A Review of Ransomware Families and Detection Methods

Helen Jose Chittooparambil[1], Bharanidharan Shanmugam[1(✉)], Sami Azam[1], Krishnan Kannoorpatti[1], Mirjam Jonkman[1], and Ganthan Narayana Samy[2]

[1] College of Engineering, IT and Environment, Charles Darwin University, Casuarina, Australia
Bharanidharan.shanmugam@cdu.edu.au
[2] Advanced Informatics School, Universiti Teknologi Malaysia, Kuala Lumpur, Malaysia

Abstract. Ransomware has become a significant problem and its impact is getting worse. It has now become a lucrative business as it is being offered as a service. Unlike other security issues, the effect of ransomware is irreversible and difficult to stop. This research has analysed existing ransomware classifications and its detection and prevention methods. Due to the difficulty in categorizing the steps none of the existing methods can stop ransomware. Ransomware families are identified and classified from the year 1989 to 2017 and surprisingly there are not much difference in the pattern. This paper concludes with a brief discussion about the findings and future work of this research.

Keywords: Ransomware classifications · Peta · Virus · WannaCry Cybersecurity

1 Background

Ransomware, also known as crypto virus, has received significant attention among cyberspace researchers in the last few years. Intruders use these malwares to steal people's private information with the help of vulnerabilities, including previous malware attacks, and threaten the victim to agree to their demand or they will lose their valuable files, data or private information. The ransom or demand may be e-gold, cryptocurrency or demands to purchase from designated stores. Ransomware is not a new concept, the first ransomware appeared in 1989 named as the PC CYBORG (AIDS) Trojan. It was delivered electronically through a floppy disk and the floppy disk was then used to attack a system [2]. Modern ransomware attacks started in 2005 with "Trojan.Gpcoder".

A malware is considered ransomware only if a minimum of three anti-virus vendors have assigned malware labels and categorised it as ransomware. The ransomware and malware can be differentiated by their attacking behaviour [1] and time taken for the attack. Malware attempts to hide behind applications, but ransomware initiates an attack immediately after installation. Ransomware is created for direct revenue generation, it often uses a countdown clock to alert the victim about the remaining time for paying the

F. Saeed et al. (Eds.): IRICT 2018, AISC 843, pp. 588–597, 2019.
https://doi.org/10.1007/978-3-319-99007-1_55

ransom. The first ransomwares displayed advertisements, but advancements in malware made it possible to block services, disable keyboards and spy on user activities [3].

During a ransomware attack, attackers use system vulnerabilities to intrude into the compromised device. The attacking probability of already attacked devices is always high. In most cases, major ransomware attacks occur on windows machines, but they can also attack android, Linux and IOS devices [4]. The ACSC 2015 Threat Report states that ransomware campaigns against Australian organizations will continue to be prominent. Every sector experienced a cyber security incident, which demonstrates the indiscriminate targeting and the sophistication of this type of threat. The number of ransomware incidents has drastically increased and is now four times higher than recorded in 2013. In 2015 the FBI received around 992 complaints regarding ransomware with the victims losing an estimated $18 billion.

Existing research's [13, 14, 21, 23] indicates that attacks of ransomware are difficult to detect or stop from occurring. The scope of this research is to understand operation of ransomware within Microsoft Windows operating systems by analysing the five-stages of operation of ransomware. In the next section, the evolution of ransomware and how the ransomware operates within a device is discussed. Section three of this paper will discuss the three families of ransomware and the five stages of the attack process. Section four discusses the evolution of ransomware and section four will elucidate the different ransomware detection methods. The last section will conclude with findings obtained from this study and recommendations for future work.

2 Literature Review

2.1 Review Stage

The main motive of introducing ransomware into the cyber world was to obtain financial gain by threatening people. There is no connection between the ransomware and the victims, but previous research shows that people who browse through unwanted websites are vulnerable to ransomware attack. The ransomwares can apply any kind of infection method that the malwares can use [5, 6, 21]. Ransomwares could be broadly classified as follows (Fig. 1) and the scope of this research is highlighted.

Scareware: This is a threat which takes advantage of people's fear. It is also known as rouge security software and was initially not considered a member of ransomware family. However, the increasing level of popularity of this malware has led to the classification of scareware within the family of ransomware. The scareware shows a message which states that the virus attacked the victim's system and it attempts to convince the victim to buy antivirus software which should remove the virus. Usually, these viruses are fake, and the antivirus software is non-functional malware [1, 8].

