectors. Those are,

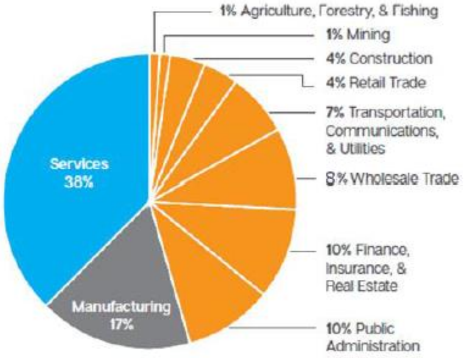

Figure1. Ransomware Infection in the Organization Sector Jan 2015 to Apr 2016[10]

The first ransomware attack was happened around 1989, that malware name was AIDS Trojan[8].Rasnsomware attacks is very effective because its deals with symmetric and asymmetric encrypting[10]. Some Common Ransomware types are CryptoWall, Brolo, Reveton,Tesla,CTB-Locker. Most of the ransomware attacks happened because of this Tesla Crypt and CTB locker.

a. Ransomware infection

The attackers Are doing some hybrid encryption technique[10],That means symmetric key will use for encryption process in the targeted hos[10]t. And public key will use to encrypt that symmetric key.In order to decrypt the symatric key,only the private key that from generated from RSA pair can do[10]. Some of the attacks stores the encrypted symmetric key in the targeted host while the users deal with dangerous[10]. That will define on blow figure[10].

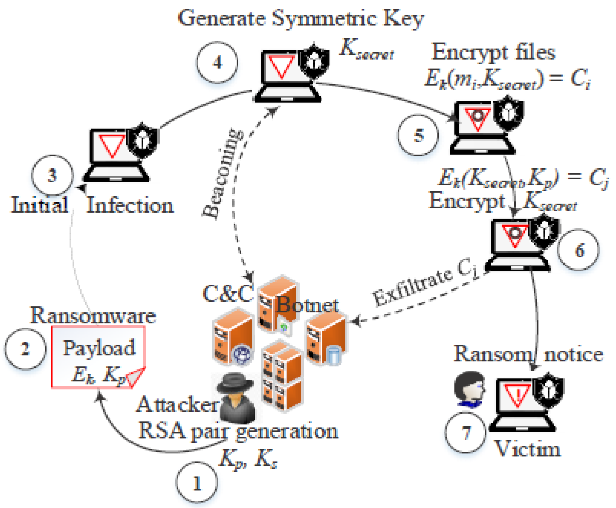

Figure2:Hybrid Encryption Crypto ransomware with key[10]

II. Objective

This literature review will cover the research areas that regarding the brief introduction of ransomware attacks and Contain review if all important research papers separately. That was done in chronological order, this mean all the research papers was reviews according to the published period. This will clarify, what is the process during the attacks, as well as various type of malware in the current world or the past, Then various type of mitigation techniques against ransomware attack. And it will talk about mitigation procedures will help to avoid these kind of problems occurrence.

III. Review of the literature

All of these research papers has been reviewed in chronological order.

A. Connection-Monitor & Connection-Breaker: A Novel Approach for Prevention and Detection of High Survivable Ransomwares(Sep 2015)

Ransomware is a software that uses encryption to earn money illegally[1].Attackers encrypt various file system on the user's hard drives or removable disks as well as shared network details too[1]. This paper based on systematic and high survivable ransomware (HSR) in the key generated and key changing protocol process[1]. And novel approach for identifying high survivable malware and intercept them from encrypting targeted host data. Ransomware can affect all of the devices that such as desktop, laptop, tablets and also mobile devices, To mitigate the encryption process before attacker start some step are here[1]. One is novel ransomware system based on attacks and novel approach for identifying the HSRs use domain generation algorithm[1]. None cryptographic ransomware mean this malware does not use the encryption technique[1]. This is for lock the screen[1] or modifies the master boot recorder or change the partition table[1]. Cryptographic Ransomware means this is using encryption algorithms and capture user's assets and asking for the payment[2]. Private Key cryptosystem ransomware means this used self-designed cipher[1] crypto system that similar to polyalphabetic substitution cipher in just first 512 bytes data of the victim's files. to mitigate the ransomware their created DGA framework[1] and Novel Monitoring. [1]

