remote sensing

MDPI

Article

A Survey on Situational Awareness of Ransomware Attacks—Detection and Prevention Parameters

Juan A. Herrera Silva *,†, Lorena Isabel Barona López *,†, Ángel Leonardo Valdivieso Caraguay † and Myriam Hernández-Álvarez †

Departamento de Informática y Ciencias de la Computación (DICC), Escuela Politécnica Nacional, Ladrón de Guevara E11-25 y Andalucía, Edificio de Sistemas, Quito 170525, Ecuador; angel.valdivieso@epn.edu.ec (Á.L.V.C.); myriam.hernandez@epn.edu.ec (M.H.-Á.)

* Correspondence: juan.herrera@epn.edu.ec (J.A.H.S.); lorena.barona@epn.edu.ec (L.I.B.L.)

† These authors contributed equally to this work.

Received: 9 March 2019; Accepted: 17 April 2019; Published: 16 May 2019

Abstract: In recent years, cybercrime activities have grown significantly, compromising device security and jeopardizing the normal activities of enterprises. The profits obtained through intimidation and the limitations for tracking down the illegal transactions have created a lucrative business based on the hijacking of users' files. In this context, ransomware takes advantage of cryptography to compromise the user information or deny access to the operating system. Then, the attacker extorts the victim to pay a ransom in order to regain access, recover the data, or keep the information private. Nowadays, the adoption of Situational Awareness (SA) and cognitive approaches can facilitate the rapid identification of ransomware threats. SA allows knowing what is happening in compromised devices and network communications through monitoring, aggregation, correlation, and analysis tasks. The current literature provides some parameters that are monitored and analyzed in order to prevent these kinds of attacks at an early stage. However, there is no complete list of them. To the best of our knowledge, this paper is the first proposal that summarizes the parameters evaluated in this research field and considers the SA concept. Furthermore, there are several articles that tackle ransomware problems. However, there are few surveys that summarize the current situation in the area, not only regarding its evolution but also its issues and future challenges. This survey also provides a classification of ransomware articles based on detection and prevention approaches.

Keywords: information security; prediction; ransomware; situational awareness

1. Introduction

According to [1], ransomware attacks have grown in recent years. In 2017, the number of WannaCry blocked attacks grew to 5.4 billion and the number of ransomware variants increased by 46 percent. The ransomware expansion has included new architectures such as Internet of Things (IoT), hospitals, police, among others [2], and even some attacks use ransomware as a decoy with the objective of cause disruption of services. In the middle of 2018, new ransomware families, like GandCrab, were emerging. At the international level, the United States (9%) and Russia (7%) have the greatest number of detected attacks. In 2018, the following ransomware families were widely spread: Alphacrypt, Jigsaw, Locky, Bat Rabbit, Cerber, Chimera, Petya, CryptorBit, Nemucod, CryptoDefense, NotPetya, CryptoLocker, CryptoWall, SamSam, TeslaCrypt, Torrentlocker, Gerber, VaultCrypt, WannaCry, among others [3].

The main reason for ransomware selection as an attack strategy is the economic benefit. The attackers request money to provide keys and recover the files and exploit the advantages of

crypto-coins to avoid being recognized. In 2016, the average demand for an infected host was $544 [4]. However, the economic damage of victims does not end there. In enterprise environments, a ransomware attack is considered as the most expensive thread because it can affect the central servers, causing productivity reduction and increasing the cost of cleaning processes. In 2017, the Nayana Web Hosting suffered the encryption of 153 servers disrupting 3400 costumer websites. The firm finally agreed to pay 397 bitcoins ($1 M), with this attack becoming the most significant reported payment [4]. However, in other attacks, the information is corrupted and cannot be recovered.

The content distribution services have also contributed to the dissemination of ransomware attacks. Today, the traditional e-mail service is the most common ransomware distribution channel. Botnets perform the spam campaigns and take advantage of social engineering mechanics to deceive users. The spam message can include a malicious link or either a malicious attachment that directly executes the ransomware. Similarly, the email can include an attachment that appears to be a legitimate file, but it begins a second stage that downloads the malicious code from a server and then executes it. Another dissemination strategy is exploit kits [4]. Although main security organizations announced a decrease of exploit kits, it rose again between May and June of 2017. In other words, the attackers take advantage of software vulnerabilities to download and install malicious software. For instance, an exploit kit can modify web servers to redirect traffic to infected advertisements or malicious links that contain ransomware. Additional dissemination methods include self-propagation, malvertising, brute-forcing passwords, sms messages, and third-party app stores. For example, EternalBlue is a famous exploit used in ransomware attacks. It was launched by Shadow Brokers group and takes advantage of a vulnerability of Server Message Block (SMB) in Microsoft computers. WannaCry ransomware exploits this vulnerability to compromise, load, and spread the malware to other machines. The attack uses SMB version 1 and 445 TCP port [5]. It is important to note that the new version of Windows 10 includes administrative tools such as PowerShell and Windows Scripting Host, which have access and privileges of system administrator. The current ransomware versions are exploiting these vulnerabilities.

Contrary to what is popularly believed, ransomware existed a long time ago. The first crypto ransomware, known as PC Cyborg, was born in December 1989 [6,7]. It used an initialization vector and a symmetric key to encrypt the files. Then, in 2004 emerged on the scene the locker ransomware (e.g., SMS, Fake FBI) and the first fake antivirus ransomware (Spysherrif, Performance Optimizer). In fact, the locker ransomware uses a different mechanism to lock the computer and then show a message to request a payment to get the key to unlocking the system. Meanwhile, fake antivirus deceives users with the promise to protect the system against viruses that do not exist or falsely improve computer performance. Simultaneously, the PGPcoder opened the new era of crypto ransomware due it executed a custom scheme to encrypt the data [6].

An additional remarkable variant is MBR ransomware (2010) because it was the first ransomware that does not encrypt a file, but it replaces the original Master Boot Record (MBR) with another code in order to lock the access to the system. In this case, the ransom message is displayed at computer boot-up time. In 2013, CryptoLocker appeared with file encryption of AES-256 and used TOR network to receive 2048 RSA for their Comand and Control server (C&C). Moreover, in 2014 the ransomware updated the payment method, including TOR-based bitcoin, to ensure anonymity. Furthermore, CTB-Locker replaced the typical proxy-based and botnet infrastructure for a new schema based on direct communication between C&C and TOR server. Then, Chimarea designed Bitmessage as their own P2P C&C messaging system based on public and private key encryption and replacing the TOR C&C model. Recently, WannaCry took advantage of old unpatched Microsoft Windows systems and acted as a worm in computers that did not perform security updates of the OS and reached 200,000 hosts over 150 countries [7]. In a nutshell, ransomware is continuously evolving and therefore, it can be considered a growing business that takes advantage of new approaches such as exploit kits and anonymous payments. Exploit kits are used for ransomware attacks, in a new model called ransomware as a Service (RaaS). Furthermore, ransomware has the ability to evade its detection through obfuscation of API calls, among others [8].

In this context, it is essential to know what happens in affected environments in order to facilitate contextual analysis. Cognitive and situational awareness concepts are considered a possible solution to this problem [9]. Situational Awareness model proposed by Endsley [10] defines three main stages in order to facilitate the analysis process and mitigate possible problems in a reactive and proactive way. Firstly, the identification and monitoring of incidents and specific parameters, not only of end devices but also network communications, allow gathering data that feed analysis and prediction phases. The second stage is focused on the correlation and analysis of collected data and the third stage provides the evolution of the whole environment through prediction and artificial intelligence methods. As a result, the application of Situational Awareness concept in ransomware environments could provide an efficient way to know how to avoid or mitigate possible attacks. Thus, there is an imperative necessity to define a set of parameters to be monitored according to Situational Awareness concept.