Lock Screen Ransomware: The lock screen ransomwares lock the victim's system until a ransom is paid for the lock key to retrieve it. It generally locks the desktop of a victim and creates a new window [9] which is used to communicate with the victim. The command and control server then control the victim's system and the new window shows messages about the ransomware threat and possible ways to unlock the system.

Crypto Ransomware: The most dangerous ransomware family is the crypto ransomware family. The ransomware encrypts the victim's files using strong encryption algorithms. In most cases cyber criminals make their own crypto systems. It is very difficult to retrieve the data back if the ransom is not paid within the period. CRYPTOLOCKER [10] is an example for the crypto ransomware which encrypts user files using a private encryption key.

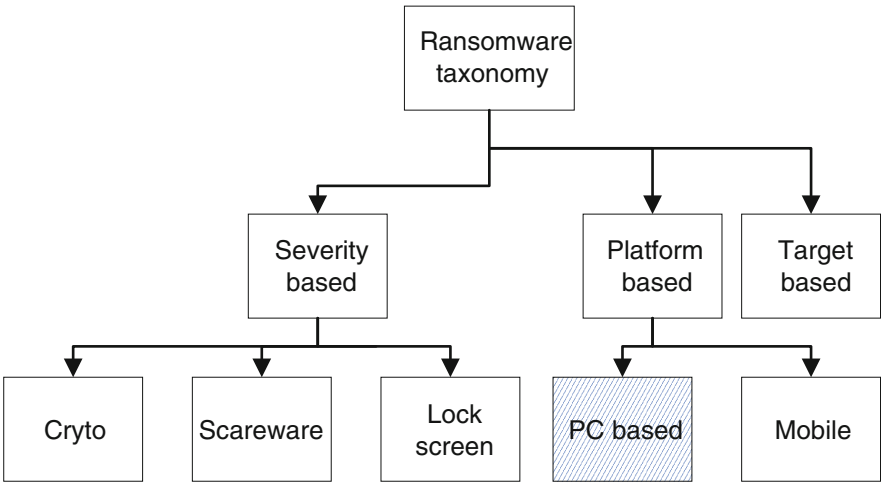

Fig. 1. Ransomware taxonomy [21]

However, the main advantage of this ransomware is that it stores the private key within the victim's system, so that further analysis can be used to access this private encryption key and retrieve the data. Reveton, otherwise also called Trojan: W32/Reveton, is an example of scareware which appeared to take control of the infected machine until the victim accepted the demand [20]. Using the RSA-2048 algorithm, file encryption ransomware encrypts the victim's documents and displays a message demanding money on the screen of the attacked device. In addition, it will also create a new instance of EXPLORER.EXE AND SVCHOST.EXE to make communication with the command and control server of the criminals [19]. Once the installation has occurred, the crypto wall will start to delete the shadow copies of files and install spyware to steal passwords saved on the victim's device as well as bitcoin wallets [22]. No machine is free from ransomware attack; mobile devices are vulnerable too. Fake messages imitating legitimate sources, which offers gifts and vouchers traps people to download ransomware executables. The latest and most effective Wannacry ransomware appeared in 2017 [18] and targeted Microsoft Windows operating systems. A ransomware attack of a system is generally defined five stages [11], refer to Fig. 2.