B. A Novel Method for Recovery from Crypto Ransomware Infections(Feb 2016)

Blackmailing the normal users through the digital platform is the increasing crime in the world[2]. Now the Attackers use some crypto Ransomware to blackmail the users[2]. Criminals are using user's simple recovering system's tools vulnerabilities in order do the attacks[2]. Most of the people are storing their credentials information in online devices that deal with the internet[2]. So having an important data without proper security is a huge risk. This paper mainly focuses on detection part and not about the possibilities of recovering damaged documents in the system after an infection. Criminals are using the bit coins payment system[2], which means that it’s hard to trace them. Ransomware is differing from other malware because this type of malware is using payloads to do the attack and as well as it includes some social engineering strategy also. Criminals using a command and control server to infect the payloads to the targeted systems [2]and activate the remote attacks as well as the encryption-decryption keys and payments process too[2]. In order to avoid these problems, there are some mitigation plans such as updating the recovery system tools and maintaining a proper firewall, update the operating system regularly and finally, maintaining reliable backups[2].

C. *Cyber Ethics and Cyber Crime: a deep delved study into legality, ransomware, underground web and bit coin wallet(Apr 2016)*

This research mainly focuses on studying the ransomware family that is called CTB Locker[3] or the Crypto Locker ransomware with the thought that in the future[3], wars will be fought through internet and the attacks will be a steady combination of both cryptography and malware to thwart information systems and security. Since the internet has expanded[3] so fast and exponentially, the threats that came with it has also increased by a moderate amount[3]. One of the newest form of cyber hack jacking in cyberspace is crypto virus or rather ransomware[3]. These locker bots sleep inside the system until a certain event is triggered[3] to become active and then hijack the system from within by encrypting files and folders an then demanding monetary reward for the release of decryption key[3]. The research delves deep into the physical money earned through each victims and the C&C Server[3], the source which resides in the Dark Net. Furthermore, the CTB Locker creates a Bitcoin wallet[3] per victim and maintain the anonymity while also earning digital money through it[3]. To counter this it is suggested to have a strong offline backup for all important files[3] as well as updated anti-virus software so as to prevent data loses instead of looking to restore files after the infection has spread. [3]

D. *Ransomware Inside Out(Sep 2016)*

This paper contains how the ransomware affect android platform[4]. Android is the most popular platform used by users nowadays. As usual, this platform also has some vulnerability, so attackers use these areas and gather their data and resort to blackmailing them[4]. This paper explains about formal methods by model checking[4]. It will automatically analyze the ransomware starting from manual checking. Android platform is an open system that allows users to load application from unauthorized sources so, this is the big threat[4]. The attacker uses this to gather information. Ransomware is very dangerous for mobile phone compared to the computer[4]. The malware will gather people's most personal things. Linux environment is also affected by ransomware called Trojan-Ransom. Linux[4]. Most of the criminals are using clickjacking method to gain user's administrative permissions[4]. Clickjacking exploits user interface[4] and then it will allow the attacker to compromise the users data. Most of these will be web-based applications[4]. Most of the user privileges send SMS, Lock the devices, steal the contacts, and steal the phone information and photos as well as other private things[4]. As per this paper, a method has been proposed which will automatically analyze the ransomware corresponding to the android[4]. When model checking is used it will create a set of rules at the test time and then start to verify the ransomware. [4]