Nowadays, there are many studies not only focused on the ransomware chronology and taxonomy but also on proposals to detect and prevent this kind of attacks. On one hand, its contributions are only related to one field and therefore covers part of the ransomware issues and challenges. On the other hand, each of these proposals takes into account some parameters or information that will be analyzed in real or controlled environments. To the best of our knowledge, there are no surveys that provide a resume of these parameters and updated state of the art focused on prevention, detection, and prediction mechanisms. It is important to note that since the last ransomware attack happened on May 2017, the research community has put special attention in detection mechanisms that avoid information and large economic loss. With that in mind, the main contributions of this paper are listed below:

- Updated state of the art focused on analysis and prevention proposals and mechanisms that aid in preventing ransomware attacks in windows devices. It will be used as a starting point for future research.
- This paper is the first proposal that resumes the parameters that are taken into account in current investigations. This can lay the foundations to propose novel Ransomware Situational Awareness models.
- It provides open issues, challenges, and related methods that confront this kind of attacks.

This document is organized into six sections, the first one being the present introduction. Section 2 presents a summary of the evolution and the life cycle of ransomware and its relation with each phase of the Situational Awareness concept. Then, Section 3 shows an updated review of the whole analysis process, from the methods to prevent ransomware attack to detection and mitigation proposals. Section 4 describes the evaluated parameters in current ransomware research not only in prevention approaches but also analysis and detection models. Moreover, the main tools used in testing are presented. Section 5 discusses the main future trends and challenges. Finally, a discussion about the topic and conclusions is presented in Section 6.

2. Ransomware Life Cycle and Situational Awareness Model

The spreading of the Internet has brought some concerns about information security, especially related to the proliferation of different kind of malwares. In order to avoid or mitigate this threat it is important to know the ransomware life cycle, its relation to the situational awareness model, and its payment methods.

2.1. Ransomware Life Cycle

The ransomware life cycle can be described in seven steps, as follows:

1. Ransomware design
2. Ransomware dissemination
3. Ransomware arrival

4. Command and Control communication (C&C)
5. Search user's information
6. Encryption
7. Extortion and financial claiming

It is clear that these steps can be modified and depend on the type of ransomware. The most well known variations are fileCoder, which encrypts files, and lockScreen, which blocks computer access [3]. The lifecycle starts when the design or the objective is established and finishes when the kidnapping and extortion are done. The whole process is in Figure 1.

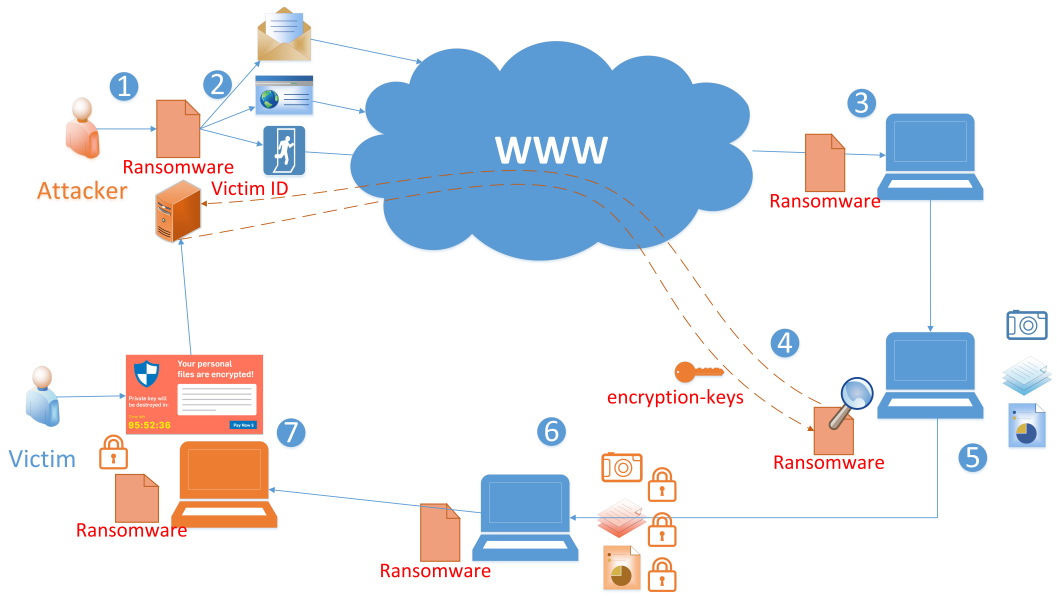

Figure 1. Steps of ransomware life cycle.

First, the developer creates a new version of ransomware. It can take advantage of the availability of several ransomware development kits (Torlocker, TOX, or Hidden Tear). Solutions such as RaaS have also provided an easy cloud platform for implementation and dissemination of new families of ransomware. This reality has enabled non-skilled individuals to collaborate on the design and creation of new ransomware versions.

Once the virus is ready, the attacker disseminates the ransomware looking for victims. The most typical infection vectors include phishing or spam e-mails, exploit kits (malvertising), downloader and trojan botnets, social engineering tactics, traffic distribution systems (TDS), among others. The infection vector can contain itself the ransomware code or malicious links to connect to a server and download the threat. Once it has arrived, the ransomware discovers the environment and gather user information. It identifies the host and generates a unique device ID. Then, the ransomware tries to connect to the C&C server to obtain an encryption key. In the fifth step, a malicious search process is executed. Commonly file extensions, such as docx, jpg, pptx, xlsx, among others, are searched.

Once the ransomware has the encryption code and the location of the victim files, the targeted files are encrypted. The original files are deleted and the encrypted files usually are renamed. Finally, the infected device executes a malicious process and displays the attacker financial claim. The message includes the payment instructions such as the kidnapping lifetime or the payment method (e.g., bitcoin transaction).

2.2. Ransomware Situational Awareness Model

The situational awareness model helps to know the real status of network and devices and facilitate the decision-making process. For this purpose, SA includes activities not only related to the

identification and monitoring of specific elements or parameters but also the aggregation, correlation, analysis, and forecasting activities. The decision-making process takes advantage of historical and new data in order to execute countermeasures over the compromised environment. The SA model proposed by Endsley [10] is based on three stages as follows:

- **Perception** This stage identifies and monitors specific assets and network parameters. It also reports ordinary events as well as new incidents. The perception phase gathers raw data related to the protected system. Then, this information must be organized in individual structures in order to facilitate the management and access of it.
- **Comprehension** Collected information is correlated and aggregated in order to simplify analysis and prediction tasks. Firstly, non-sensitive and redundant data are discarded and then a preliminary analysis is done.
- **Projection** This stage applies analysis techniques to forecast the behavior of the system and tracks its evolution. This phase takes into account countermeasures previously applied and their impact on the environment. Combining historical and current information proactive and reactive actions or responses are executed.

In this context, the combination of Situational Awareness with ransomware life cycle can aid to prevent or mitigate this kind of threat, as shown in Figure 2.