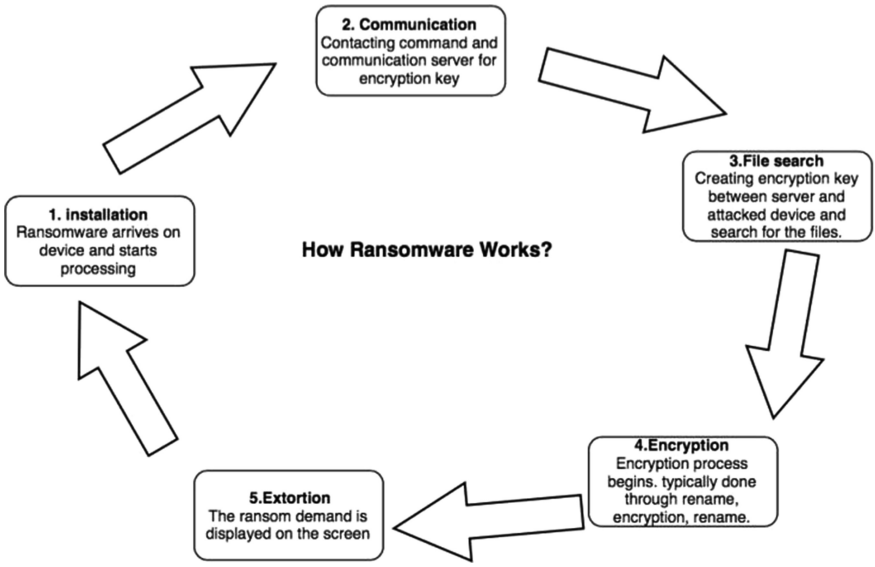

Fig. 2. Five stage process of Ransomware

2.2 Installation

The installation sets up the ransomware in victim's system and creates an environment to work in. Most ransomware hide behind the root path of the AppData or in the local AppData folder. During the installation execution, it randomly creates a file name inside the AppData folder [7]. Prior to that it will delete the original executable files available in the system. After creating the new file, it will then update the registry key files, containing information about tuning parameters, system configurations and user preferences, with the new registers on the device.

The modification of registry key files is done to obtain persistence of the device unless it reboots. Such persistence is obtained by executing an auto run process of registry keys that enables the malware to perform their execution while the device runs in a safe mode. Finally, to delete the shadow copies, the ransomware hijacks most of the executable files of that specific device.

2.3 Communication

For a complete ransomware attack, the ransomware needs to contact a command and control server. One possible way to establish the connection between the victim's device and command and control server is through a TOR network. After the installation of the ransomware file, the device will communicate with the command and control server to obtain the encryption key. Then using this encryption key, the ransomware will encrypt the selected files on the victim's device. To initiate the process, a communication setup has to be executed on the victim device to begin the communication between the command and communication server and the victim's device.

Then a domain is hosted to reach out the ransomwares by a Domain Generating Algorithm (DGA) [7]. These algorithms can generate a list of pseudo random domain names and are able to create thousands of command and control domains on a daily basis. The main advantage to the attackers of creating such domains is that they are very difficult to be shut down.

2.4 File Search and Encryption Process

Encryption is the major process for the crypto ransomware. For the encryption procedure, the server needs to generate an encryption key between the victim's computer and the command and control server. This differs in symmetric and asymmetric encryption, where in the symmetric encryption the same secret key is used for both encryption and decryption. In asymmetric encryption, a private key known only by the owner is used as well as a public key. The encryption method uses the public key and the decryption method uses the private key. The keys are protected using different methods [10]. The public key is embedded into the ransomware or obtained from the command and control server and it is then used to encrypt the symmetric key. After encryption, the key is stored in the infected system [12]. After obtaining the encryption key, the encryption procedure begins. The sender encrypts the plain text using the public key and on the receiver side the text is decrypted using the private key. The files are encrypted using the server generated encryption key and removes the original file. The encryption method is used to secure the communication channel between the ransomware and the command and control server. The dual encryption method is used because of performance and convenience. In some processes the ransomware uses individual keys per file [8], so breaking that key would only give access to that file. After initiation, the ransomware will create an encrypted copy of the original file and attempts to destroy all copies of the original ones. It renames the encrypted copy with the original file name with some extensions added.

2.5 Extortion

In the final stage, a ransom is demanded and displayed on victim's system [6]. There will be a time limit to pay the ransom before the criminals destroy the decryption key. They might use different payment methods for ransom payment. Certain ransomware will allow you to decrypt one file for free to assure you that the key is valid on your device. One type of payment is through Bitcoins, which may be an anonymous payment. More recent ransomware proceeds to delete files to threaten you in paying the ransom quickly. But there is no guarantee that the key they provided will help you to decrypt your files. There are ways in which the time for paying is set in the victim's device. The CMOS can be used as countdown for payment so that even if the user goes offline it will monitor the time limit. The ransom often increases automatically after a given time limit for the payment and updates this with the command and control server.

3 Ransomware Evolution and Detection Methods

The attack of ransomware is not new, and the first ransomware attack occurred in 1989 by ransomware named "PC cyborg", which belongs to the crypto ransomware family. The next major attack occurred five years later in 1994 by the ransomware named the OneHalf virus. In 2004, the "GP coder" marked the beginning of the crypto ransomware attack era. From 2011 to 2013. RansomLock however, was from the so-called locky ransomware family. The attack rate of ransomware steadily increased in the following years. In 2014, Bucbi, TorrentLocker, CryptoWall, CryptoDefence, Cryakl, Reactor, CTB-Locker, CryptoGraphiLocker, Cryptowall2, CryFile, KetBTC, BandarChor, Virlock, KEYHolder and Operation Global 3 appeared. In 2015 thirty-five ransomwares appeared. The major ransomware attacks occurred in 2015, 2016 and 2017 as illustrated in Fig. 3 below. Ransomware attacks and the evolution of new ransomware families have increased due to the success of ransomware attacks.