E. *Using Software-Defined Networking for Ransomware Mitigation: The Case of Crypto Wall (Nov 2016)*

This paper says how to mitigate the ransomware attacks using software-defined networking Methods[5]. In order to do those, first analyzes the behavior of most common ransomware. To do that, they have introduced SDN based system[5] that is created using Open Flow[5] which will provide real-time reaction to this threat. And most important thing is this system does not affect the Overall network's performance[5]. It will help to overcome the current network systems. In the SDN Control[5], data planes are separated so the network can survive in logically centralized manner[5]. SDN paradigm is the protocol that will allow access to networking devices[5] such as routers and switches which depend on the internal flow of the network tables. They are all managed by the external controller[5]. SDN has the ability to offer the powerful and unique network security more efficiently and in a flexible[5] behavior. When this system identifies that a particular host got affected or any harmful thing, then the controller can immediately do the mitigation actions such as update the network rule on the network devices[5]. If there is any malicious activity on the network, the system will Block the host traffic immediately or it can disconnect all the devices from the network[5]. SDN is an anomaly-based detection[5] system. SDN can work to identify network attacks, detect malicious application in mobile phones or monitor the dynamic cloud networks[5]. If any harmful activity is detected, then this system will block the Connection or block the infected hosts by applying the controlling protocols in the real time. This will give more effective and specific mitigations. Example, system will shut down host proxy server when any incident happens for protecting the users[5]. If the connection is stopped attacker can't encrypt the files. This system will depend on day to day update of malicious software proxy servers. There are two approaches to mitigate from ransomware those are well-known network traffic characteristics and pattern based characteristics[5].

F.Ransomware: Studying Transfer and Mitigation(Dec 2016)

Cybercrimes at the current time are mostly all about on gaining monetary returns other than most other way of gains[6]. This research paper focuses on finding out the dependence of ransomware on certain aged people and in education alike. Research on how easy it is to transfer ransomware through the internet is also discussed[6]. Analysis was done through literature study, surveying and analyzing the outcomes of the above to find out the most used infection methods such as torrent download clients and sites as well as software vulnerabilities[6]. Through these analysis, an understanding on how and why the ransomware is so effective has been come to. The consensus is, most of the company employees seem to depend on IT department to prevent malware threats and not have awareness[6] on how to prevent them themselves. With the insight, the study went on to explore the possibilities of discovering measures [6]and actions that can be taken to counter the ransomware attacks. Even though there are more than enough working mitigation strategies, many affected victims do not even bother to use them. Finally, it was confirmed that almost all the people affected by ransomware is either unable or unwilling to pay the demand.[6]

G.Knowing the Ransomware and Building Defense Against it – Specific to HealthCare Institutes (Jan 2017)

Health care system is one of the most affected systems with ransom ware attacks[7]. Cyber criminals mainly target this area because its deals with huge number of patients credentials data so it could help to get huge amount of it[7]. This malware can be sent as normal mail, that may contain 'invoice details' and some legitimate forms then the users think as normal mail and store it, so the malicious file will go to the organization's network easily through the firewall[7]. Then it will do the malicious activity such as encrypting the files that was in the system. After that, some windows will appear and may contain what are the procedures for finding the key to decrypt the credential files[7]. Since this is a health care industry, the effect will be huge because of patient's data[7]. When the malware get infected all of the data will get encrypted and they cannot be accessed by legitimate users until the payment procedure is done[7]. Most of the health care industries are not upgraded to the modern prevention systems. Some of them are doing but slowly[7]. So the attackers use this vulnerabilities and attack to earn[7]. Most of the malware, blocks user access to the data files such as Word files, PDF documents, Videos and so on[7]. Then when the payment is done then, the decryption key will be sent to the affected system. This will take 3 or 4 days so during these days there will be huge loss to origination such as loss of productivity, loss in the business[7]. In order to avoid these problems every originations have to do the backup in regular manner and separate the backup file from the online infrastructure and make the system update and patch often. Purchasing efficient email scanning tools as well as educating healthcare employees about modern world attacks will do much good to the system too[7].