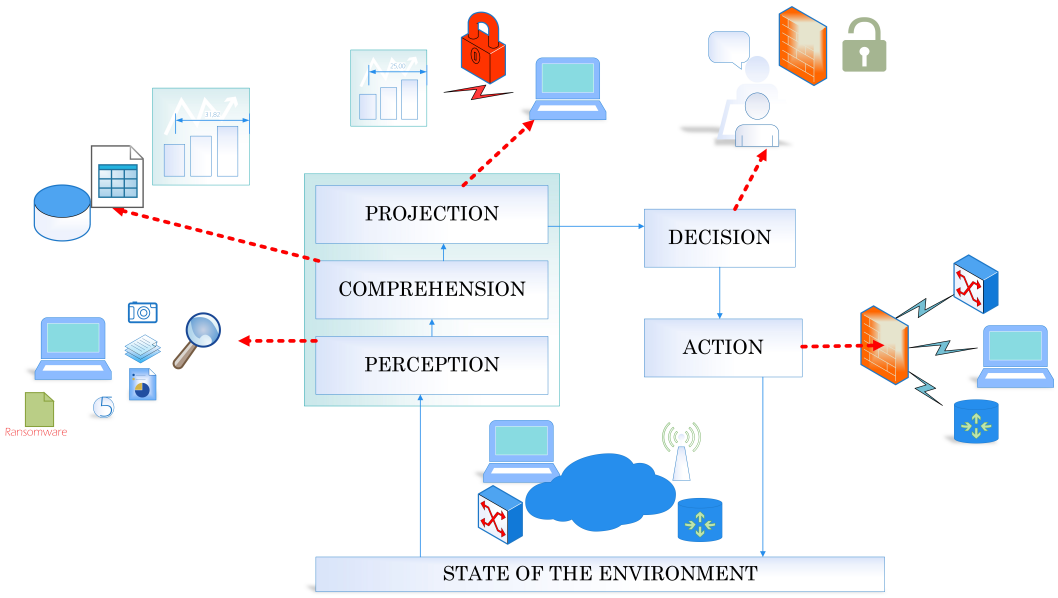

Figure 2. Endsley Situational Awareness Model and Ransomware Protection & Mitigation.

Firstly, the **Perception** layer is implemented in different tools responsible for gathering information. The obtained metrics can include C&C communications, filesystem activity, MBR communications, System API calls, among others. Then, the **Comprehension** layer uses the collected data to gain knowledge about the actual situation of the monitored elements. This is achieved through the use of interpretation, evaluation, and pattern recognition techniques. Since ransomware requires to gather user information, connect to the C&C server, obtain an encryption key, search for user files, its particular behavior could be detected. In this regard, given the complexity of ransomware attacks, there is an evident need for correlating different metrics in order to identify suspicious behavior. Meanwhile, the main objective of the **Projection** level is to take advantage of the actual knowledge of the system in order to make predictions about the future status of the analyzed elements. A reliable prediction is one of the most critical features in the context of ransomware attacks because it is difficult to recover the files once they are encrypted. Consequently, a timely and reliable prediction of a ransomware attack is fundamental to design an efficient, proactive response.

The **Decision** layer receives the projection ransomware alerts and establishes a response plan to avoid/mitigate the attack. The action plan depends on the access to different mitigation tools and the privileges to modify/reconfigure the system. For instance, it can include a new Firewall/IDS reconfiguration, insert a new rule in the switch to block suspicious packets, insert a honeypot in a specific network location, among others. In the **Action** layer, the action plan is executed. Depending on the network type, the actions can be accomplished in a specific point or in a distributed way. If the action plan is correct and the actions are correctly implemented, the **State of the Environment** of the system could avoid/mitigate the effect of a ransomware attack.

2.3. Payment Methods

In recent years, the success of ransomware as a method to illegally make money has been promoted by the arrival of new cryptography-based electronic currency [11]. Unlike traditional money transactions, the new digital currencies do not receive the control and monitoring of a centralized authority. Similarly, it provides ubiquity and fairness in real-time transactions. These digital currencies are kind enough to guarantee a certain level of anonymity. Consequently, cybercriminals take advantage of these features to expand their illegal activities.

Nowadays, bitcoin [12] is the most well known digital currency, although other blockchains have much higher transaction numbers (e.g., EOS). Bitcoin achieved popularity by promising users a fully decentralized currency. Satoshi Nakamoto is the nickname used by the person or working group that developed the idea of peer-to-peer electronic currency. The bitcoin payments are made using the bitcoin address as a unique identifier of the payment recipient. The payer creates a transaction message that includes the payee bitcoin address and the amount of transfer. Then, the transaction is authenticated through the digital sign (private key) of the corresponding address. Finally, the mining process confirms and broadcast the transaction. All confirmed transactions are registered in the blockchain and the chronological order is validated through cryptography. Consequently, the transaction is irreversible when the payment is confirmed.

The economic impact of ransomware depends on the circumstances of the attack, particularly its origin, ransom type, virus spread, the amount of demanded ransom, among others. With regard to the amount of ransom demanded, cybercriminals usually specify the ransom in bitcoins (1 BTC), or its equivalent in dollars. In 2016, the average rescue reached a value of USD 1,077.00 because the attackers believe they can get more income. However, the average real rescue demand has declined to settle at around USD 500.00 [4]. According to [11], CryptoLocker and CryptoWall received the maximum number of payments. The number of CryptoLocker payments is 51,766 BTC (USD 42,292,191), while CryptoWall reached 51,278 BTC deposits, equivalent to USD. 45,370,589.00. KeRanger and NotPetya reached minimal incomes of 4175.35 and 10,284.42, respectively. Regarding the origin of the attack, China (21%), EEUU (11%), Brazil (7%), and Russia (6%) lead the statistics of malware attacks, which include ransomware [1].

2.4. Current Research

The evolution and impact of ransomware attacks in the last decade have revealed the imperative need to discover an efficient way to mitigate or avoid this threat. In this context, there are several studies and proposals that aids with this purpose as is shown in Table 1.

Table 1. Summary of current research.

Reference	Year	Keywords/Topics	Kind of Research		
			Review	Proposal	Testing
[6]	2016	Detection, machine learning, Support Vector Machine (SVM), regularized logistic regression			X
[7]	2016	Ransomware evolution, datasets	X		X
[11]	2018	Ransomware economic impact, bitcoin trace	X		
[12]	2017	Economic analysis	X		
[13]	2017	Prevention, pattern, random forest, exploit kits, supervised machine learning			X
[14]	2016	Honeypot, detection		X	X
[15]	2017	C&C, IoT attacks	X	X	
[16]	2018	Detection methods, Decision Tree Classifier	X		X
[17]	2018	API calls, detection	X		
[18]	2017	Detection, V-detector negative selection algorithm, feature extraction			X
[19]	2018	Detection, prevention, entropy information			X
[20]	2018	Ransomware taxonomy, state of the art on prevention, detection and prediction.	X		
[21]	2018	Unsupervised detection method, artificial neural networks, Hardware Performance Counter (HPC).			X
[22]	2018	Detection, honey file, protection			X
[23]	2018	Detection, mitigation, Software Defined Networking (SDN)			X
[24]	2016	Detection mechanism			X
[25]	2017	Analysis and detection, simple Logic (SP), SVM			X
[26]	2017	Cryptoanalysis, detection	X		X
[27]	2017	Deep learning, Long-short term memory (LSTM)			X
[28]	2017	Crypto model, encryption keys, proactive prevention			X
[29]	2018	Dynamic analysis, anomaly detection, SVM			X
[30]	2018	Backups, disaster recovery, risk assessment	X		
[31]	2017	Deep networks, detection			X
[32]	2017	Recurrent neural network (RNN), detection			X
[33]	2018	Mitigation, detection	X	X	
[34]	2017	Ransomware evolution, safety measures	X		
[35]	2018	Detection, mitigation, SDN, NFVs		X	
[36]	2017	Crypto-Ransomware, bitcoin, Cybercurrency		X	
[37]	2019	Static analysis, opcode, Machine learning			X
[38]	2018	Security, model checking, android			X
[39]	2018	Bitcoin, crypto-currency, payment	X		
[40]	2018	Volatile memory forensics memory dumps			X
[41]	2019	Deep learning, convolutional neural network, LSTM			X
[42]	2018	Remote Desktop Protocol (RDP), detection			X
[43]	2018	Behavioral detection, anomaly	X		
[44]	2018	Detection, deception systems			X
[45]	2018	Real time detection, access control, file operation			X
[46]	2018	Encryptor, file protection, document editing			X
[47]	2017	Cyber threats, security audit, penetration testing, IoT, privacy	X		

Table 1 presents a summary of the different phases followed during an investigation. These are: the review of the state of the art, proposal, and testing. It also shows the keywords and central topics of each paper in order to facilitate future research. For instance, a ransomware taxonomy and its success factors are presented in [43]. This state of the art is focused on ransomware counteraction from the prevention approach as well as detection concept. It also highlights the research direction in this field and its impact [47]. Some authors show ransomware evolution, the most common infection, and payment methods [33,34]. They also present the kind of target users, safety measures, and the market model as a business. For instance, a ransomware economic analysis is carried out in [11,12]. In both approaches, the economic impact of ransomware is reported. They also provide an analysis of the payment strategies, such as bitcoins, and how they contribute to ransomware proliferation.