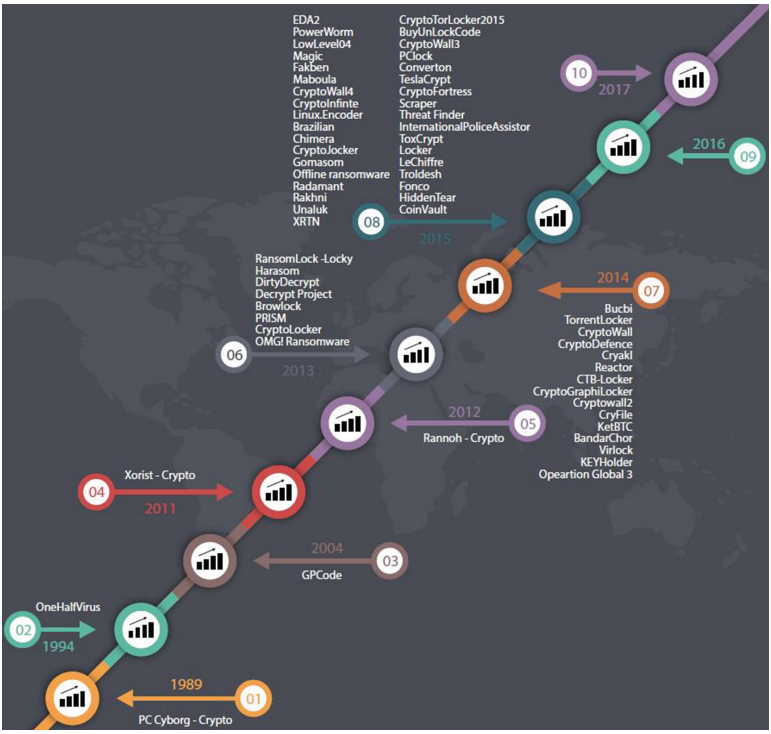

Fig. 3. Ransomware timeline

3.1 Study of Existing Methods

In the UNVEIL method [13], researchers analysed and detected ransomware attacks and modelled the behaviour using a dynamic analysis methods. To monitor how the ransomware interacts, an artificial but realistic execution environment is used which is created by the system automatically [13]. Then the interaction process with the file system is closely monitored to precisely characterize the cryptographic behaviour of the ransomware. The UNVEIL method flags suspicious behaviour as "like ransomware" and the operation of the ransomware is then identified to differentiate different classes of ransomware. UNVEIL uses two steps: the first step is to generate a user environment and the second step is to monitor file system activity [13]. Wecksten et al. [14] analysed four crypto ransomwares in a virtual machine with a Windows 7 operating system. For the investigation, the Cryptowall, Tesla Crypt, CTB Locker and Locky ransomware were used and the infection has been analysed using zeltzers [14]. In addition, the researchers used the software process monitor and regshots for tracking the process activity, file system activity and registry manipulation. This experiment identified that the crypto ransomware attacks are dependent on software named vssadmin.exe in the victim's device [14]. They claim that the attack can be easily prevented by avoiding access to the vssadmin.exe software. The remaining experiment was conducted by renaming the vssadmin.exe with shadow copies being created. Because of this prevention method, the ransomware could not find the restore point which was created before infection and that made it possible to restore all the information [14]. Moore [15] tried to detect the ransomware using a honeypot folder. The honeypot folder is created to monitor the changes occurring in the folder [15]. In addition, the Microsoft File Server Resource Manager feature was used for the file screening service and the Event Sentry was used to manipulate the Windows security logs [15]. This alert can then assist the system administrator to prevent further damage to the system [15].

The main aim was to determine a suitable ransomware detection method and to deploy an additional layer of security to the network to protect network actions rather than shutting down a server for the user when trying to update a file. When the first detection of a change has been encountered, a trigger would occur [15]. This was used to look for the email that caused the change in the monitored folder. If more activity was then encountered, the second hierarchical level was triggered. In the third hierarchical stage, the intensity of activity results in terminating the network service [15]. And finally, the fourth stage occurs when a final threshold of changes has been encountered. At this point, alerting the administrator and blocking the users access was not enough to stop the spread of damages, and therefore the ultimate protection would be to shut down the server [15].