H. Know Abnormal, Find Evil: Frequent Pattern Mining for Ransomware Threat Hunting and Intelligence(Feb 2017)

Cyber criminals doesn't only pose a threat to business, but also to government as well as other financial institutions across the entire globe[8]. Since the emergence of crypto-ransomware, cyber threat terrain has undergone a significant evolution[8] and which is not in a good way to PC users[8]. The critical detection system of ransomware depends much on how fast and precise the system log mining[8] is to find anomalies and prevent them[8]. This research utilizes a series of orderly pattern mining to find the most frequent pattern of activities used in different ransomware families[8]. 99% of detection accuracy from goodware samples[8] as well as another 96.5% detection accuracy from given specific ransomware samples[8] were achieved in detecting ransomware instances[8]. The results shows the feasibility and adequacy of trying out pattern mining techniques to detect good properties of applications to hunt if they are ransomware[8]. The research also found peculiar frequent patterns in these ransomware families and used them to identify ransomware sample family and find insight about threat profile and actors of specific targets. [8]

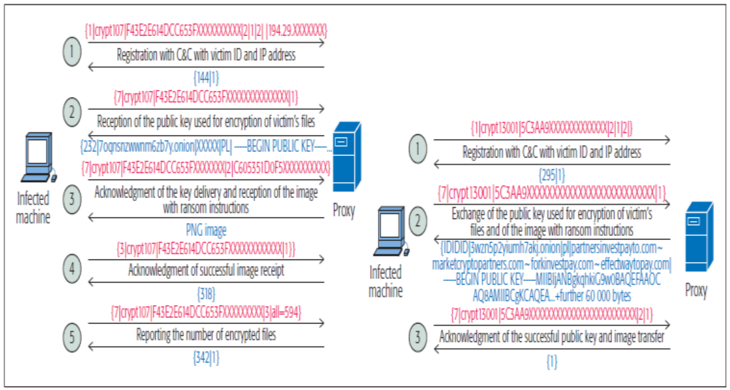
{1|crypt107|F43E2E614DCC653FXXXXXXXXXX|2|1|2| |194.29.XXXXXXX}
1
Registration with C&C with victim ID and IP address
{144|1}
{7|crypt107|F43E2E614DCC653FXXXXXXXXXXXXXX|1}
2
Reception of the public key used for encryption of victim's files
{232|7oqnsnzwwnm6zb7y.onion|XXXXX|PL| ----BEGIN PUBLIC KEY----...
{7|crypt107|F43E2E614DCC653FXXXXXXX|2|C605351D0F5XXXXXXXXXX}
3
Acknowledgment of the key delivery and reception of the image with ransom instructions
PNG image
{3|crypt107|F43E2E614DCC653FXXXXXXXXXXXX|1}}
4
Acknowledgment of successful image receipt
{318}
{7|crypt107|F43E2E614DCC653FXXXXXXXXX|3|all=594}
5
Reporting the number of encrypted files
{342|1}
Infected machine
Proxy
{1|crypt13001|5C3AA9XXXXXXXXXXXXXX|2|1|2|}
1
Registration with C&C with victim ID and IP address
{295|1}
{7|crypt13001|5C3AA9XXXXXXXXXXXXXXXXXXXXXXXXXX|1}
2
Exchange of the public key used for encryption of victim's files and of the image with ransom instructions
{IDIDID|3wzn5p2yiumh7akj.onion|pl|partnersinvestpayto.com~marketcryptopartners.com~forkinvestpay.com~effectwaytopay.com|----BEGIN PUBLIC KEY----MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA...+further 60 000 bytes
{7|crypt13001|5C3AA9XXXXXXXXXXXXXXXXXXXXXXXX|2|1}
3
Acknowledgment of the successful public key and image transfer
{1}
Infected machine
Proxy

Figure3: Communication of Cryptowall version 3.0 at left and 4.0 at right[5]