Moreover, a set of suggestions to enhance the information security risk assessment guidance, specifically NIST SP 800, is given in [30]. This study reviews the current backup approaches with the purpose of providing a guide in order to address ransomware attacks, according to NIST SP 800 security management. On the other side, there are proposals focused on ransomware in Android devices [7] or the IoT area [15]. For example, Zahnra et al. [15] proposes a model for analyzing incoming TCP/IP traffic (header), using a command and control server (C&C) with ransomware blacklists. It is important to note that the analysis of ransomware threats in Android or IoT devices is out of the scope of this article.

Furthermore, one of the most important challenges is to provide enhanced mechanisms to predict ransomware attacks before they happens and then apply countermeasures. On one hand, there are several articles that show novel detection and prediction methods [7,13,14,18]. On the other hand, some prevention mechanisms are presented in order to established some principles and suggestions to avoid a ransomware attack or loss of information [22,23,28,30]. In [28] a key vault to protect and store the session keys is proposed. Furthermore, there are some proposals that allow the mitigation of ransomware attacks, such as the deployment of sensors and actuators [35]. It takes into account the self-organized concept in order to provide a smart calibration and management of responses. It also considers the situational awareness concept to know the real situation of the protected environment.

It is important to highlight that big companies and organizations like the European Commission are pushing research in information security through funded projects such as RAMSES [48] or CYBECO [49]. On one hand, Supporting Cyber insurance from a Behavioral Choice Perspective (CYBECO) develops new tools and algorithms in order to build more secure communication and network systems. It takes into account the behavior not only of cyber attackers but also the owners of end devices or infrastructures. On the other hand, an Internet Forensic platform for tracking the money flow of financially motivated malware (RAMSES) facilitates digital forensic research in order to identify internet attackers or scams. For this purpose, the RAMSES project correlates and analyzes data gathered from the Internet, particularly malware attacks such as banking trojans or ransomware.

As a result of this preliminary analysis, there are different investigations that introduce concepts like a pattern recognition or prediction techniques in order to facilitate not only preventive actions but also reactive and proactive responsea behind ransomware attacks, as is detailed in the following sections.

3. Ransomware Analysis

Nowadays, the research community is working in novel methods and strategies for mitigating ransomware attacks, covering the whole analysis process to ensure information security in three main branches: prevention, detection, and prediction. The key idea behind these concepts is the diagnosis of the device state and prediction of possible attacks. Then, with gathered information, the best-suited countermeasures or actions behind suspicious events are decided. For this purpose, intelligent methods have been introduced in current research such as Bayesian Networks (BN), decision trees, Support Vector Machine (SVM), among others. Each of these branches is focused on a specific activity, as follows:

- **Prevention** This area is related to actions that are being used to avoid or minimize the possibility of a ransomware attack. These actions can include an updated operating system, the installation or use of a specialized application, among others. It also includes making file backups to avoid the extortion. The main objective of this phase is to close system vulnerabilities or security holes that were used in the past.
- **Detection** This phase intends to apply different mechanisms in order to detect ransomware attacks during or after it happens. The key idea of detection is to diagnose the end devices and then discover suspicious events or conditions. In this way, it is possible to avoid a possible attack in its initial phase, minimizing the impact on the system. Detection could also include both proactive and reactive responses.
- **Prediction** This area has the purpose of avoiding the attack before it takes place, which is achieved by means the gathering of different parameters or connections in end devices, then this information will be analyzed and correlated in order to predict possible attacks. One of the main pillars of prediction is the introduction of intelligent techniques. Based on prediction, the users can apply countermeasure to stop or avoid the attack.

In this context, this section presents the current research classified by prevention mechanism and detection/prediction approaches. It is worth mentioning that prediction and detection normally are used as interchangeable concepts. Some authors call the detection phase as "early prediction". This section also includes the description of these proposals and their characteristics.

3.1. Detection And Prediction

In order to know the real state of the end device and deploy countermeasures behind a suspicious event, it is essential to know what is going on and how to respond to this situation. In this context, the whole analysis process starts with the data gathering or feature extraction. In the detection phase, this information could be correlated and analyzed. Then, predictions can be done based on this set of metrics. Finally, if a relevant event is detected or predicted, a reactive or proactive response can be applied. Several proposals use different approaches and intelligent techniques in order to aid in the detection and prediction process. The first step consists of the feature extraction in network communications, registers, API calls, among others, and then classifies and analyzes them.

In this context, Gangwar et al. [13] proposed a mechanism to detect ransomware by means the analysis of patterns such as file paths, network activity, dropped file, ransom footprint, among others. For this purpose, different metrics were gathered through exploit kits. Then, the application payload was analyzed, including goodware and malware samples. Then, J48 Decision Tree, Random Forest, and Naive Bayes were used in order to classify these patterns. Furthermore, a dynamic analysis to detect ransomware on the user data observing the file system is proposed in [26]. This approach saves a registry with the file access rates, and at the same time the user activity is monitored in their own device through Process Monitor software. Registries, process activity, network, and entropy are parameters considered in the analysis process. The file system I/O accesses were recorded and execution screenshots were captured.

On the one hand, the research known as EldeRan [6] presents a mechanism for the dynamic classification of ransomware through some features such as Windows API calls, registry key operations, directory and file system operations, among others. Each user application is classified by means of a machine learning algorithm like a Logistic Regression classifier. Furthermore, this proposal also provides a method to create signatures for new ransomware family. On the other hand, an anomaly detection method to detect suspicious behavior is presented in [21]. This work is known as RAPPER and it gathers information from HPC statistics. Moreover, two approaches were taken into account, which are Artificial Neural Network and Fast Fourier Transformation (FFT).

Part of the current research analyzes the behavior of API calls. For example, Lu et al. [18] proposed a ransomware detection method based on V-detector negative selection algorithm combined with a mutation optimizer. This proposal takes into account three main features: API function calls (crypto,

processes, services), behavioral expressions (network, registers and directory operations), and memory. In [17], fourteen ransomware families are analyzed using API calls for Windows systems. This work characterizes ransomware behavior versus normal operations and then identifies specific API calls that have been used in ransomware infection. Similarly, Chen et al. [25] analyzed API calls by means of data mining algorithms such as Support Vector Machine (SVM) and Random Forest (RF), among others. The process includes four main phases: (i) raw feature extraction, (ii) preprocessing, (iii) selection, and (iv) analysis through learning algorithms. Moreover, in [27] long-short term memory is used in order to classify a binary sequence of API calls. The feature extraction was done by Cuckoo sandbox capturing API calls, file operations, and registry values. Other proposals [29,37] use a supervised machine learning approach in order to detect ransomware threats. In [29], each Window API call is counted and then the vector model is represented by an SVM algorithm. The collected logs contain not only Windows API calls but also process and communication status.