Scaife et al. [16] present an early detection system, CryptoDrop, to alert a user during suspicious file activity. It can halt a process that appears to be tampering with a large amount of the data using a set a of behaviour indicators. Then the system can be parameterized for rapid detection with low false positives by combining a set of indicators common to the ransomware [16]. This research indicated that careful analysis of the behaviour of ransomware can detect it and can mitigate significant loss of data. By doing so, an early warning system has been created that can detect the malicious program through monitoring of the user's data [16]. Each ransomware uses

their own algorithm to perform these specific activities. The character of ransomware can be divided into three classes [16]. The first class includes the generic behaviour of ransomware. The renaming behaviour can also be added within this class. In the second class, the ransomware moves the files out of the user's documents directory, then it reads the contents within the file, writes the encrypted contents for each file, and moves the file back to the directory [16]. Renaming can also occur with this second class of ransomware, i.e. when the files are moved back into the directory, the name of the file may be different. The third class of ransomware reads the original file to create a new independent file containing the encrypted contents. It then deletes or overwrites the original file and its shadow copies [16]. For the analysis, a set of data was built representative of measured user document directories. The distribution of file types over the entire file system and document directories was examined. A document corpus of 5099 files with 511 total directories was constructed [16]. Data was then randomly selected from different data sets and placed in different directories. For placing the directory tree, a user's document folder was placed in a cuckoo sandbox running on a Windows 7 machine. The amount of data loss was used as metric to detect the ransomware attack [16]. By detecting the attack early, further attacks were controlled, and the remaining unaffected data was saved. Also, the frequency of file format attacks was calculated. The results showed that ransomware preferred to attack productivity files rather than the media files such as pictures and music [16].

3.2 Evaluation of Existing Methods

Using the UNVEIL method [13], attackers can easily identify the automatically generated user environments and this approach will make it easier for the ransomware to hook with the documents and specific operations in the operating system. Also, most of the ransomware will never encrypt the files in the same locations. The ransomwares will try to shuffle the files and will change the master file system. By making the file unreadable, changing the file names and extensions, it is very difficult for the victim to identify which files are encrypted. The ransomwares can also lock the monitor and will take the rights from the victim. Clearly, it is not possible to analyse and stop the ransomware using file system activity. The novel method described in [14] is only effective when it repairs the damaged structure. The local hard drive would be unusable or permanently damaged at file system level. And the researchers also declared in this article that the presented solution might not be the most suitable one. They highly recommended implementing a proper backup at regular intervals to save all the information in another place.

The honey pot technique [15] can be used to detect a ransomware attack, however this method only focusses on the honeypot folders. In the early detection method [16, 23], the high latency creates an operation so that the file is often locked and cannot be opened by the ransomware. So, the possibility of saving the data files from further attack is also reduced using this technique. Table 1 presents the ransomware detection of the reviewed methodologies over the processing of ransomware. Various approaches have been used to detect ransomware attacks, however there is no method detected all stages. Table 1 represents the ransomware detection of the reviewed methodologies over the processing of ransomware. All these methodologies are focused on

ransomware detection based at system file level. Monitoring changes from file levels has significant disadvantages. The ransomware attack process is going through five different stages and the file encryption process starts in the fourth stage. So, further investigation is required to identify the best solution that meets the requirements such as identifying the ransomware attacks from its previous stages.

Table 1. Ransomware detection methods

Process → Existing works	Installation	Communication	File search	Encryption	Extortion
UNVEIL [13]	N	N	Y	N	N
Mattias et al., [14]	N	N	Y	N	N
Honeypot Techniques [15]	N	N	Y	N	N
Cryptolock [16]	N	N	N	Y	N
Behavioral analysis [23]	N	Y	Y	N	N

4 Conclusion and Future Work

Ransomware attacks will continue to increase because of the increased use of the Internet. In this paper, three different families of ransomware and five-stages of operation of the ransomware are identified. Section three portraits the evolution of ransomware by showing the time line from 1989 to 2017. The monitoring of ransomware processes and operating systems activity is an effective method to find solutions for ransomware attacks. But from the evaluation of the existing methods we can conclude that none attempt to detect or stop the ransomware in the initial two stages. Detection at a later stage will increase the impact of ransomware attack, so that a solution to detect ransomware from its initial two stages is desirable to reduce the impact of ransomware. Future work of this research focuses on closely monitoring each stage of live ransomwares which attack Microsoft Windows operating systems in a controlled test environment. By allowing the ransomware to attack a device we can identify the ransomware processes, how it attacks operating system and finally the impact of the ransomware attack.