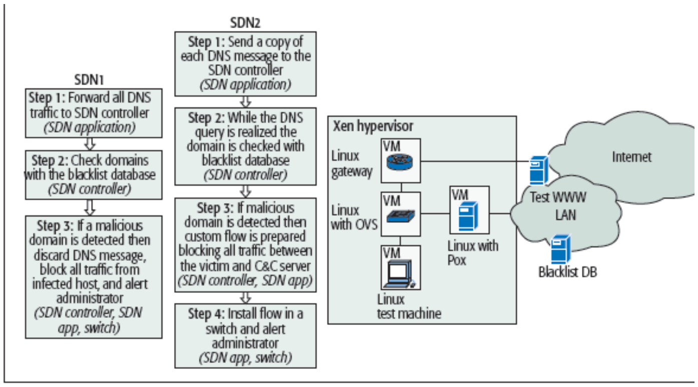
SDN1
Step 1: Forward all DNS traffic to SDN controller (SDN application)
Step 2: Check domains with the blacklist database (SDN controller)
Step 3: If a malicious domain is detected then discard DNS message, block all traffic from infected host, and alert administrator (SDN controller, SDN app, switch)
SDN2
Step 1: Send a copy of each DNS message to the SDN controller (SDN application)
Step 2: While the DNS query is realized the domain is checked with blacklist database (SDN controller)
Step 3: If malicious domain is detected then custom flow is prepared blocking all traffic between the victim and C&C server (SDN controller, SDN app)
Step 4: Install flow in a switch and alert administrator (SDN app, switch)
Xen hypervisor
VM
Linux gateway
VM
Linux with OVS
VM
Linux with Pox
VM
Linux test machine
Internet
Test WWW LAN
Blacklist DB

Figure4: SDN based application [5]

I. UNVEIL: A Large-Scale, Automated Approach to Detecting Ransomware (Feb 2017)

As per this paper, ransomware is not a new thing to this world[9]. It was created awhile back but very recently made a huge impact in each and every field[9]. Ransomware is normally doing the operation of the targeted system and make it inaccessible to the legitimate user by remote instructions[9], encryption, overwrite and delete the user's important files]9[. There are many antivirus or malware detection systems but many of these do not detect any ransomware[9]. This research talks about some dynamic analysis system[9]. This system is called as UNVEIL[9]. This system is designed to detect or find the ransomware. The system has an ability to find the new ransomware which that not is in any anti-virus system[9]. Since ransomware uses user's file on the system, the UNVEIL system will create a virtual user interface like original[9], and then it detects the ransomware when the malware tries to infect itself to the system. At the same[9]

J. Reasoning Crypto Ransomware Infection Vectors with Bayesian Networks (June 2017)

Techniques used in ransomware have evolved into such a powerful version[10] that the most resilient ones make recovery of data almost impossible[10]. Because of this most of the countermeasures in present tend to focus more on recovery than preventing the attack itself[10]. This research looks at ransomware attacks from infection vector point of view[10]. The research uses Bayesian network statistics to understand and deduce the most common ransomware vectors and to follow the infection chain of crypto ransomware[10]. It should be noted that to capture the unpredictability of Bayesian network, attack and sensor nodes were used[10].

IV. Future Researches

future research will extend the method that now used for the teasing to Computers and metamorphic malware in order to check whether this mitigation procedures are useful to detect harmful payloads related to the computers. and do the forensic by design to monitor the ransom ware detection and mitigation and rollback. Then applying the fuzzy classification to reduce the ransom-ware attack. Some of more planes will execute in future, Those are Analyze the different type of threats.

V. Conclusion and Recommendation

In this review paper, by analyzing the important researches, it will help to give the awareness of ransomware to the people who don't know how to create countermeasures. Rasnsomware is a malware that widely spreads through the internet based services. Most of the companies that got affected in the past was because of the irresponsibility and ignorance of the employees. And as for the prevention technique, existing techniques work well but, only a few people know about the knowhow of using them. As per this paper, some mitigation techniques are heavily recommended for common users which are to update the anti-virus software, maintain a healthy firewall properly, regularly update the operating system and applications as well as having a proper backup scheme. These countermeasures will help to avoid these kinds of attacks.