Some proposals use the honeypot concept in order to deploy a trap. In [14], some honeypot system approaches were presented in order to detect ransomware. It monitors a honeypot folder with an FSRM File Screen through the monitoring of Windows Event. The logs were caught by means of the EventSentry monitoring tool. UNVEIL [24] analyses the victim device in order to detect a ransomware attack. For this purpose, an artificial environment was deployed. It has special files (file lockers) that are monitored and deployed across the infrastructure. Some screenshots are taken in three phases: before, during, and after the attack is completed. The filesystem activity reflects changes in each I/O operation and their parameters such as timestamp, pointers to data buffers, etc. Furthermore, Gómez et al. [22] proposed a honey file as a mechanism to catch and response behind crypto ransomware attacks. It takes into account countermeasure actions in order to solve the possible infection. This action includes the file's lock when it is accessed.

Furthermore, there are some proposals that focus on the analysis or enhancement of encryption methods. For instance, Zavarsky et al. [7] performed a simple test to demonstrate ransomware detection using Cuckoo Sandbox and Anubis. For this purpose, it checks MD5 checksum values, register and file system activities, network communication, among others. Moreover, MD5 values are checked against the antivirus engine by means of the File Fingerprinting technique. In [28], enhanced file encryption, known as Paybreak, was proposed. The files are decrypted after they have been compromised by means of a hybrid encryption approach. PayBreak uses an asymmetric key pair that is saved in a secure key vault. On the one hand, the public key is configured with the user instructions. On the other hand, the private key is stored in a safe place. The system continuously stores the encrypted key pair in the vault. If the device is compromised, the vault is accessed with the private key.

Another method to characterize and detect ransomware threats is monitoring communication between the compromised devices and C&C server. In this context, NetConverse [16] introduces a machine learning method in order to detect a ransomware attack. This proposal extracts network traffic features such as IP address, packets, ports, protocols, among others. These features are extracted by means of a network analyzer tool called TShark. Meanwhile, Cabaj et al. [23] presented a ransomware detection method based on the introduction of the SDN concept. The main idea behind this proposal is the characterization of HTTP traffic and crypto ransomware communications, specifically CryptoWall and Locky. The communication is established between the infected devices and the proxy server. If suspicious behavior is detected, the SDN controller blocks the IP or domain. Furthermore, the SDN concept is also applied in [50]. This work tracks the behavior of crypto locker ransomware using asymmetric encryption. The time taken for file encryption will be observed (different data sizes) in order to mitigate the threat.

Nowadays, anti-ransomware tools are a good option in order to prevent this kind of threat. These tools must include the following characteristics: (i) detection of suspicious behavior, (ii) attack prevention, and (iii) remediation mechanisms. It is important to note that most of anti-ransomware

tools are able to detect, block, and restore encrypted files. The detection process is done by means of behavioral and forensic analysis [51].

3.2. Prevention

One of the main strengths for ransomware success is that the extortion or information kidnaping can be done with relatively low risk. Nowadays, there is not an easy way to follow the origin of the attack as well as the money trace. In this context, a feasible opportunity is that the users could be able to prevent the attack before it happens or the user can restore their original files. As a result, the user will be able to break the ransomware lifecycle. On one hand, there are some suggestions that can be applied in end devices in order to prevent or reduce the probability of suffering ransomware attack. On the other hand, there are some proposals that intend to prevent the information loss produced by these threats.

For instance, File Server Resource Manager (FRSM) is a mechanism of Windows Server (role service) that allows to classify and manage the information stored on servers. These capabilities include file screening, quote management, storage reporting, among others. Another example is presented in [14]. This research applies a honeypot to prevent a ransomware attack before it happens. For this purpose, two approaches are tested, which are file screening service and the monitoring of EventSentry. Moreover, in [52], four recommendations to prevent ransomware attack are presented: (i) backup, (ii) avoid email links and attachments, (iii) patch and update security software, and (iv) if the machine is infected, turn it off in order to minimize the damage. Similarly, Jung et al. [19] proposed a model to detect and respond behind ransomware attacks. It takes into account prevention and post-detection actions. The system consists of monitoring, detection/analysis, file backup (secure zone), and a gray list classification system.

After a ransomware infection, another interesting approach is the file recovery. For instance, PayBreak [28] prevents data loss through the storage of session keys in a protected key vault. Thus, only the legitimate user can access the information and is able to recover their own information. It is important to note that one of the main recommendations given by security companies is to take the public keys from trusted sources such as the public Certificate Authority (CA). This approach allows controlling suspicious or unauthorized encryption processes [53].

It is important to highlight that the main security enterprises and big companies provide suggestions and guides in order to prevent ransomware attacks, such as Microsoft [54] or Symantec [1]. Microsoft is able to monitor Windows security logs by means of EventSentry, which is a Security Information Management tool (SIM). When an activity passes a threshold, specific actions are triggered. In [55] a complete checklist and guide to prevent ransomware attack are presented.

Some preventive actions to avoid getting infected include making a periodic information backup, train the user, or create different privilege levels and segments. Making backups is a reactive measure that prevents losing information or having to pay the rescue. It is important to highlight that backups must be done outside of the network. Another big problem is the user habits, and therefore it is important to train all users and explain the risks and security threats associated with the use of computer and network resources. Moreover, each user must have an appropriate segment and level to access or control their resources and information. Segmentation controls the traffic between networks and isolates some critical services and resources [51,56].

Furthermore, prevention actions also include access control lists, regular backups, applying patches and updates, deployment of security products, enabling file recovery systems, disabling macros to remote control, limiting sharing options or unused wireless connections, using key vaults and inspect suspicious email or URLs, review shared and external resources, use anti spam, antivirus solutions, firewall and content filter (block some extensions considered dangerous), show file extensions (to detect malicious files with double extension), block advertising and pop-ups, and protect the MBR table, among others. Moreover, the right control of user permissions, stronger authentication mechanisms, and the implementation of best practices to remote desktop control are needed [43]. It is important to

note that prevention actions are only the first step to avoid information loss but it does not ensure that a ransomware attack compromises end devices. Moreover, the prevention suggestions come from the study of ransomware regarding detection and prediction research.

4. Evaluated Parameters on Current Research

One of the main challenges of information security is to know what happens with the devices connected in a system and their communications, and more importantly how to prevent and mitigate possible threats. All of these issues can be covered by means of a Ransomware Situational Model. In this context, there are several parameters taken into account in the current research such as file system operations, entropy, registry keys, checksum values, file hashes, disk usage, and open connections, among others. Table 2 shows a summary of different parameters that were studied and evaluated in current research. It also includes the tools used not only to deploy a secure environment for testing purposes but also the programs or approaches that facilitate the gathering, correlation, and analysis of the information.