References

1. Luo, X., Liao, Q.: Awareness education as the key to ransomware prevention. Inf. Syst. Secur. **16**(4), 195–202 (2007)
2. Kharraz, A., Robertson, W., Balzarotti, D., Bilge, L., Kirda, E.: Cutting the Gordian Knot: a look under the hood of ransomware attacks. In: Detection of Intrusions and Malware, and Vulnerability Assessment, DIMVA (2015)
3. Monika, P.Z., Lindskog, D.: Experimental analysis of ransomware on windows and android platforms: evolution and characterization. Procedia Comput. Sci. **94**, 465–472 (2016)

4. Sjouwerman, S.: Ransomware In YouTube Ads, Techtalk.pcpitstop.com, 2014 (2016). http://techtalk.pcpitstop.com/2014/08/26/ransomware-youtube-ads/. Accessed 14 June 2018
5. ACSC 2015 report, 2015 Cyber Security Survey: Major Australian Businesses, Australian Government, Canberra (2015)
6. Mercaldo, F., Nardone, V., Santone, A.: Ransomware inside out. In: 2016 11th International Conference on Availability, Reliability and Security (ARES). SBA Research, Austria (2016)
7. Melendez, M.: Ransomware: An Analysis of a Growing Threat Landscape, Order No. 1605452. Utica College, Ann Arbor (2015)
8. Haas, P.D.: Ransomware Goes Mobile: An Analysis of the Threats Posed by Emerging Methods, Order No. 1586729. Utica College, Ann Arbor (2015)
9. Puodzius, C.: How encryption molded crypto-ransomware, WeLiveSecurity (2017). https://www.welivesecurity.com/2016/09/13/how-encryption-molded-crypto-ransomware/. Accessed 14 June 2018
10. Hampton, N., Baig, Z.A.: Ransomware: emergence of the cyber-extortion menace. In: 13th Australian Information Security Management Conference, Australia, pp. 47–56 (2015)
11. Wyke, J., Ajjan, A.: The Current State of Ransomware, SophosLabs (2015)
12. Brewert, R.: Ransomware attacks: detection, prevention and cure network security, pp. 5–9 (2016)
13. Kharaz, A., Arshad, S., Mulliner, C., Robertson, W., Kirda, E.: 25th USENIX Security Symposium (USENIX Security 16), 1st edn., pp. 757–772. USENIX Association, Berkeley (2016)
14. Wecksten, M., Frick, J., Sjostrom, A., Jarpe, E.: A Novel Method for Recovery from Crypto Ransomware Infections, p. 1354 (2016)
15. Moore, C.: Detecting Ransomware with Honeypot Techniques. In: 2016 CCC, Jordan, p. 77 (2016)
16. Scaife, N., Carter, H., Traynor, P., Butler, K.R.B: CryptoLock (and Drop It): stopping ransomware attacks on user data. In: 36th International Conference on Distributed Computing Systems (ICDCS), p. 303 (2016)
17. Sterling, B.: Ransomware: the basics, WIRED (2017). Accessed 14 June 2018
18. Mathews, L.: WannaCry Ransomware Situation Gets Worse as Copycats and Fake Decryptors Appear, Forbes (2017)
19. Constantin, L.: IDG News Service, "Widespread exploit kit, ransomware program, and password stealer mixed into dangerous malware cocktail Cybercrime group combines Pony, Angler and CryptoWall 4.0 in a single campaign" (2015). https://www.pcworld.com/article/3012112/security/widespread-exploit-kit-password-stealer-and-ransomware-program-mixed-into-dangerous-cocktail.html. Accessed 14 June 2018
20. Bacani, A.: REVETON Ransomware Spreads with Old Tactics, New Infection Method. In: TrendMICRO (2014). Accessed 14 June 2018
21. Al-rimy, B.A.S., Maarof, M.A., Shaid, S.Z.M.: Ransomware threat success factors, taxonomy, and countermeasures: a survey and research directions. Comput. Secur. **74**, 144–166 (2018)
22. Shanmugam, B., Azam, S., Yeo, K.C., Jose, J., Kannoorpatti, K.: A critical review of Bitcoins usage by cybercriminals. In: 2017 International Conference on Computer Communication and Informatics (ICCCI), Coimbatore, pp. 1–7 (2017)
23. Hampton, N., Baig, Z., Zeadally, S.: Ransomware behavioural analysis on windows platforms. J. Inf. Secur. Appl. **40**, 44–51 (2018)