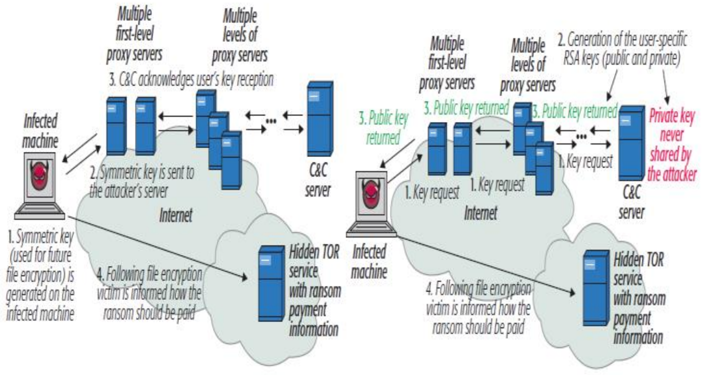
Multiple first-level proxy servers
Multiple levels of proxy servers
3. C&C acknowledges user's key reception
Infected machine
2. Symmetric key is sent to the attacker's server
C&C server
Internet
1. Symmetric key (used for future file encryption) is generated on the infected machine
4. Following file encryption victim is informed how the ransom should be paid
Hidden TOR service with ransom payment information
Multiple first-level proxy servers
Multiple levels of proxy servers
2. Generation of the user-specific RSA keys (public and private)
3. Public key returned
3. Public key returned
3. Public key returned
Private key never shared by the attacker
1. Key request
1. Key request
1. Key request
C&C server
Internet
Infected machine
4. Following file encryption victim is informed how the ransom should be paid
Hidden TOR service with ransom payment information

Figure4: On the left symmetric and on the right it asymmetric crypto ransomware. [5]

a. Countermeasures strategies for ransomware .

1) Avoid to click the popups and ads in while browsing [6]
2) *Update the anti-virus system immediately when the update is released.[6]*
3) Do not submit the request of malware.
4) Beware when got emails form unknown users and don't click the attachments.[6]
5) When the malware is found disconnect the internet form the computer and reinstall the os as soon as possible.
6) Give awareness and training to employees;
   About access control system and policies and controls.[6]

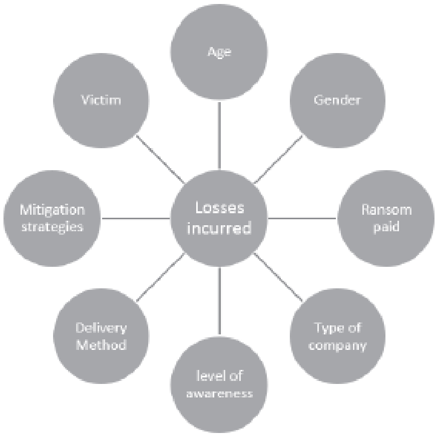

Figure5: dependency of losses on parameters[6]

VI. ACKNOWLEDGEMENT

Being very thankful to srilanka institute of information technology,malabe, For all the facilities to get those research papers and other resources.

VII. REFERENCES

[1]M. Ahmadian, H. Shahriari and S. Ghaffarian, "Connection-monitor & connection-breaker: A novel approach for prevention and detection of high survivable ransomwares", *2015 12th International Iranian Society of Cryptology Conference on Information Security and Cryptology (ISCISC)*, 2015.

[2]M. Wecksten, J. Frick, A. Sjostrom and E. Jarpe, "A novel method for recovery from Crypto Ransomware infections", *2016 2nd IEEE International Conference on Computer and Communications (ICCC)*, 2016.

[3]R. Upadhyaya and A. Jain, "Cyber ethics and cyber crime: A deep dwelved study into legality, ransomware, underground web and bitcoin wallet", *2016 International Conference on Computing, Communication and Automation (ICCCA)*, 2016.

[4]F. Mercaldo, V. Nardone and A. Santone, "Ransomware Inside Out", *2016 11th International Conference on Availability, Reliability and Security (ARES)*, 2016.

[5]K. Cabaj and W. Mazurczyk, "Using Software-Defined Networking for Ransomware Mitigation: The Case of CryptoWall", *IEEE Network*, vol. 30, no. 6, pp. 14-20, 2016.

[6]R. Shinde, P. Van der Veeken, S. Van Schooten and J. van den Berg, "Ransomware: Studying transfer and mitigation", *2016 International Conference on Computing, Analytics and Security Trends (CAST)*, 2016.

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

[8]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*, pp. 1-1, 2017.

[9]E. Kirda, "UNVEIL: A large-scale, automated approach to detecting ransomware (keynote)", *2017 IEEE 24th International Conference on Software Analysis, Evolution and Reengineering (SANER)*, 2017.

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