The analysis presented in Table 2 has revealed that Cuckoo [57] sandbox is the preferred tool for testing and evaluation. Cuckoo allows the deployment of a secure environment for testing with a different kind of malware. When an attack is simulated, every action carried out by the malware is stored (logs and reports). One of the main advantages of Cuckoo is that it works in an emulated environment. It is worth mentioning that ransomware samples can be obtained in VirusTotal, VirusShare, or some authors generate or emulate their own ransomware. In essence, most of the authors take into account the following features:

- **Content similarity and entropy** It allows determining how similar the data is. Entropy is based on the degree of randomness of the bytes in a file. Typical file types, such as HTML or doc, have a lower entropy value compared with binary files (exe, dll). Encryption produces typically a high entropy. Therefore, if the file has been changed and it is too different in comparison with the expected average entropy, it can be considered a potential threat. It is important to note that a high entropy for itself is not a conclusive parameter to predict ransomware attacks because other normal processes like compression imply a high entropy value. Furthermore, newer versions of ransomware are reducing the entropy and, consequently, a lower value does not guarantee a possible infection. Entropy can be used as a part of an attack vector in order to predict ransomware threats.
- **Monitoring C&C Communications** In ransomware attacks, a C&C server propagates instructions in order to infect or take control of devices called bots. In this context, the monitoring of unusual or continuous communications with specific internet sites will be done. For this purpose, researches are using innovative technologies such as SDN in order to block the communication with the C&C server when it is happening. For instance, in [58] a system to monitor suspicious network traffic is proposed. It blocks infected devices, in a real-time manner, through rules applied by the SDN controller. Moreover, concepts like Network Function Virtualization (NFV) aid to mitigate this problem by means of the deployment of specialized network functions like Deep Packet Inspectors (DDI) or honeypots. Besides, Domain generation algorithms (DGA) generate a set of domain names that are used by the C&C server and leave a trace in network traffic [59]. It is important to note that some ransomware samples do not need an internet connection to encrypt files.
- **Filesystem activity** A ransomware inevitably uses function calls (e.g., I/O Requests) to execute malicious operations in the OS filesystem. The system under attack can exhibit an abnormal file system activity since a large number of equal file system access can be requested. The main suspicious activities related to the file system can include changes in Master File Table (MTF) and I/O Request Packets (IRP) [60]. During a ransomware attack, the MTF can be encrypted and the Master Boot Record (MBR) is overwritten. Thus, monitoring these elements is an effective strategy to detect ransomware.

- **Monitoring registry values** It has been observed that during a ransomware attack, several registry values are modified. For instance, many ransomware variants modify the values of HKEY_LOCAL_MACHINE\System\CurrentControlSet\control\N1s\ComputerName \ActiveComputerName and HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsNT \CurrentVersion \WinLogon, HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows \CurrentVersion \Run. Similarly, the value of HKLM\Software\Microsoft\Cryptography \Defaults\Provider Types\Type 001 as the Microsoft Strong Cryptographic Provider is read [7]. Other variants remove the volume shadow copies (Volume Snapshot services VSS files) in order to avoid the use of these backups to recover the system. Finally, ransomware opens a txt instruction file and fills it with the image of attacker payment information and changes the desktop background to the bitmap image. In other words, the HKCU\Control Panel\Desktop\Wallpaper value is set to %CSIDL_DESKTOPDIRECTORY%_Locky_recover_instructions.bmp [46]. In the case of encryption ransomware, crypto libraries and registers are used or accessed.
- **Privilege Escalation** It is considered one of the most distinctive features of ransomware attacks. Once the malicious software is downloaded on the system, it monitors the environment to check their access capabilities and, if necessary, asks for administration rights. This access request is externalized as an app authorization button in Android devices or a malicious window requesting authorization in Windows elements (update patch). Once the attack obtains administrator privileges, it continues the attack by locking the victim device (Windows) or setting a new lock screen PIN (Android).
- **Monitoring API and DLL calls** The use of APIs is one of the most common ways of software development. Through it, a set of procedures, protocols, and tools is provided as logical building blocks. The programmer puts the blocks together according to their particular objective through API requests and API calls. Similarly, the attacker uses the available APIs for executing malicious activities. Therefore, some characteristics of API calls (e.g., time, type, number, sequence) can be used to model the application behavior. Then, a classifier can be trained in order to detect suspicious activities. For example, a suspicious sequence in API Windows is the use of GetThreadDesktop, CreateDesktopW, and SwitchDesktop [60]. Even though the attacker could avoid the use of API calls, the use of native APIs requires significant work due to lack of compatibility and available documentation.
- **Modifications of Master Boot Record (MBR)** A group of ransomware attacks is specialized in changing the Master Boot Record, which contains the executable boot code and the partition table. This attack takes advantage of the well-known position of the MBR (first sector of a hard disk) and the startup procedure. Then the system boot process loads the MBR instructions in memory and transfers it to the control system at boot time. In this context, the malicious software modifies the boot code with a bogus MBR that blocks the normal boot procedure and displays a message requesting a ransom.
- **Monitoring specific file type, file path, or directories** It includes monitoring modifications of files to find out an unusual increase of specific extensions, such as .locky. It also oversees the Volumen Shadow Copy service (VSC) in order to avoid that shadow copies of the systems can be erased. Moreover, it is crucial monitoring URLs and web pages.

Table 2. Summary of evaluated parameters and tools.

Reference	Year	Evaluated Parameters	Tools/Datasets
[6]	2016	API invocations, registry keys, file directory operations, dropped files.	VirusShare, Cuckoo sandbox, VirusTotal, Matlab
[7]	2016	Filesystem and registry in Windows; checking the MD5 hash values from Virus, file system and register activity, network communications	PEiD, PEView tool, Cuckoo, Anubis
[14]	2016	Honeypot folder monitored with an FSRM File Screen	EventSentry, FSRM
[24]	2016	File path, time attributes, filesystem I/O activity	Cuckoo, OpenSSL, VirusTotal
[13]	2017	Listing of the file path and dropped file, ransom note, network activity, analyzing application payload	Cuckoo, Wireshark, tracewrangle3, Dionaea Honeypot
[15]	2017	C&C communication, public key, the connection established between victims and the C&C server.	Framework Proposal
[18]	2017	Hard disk reading and writing, the encryption and deletion of files, crypto APIs. Three types of features: API functions, behavioral expression (count IP address, ports, etc) and memory feature.	Cuckoo Sandbox, Volatility
[25]	2017	API calls (GetModuleFileNameA, NtCreateSection, NtCreateFile, NtMapViewOfSection, NtWriteFile)	API Monitor tool, Weka
[26]	2017	File system, registry, process activity, entropy, API functions (ReadFile, QueryInformation), Master File Tables, System Service Descriptor Table	bCuckoo, VirusTotal, Process Monitor
[27]	2017	API calls, registry values	Cuckoo Sandbox
[28]	2017	Crypto Function Hooking, CryptoAPI, File recovery, SHA1 functions	Cuckoo sandbox, Raddar, VirusTotal
[31]	2017	121 API call functions (NtEnumerateValueKey, NtOpenSection, closesocket, CryptDecodeObjectEx, GetFileAttributesW)	Cuckoo sandbox, TensorFlow, Open Malware, VirusTotal
[32]	2017	API call sequences (NtOpenFile, RegOpenKeyExA, ioctlsocket, NtResumeThread, etc)	Cuckoo sandbox, VirusTotal
[16]	2018	Network features (Protocol, source and destination address, ports, packets, duration)	Tshark, Weka, Kali Linux
[17]	2018	API calls (CopyFile, CreateDirectory), InternetOpen, CryptoDeriveKey, SetFileAttributes, GetFileType, GetFileSize, CryptoGenKey, CryptoDecodeObject)	Windows Power Shell, bash scripts, ProcMon
[19]	2018	The entropy value, of the file, was calculated (its format)	Watchdog Module
[21]	2018	Cache-references, cache-misses, branch-misses and branches.	iperf tool, sandbox, Kera,
[22]	2018	FIFO files, infinitive files	Bash-ransomware, linux suite, linux encoder, OpenSSL
[23]	2018	HTTP message sequences and their corresponding sizes.	Cuckoo, Alexa websites, POX
[29]	2018	API calls	Cuckoo sandbox

5. Future Trends and Challenges

Ransomware attacks can cause large disruptions in all kind of organizations. By implementing conventional practices like antimalware, they protect and defend their systems from known ransomware variants. However, the sophistication and continuous evolution of ransomware means that these strategies are not enough to identify and block new attacks. In this context, the detection of ransomware attacks is one of the most challenging objectives of researchers. It is clear that once the encryption is executed, the data is compromised and the damage is irreversible. For this reason, the detection of the ransomware (before encryption) is challenging. Today some solutions can detect the attack in the first phases, but it sacrifices the encryption of some files before the detection. To resolve this, one of the future trends includes ransomware prediction in order to detect the threat in the pre-encryption phase and stop the attack in time. Despite the fact that there are some ransomware prediction solutions, the experiments demonstrate that the false positive rate is still high (20%). In order to improve the accuracy and effective detection, the use of machine learning or statistical approaches is highly recommended. It aids in the identification of ransomware features and detect the initial phase of the attack.

The dynamic analysis based on patterns of system calls can help to differentiate a legitimate encryption software and a ransomware attack. For instance, the presence of cryptographic API calls used not only to obtain key containers but also to generate public and private keys is expected for the typical process of file encryption. Furthermore, the detection models could analyze the structural and operational behavior of the toolkits used to build ransomware attacks. Another interesting research area is the inclusion of honey-files deployed to catch and block the ransomware when it tries to read the files. The comparison of the file, before and after the attack, concerning entropy and similarity-based measurements, could give signals of a ransomware detection. It is also important the generation of new mechanisms to discriminate between a benign or malign attack by means of the combination, not only considering high or low file entropy value but also considering monitoring network and file system activity.

The performance of the ransomware detection process could be improved thanks to the use of a new generation of cloud-based ransomware detection services, particularly in devices with limited energy/CPU resources (mobile, IoT). It is worth mentioning that a lot of ransomware experiments do not follow standard approaches. For this reason, the need for consistently validated datasets would facilitate ransomware research. Additional future work includes the development of a knowledge base of the financial behavior of ransom monetary transactions. The use of data mining techniques to track down the money can help to become susceptible and expose adversaries.

The development of new network technologies has gained the attention of ransomware researchers and these can contribute to the analysis, detection, and prevention tasks of this kind of attacks. New network paradigms, such as Software Defined Networking (SDN) [61], Network Function Virtualization (NFV) [62], and Self-organized Networking (SON) [63], have changed the vision of private, closed, static network environments. The network administrator can create their own network programs (Network Functions), and customize the network behavior according to the user needs. In this context, the flows can be analyzed in order to detect suspicious network behavior and take preventive actions, such as redirect/block the traffic and track down the source of the attack.

The primary motivation of ransomware developers is the illegal revenues gained from the victim payments who choose to pay the ransom. In this context, the development of new solutions for data backup and recovery will make it possible for victims to recover their data without paying the ransom. The contribution of distributed computing backup and recovery systems, as well as a cloud-based recovery solution, can help to decrease the impact of ransomware attacks. As soon as the ransomware attacks become worthless, the interest in developing new hazards will decrease.

Finally, one of the main challenges is related to law enforcement. Nowadays, there are security holds because ransomware is based on anonymity. On one hand, the attack trace or the C&C server that controls the encryption process cannot be tracked easily. On the other hand, payment methods

like bitcoin allow hiding payment route. Thus, it is important to establish general legal agreements in order to prevent extortion.

6. Conclusions

Ransomware is one of the critical threats facing not only end users but also organizations. The number of enterprises and organizations affected by ransomware is growing and the financial losses and reputation damage are extensive. Also, the evolution of new markets and business models such as mobile communication, IoT, Cloud-based services, and the perception of anonymity provided by digital currencies have promoted the development of new variants of ransomware. Although the research community is working hard on novel methods to prevent and avoid ransomware attacks, there is a marked tendency towards the utilization of more cognitive mechanisms in order to gain real knowledge not only of end devices but also of network elements. The key idea is to find the right characteristics that have been changing in the system, allowing the identification of suspicious behavior and, consequently, the detection and prevention of threats. Ransomware attacks are not going to disappear in the medium term because they are carried out when the attacker discovers a new configuration weakness in end devices. For that reason, it is necessary to implement a progressive security strategy and discuss the legal issues in order to track this kind of attack. The community must be aware of the current situation in each country and how it could impact the third parties involved.

The primary objective of the present article is to facilitate the research work in this area through the presentation of updated studies that summarize the current investigations and show a holistic ransomware view. For this purpose, a complete description of the ransomware evolution, its life cycle, and its relation with the Situational Awareness concept are presented. It includes a complete description of the ransomware life cycle from the attacker's design and dissemination to the extortion of the victim. Similarly, a description of the common payments methods, like bitcoin, is included. Moreover, in order to facilitate the testing phase of future investigations, a detailed summary of several parameters that have been evaluated in the current research is introduced. To the best of our knowledge, the present contribution is the first work that covers this aspect. Furthermore, an updated state of the art in prevention, detection, and protection, as the main areas related to minimizing the impact of ransomware threats, is presented. The work concludes with an analysis of the main challenges and hot topics in the ransomware research field.

The internet has become a strategic ecosystem for different human activities, such as production, communication, entertainment, and economy, among others. Therefore, building and maintaining a secure digital network environment are a central topic in different research areas. Despite the fact that ransomware has evolved as one of the most common cybersecurity threats, the analysis and development of new prevention, detection, and protection methods will help to reduce the attacker revenues and decrease the incentive behind this illegal activity.

Author Contributions: The authors contributed equally to this work. They also read and approved the final manuscript.

Funding: Escuela Politécnica Nacional funded this research under grant agreement number PII-17-14 for the development of the internal research project "Ransomware a gran escala por medio de Seguridad Cognitiva", 2018.

Conflicts of Interest: The authors declare no conflict of interest.

Abbreviations

The following abbreviations are used in this manuscript:

BN	Bayesian Network
BTC	Bitcoin
CA	Certificate Authority
C&C	Command and Control
DGA	Domain Generation Algorithms

FRSM	File Server Resource Manager
HPC	Hardware Performance Counter
IRP	I\O REquest Packets
MBR	Master Boot Record
MFT	Master File Table
NFV	Network Function Virtualization
RaaS	Ransomware as a Service
RF	Random Forest
RDP	Remote Desktop Protocol
RNN	Recurrent Neural Network
SA	Situational Awareness
SDN	Software Defined Networks
SMB	Server Message Block
SON	Self-organized Networking
SVM	Support Vector Machine
TDS	Traffic Distribution System
VSC	Volumen Shadow Copy

References

1. Cleary, G.; Cox, O.; Lau, H.; Nahorney, B.; Gorman, B.; O'Brien, D.; Wallace, S.; Wood, P.; Wueest, C. ISTR 2018. *Internet Secur. Threat Rep.-Symantec* **2018**, *23*, 80–89.
2. Azmoodeh, A.; Dehghantanha, A.; Conti, M.; Choo, K.K.R. Detecting Crypto-ransomware in IoT Networks based on Energy Consumption Footprint. *J. Ambient Intell. Hum. Comput.* **2017**, *9*, 1141–1152. [CrossRef]
3. Eset, E. *ESET Security 2018*; Technical Report; ESET: Bratislava, Slovakia, 2018.
4. O'Brien, D. Ransomware 2017, An ISTR Special Report. Symantec. Available online: https://www.symantec.com/content/dam/symantec/docs/security-center/white-papers/istr-ransomware-2017-en.pdf (accessed on 5 April 2019).
5. Kumar, M.S.; Ben-Othman, J.; Srinivasagan, K. An Investigation on Wannacry Ransomware and its Detection. In Proceedings of the 2018 IEEE Symposium on Computers and Communications (ISCC), Natal, Brazil, 25–28 June 2018; pp. 1–6.
6. Sgandurra, D.; Muñoz-González, L.; Mohsen, R.; Lupu, E.C. Automated Dynamic Analysis of Ransomware: Benefits, Limitations and Use for Detection. *arXiv* **2016**, arXiv:1609.03020.
7. Monika; Zavarsky, P.; Lindskog, D. Experimental Analysis of Ransomware on Windows and Android Platforms: Evolution and Caracterization. *Procedia Comput. Sci.* **2016**, *94*, 465–472. [CrossRef]
8. Bajpai, P.; Sood, A.K.; Enbody, R. A Key-management-based Taxonomy for Ransomware. In Proceedings of the 2018 APWG Symposium on Electronic Crime Research (eCrime), San Diego, CA, USA, 15–17 May 2018; pp. 1–12.
9. Kelley, D. *Cybesecurity in the Cognitive Era: Priming your Digital Immune System*; Technical Report; IBM: Somers, NY, USA, 2016.
10. Endsley, M.R. Design and Evaluation for Situation Awareness Enhancement. *Proc. Hum. Factors Soc. Annu. Meet.* **1988**, *32*, 97–101. [CrossRef]
11. Conti, M.; Gangwal, A.; Ruj, S. On the Economic Significance of Ransomware Campaigns: A Bitcoin Transactions Perspective. *Comput. Secur.* **2018**. [CrossRef]
12. Hernandez-Castro, J.; Cartwright, E.; Stepanova, A. Economic Analysis of Ransomware. *arXiv* **2017**, arXiv:1703.06660.
13. Gangwar, K.; Mohanty, S.; Mohapatra, A. Analysis and Detection of Ransomware Through Its Delivery Methods. In Proceedings of the International Conference on Recent Developments in Science, Engineering and Technology, Gurgaon, India, 13–14 October 2017; Springer: Berlin/Heidelberg, Germany, 2017; pp. 353–362.
14. Moore, C. Detecting Ransomware with Honeypot Techniques. In Proceedings of the 2016 Cybersecurity and Cyberforensics Conference (CCC), Amman, Jordan, 2–4 August 2016; pp. 77–81.

15. Zahra, A.; Shah, M.A. IoT based Ransomware Growth Rate Evaluation and Detection using Command and Control Blacklisting. In Proceedings of the 2017 23rd International Conference on Automation and Computing (ICAC), Huddersfield, UK, 7–8 September 2017; pp. 1–6.
16. Alhawi, O.M.; Baldwin, J.; Dehghantanha, A. Leveraging Machine Learning Techniques for Windows Ransomware Network Traffic Detection. In *Cyber Threat Intelligence*; Springer: Heidelberg, Germany, 2018; pp. 93–106.
17. Hampton, N.; Baig, Z.; Zeadally, S. Ransomware Behavioural Analysis on Windows Platforms. *J. Inf. Secur. Appl.* **2018**, *40*, 44–51. [CrossRef]
18. Lu, T.; Zhang, L.; Wang, S.; Gong, Q. Ransomware Detection based on V-detector Negative Selection Algorithm. In Proceedings of the 2017 International Conference on Security, Pattern Analysis, and Cybernetics (SPAC), Shenzhen, China, 15–17 December 2017; pp. 531–536.
19. Jung, S.; Won, Y. Ransomware Detection Method based on Context-aware Entropy Analysis. In *Soft Computing*; Springer: Heidelberg, Germany, 2018; pp. 1–10.
20. Al-rimy, B.A.S.; Maarof, M.A.; Prasetyo, Y.A.; Shaid, S.Z.M.; Ariffin, A.F.M. Zero-Day Aware Decision Fusion-Based Model for Crypto-Ransomware Early Detection. *Int. J. Integr. Eng.* **2018**, *10*, 82–88. [CrossRef]
21. Alam, M.; Bhattacharya, S.; Mukhopadhyay, D.; Chattopadhyay, A. RAPPER: Ransomware Prevention via Performance Counters. *arXiv* **2018**, arXiv:1802.03909.
22. Gómez-Hernández, J.; Álvarez-González, L.; García-Teodoro, P. R-Locker: Thwarting Ransomware Action through a Honeyfile-based Approach. *Comput. Secur.* **2018**, *73*, 389–398. [CrossRef]
23. Cabaj, K.; Gregorczyk, M.; Mazurczyk, W. Software-defined Networking-based Crypto Ransomware Detection using HTTP Traffic Characteristics. *Comput. Electr. Eng.* **2018**, *66*, 353–368. [CrossRef]
24. Kharraz, A.; Arshad, S.; Mulliner, C.; Robertson, W.K.; Kirda, E. UNVEIL: A Large-Scale, Automated Approach to Detecting Ransomware. In Proceedings of the USENIX Security Symposium, Austin, TX, USA, 10–12 August 2016; pp. 757–772.
25. Chen, Z.G.; Kang, H.S.; Yin, S.N.; Kim, S.R. Automatic Ransomware Detection and Analysis Based on Dynamic API Calls Flow Graph. In Proceedings of the International Conference on Research in Adaptive and Convergent Systems, Krakow, Poland, 20–23 September 2017; pp. 196–201.
26. Kardile, A.B. Crypto Ransomware Analysis and Detection Using Process Monitor. Ph.D. Thesis, UT-Arlington, Arlington, TX, USA, 2017.
27. Maniath, S.; Ashok, A.; Poornachandran, P.; Sujadevi, V.; Sankar, A.P.; Jan, S. Deep Learning LSTM based Ransomware Detection. In Proceedings of the 2017 Recent Developments in Control, Automation & Power Engineering (RDCAPE), Noida, India, 26–27 October 2017; pp. 442–446.
28. Kolodenker, E.; Koch, W.; Stringhini, G.; Egele, M. PayBreak: Defense against Cryptographic Ransomware. In Proceedings of the 2017 ACM on Asia Conference on Computer and Communications Security, Abu Dhabi, UAE, 2–6 April 2017; pp. 599–611.
29. Takeuchi, Y.; Sakai, K.; Fukumoto, S. Detecting Ransomware using Support Vector Machines. In Proceedings of the 47th International Conference on Parallel Processing Companion, Eugene, OR, USA, 13–16 August 2018; p. 1.
30. Thomas, J.; Galligher, G. Improving Backup System Evaluations in Information Security Risk Assessments to Combat Ransomware. In *Computer and Information Science*; CCSE: Richmond Hill, ON, Canada, 2018; Volume 11, ISSN 1913-8989.
31. Vinayakumar, R.; Soman, K.; Velan, K.S.; Ganorkar, S. Evaluating shallow and deep networks for ransomware detection and classification. In Proceedings of the 2017 International Conference on Advances in Computing, Communications and Informatics (ICACCI), Udupi, India, 13–16 September 2017; pp. 259–265.
32. Kwon, I.; Im, E.G. Extracting the Representative API Call Patterns of Malware Families Using Recurrent Neural Network. In Proceedings of the International Conference on Research in Adaptive and Convergent Systems, Krakow, Poland, 20–23 September 2017; pp. 202–207.
33. O'Kane, P.; Sezer, S.; Carlin, D. Evolution of Ransomware. *IET Netw.* **2018**, *7*, 321–327. [CrossRef]
34. Mauraya, A.; Kumar, N.; Agrawal, A.; Khan, R. Ransomware: Evolution, Target and Safety Measures. *Int. J. Comput. Sci. Eng.* **2017**, *6*, 80–85. [CrossRef]
35. Sotelo, M.; Maestre, J.; García, L. A novel Self-Organizing Network solution towards Crypto-ransomware Mitigation. In Proceedings of the 13th International Conference on Availability, Reliability and Security, Hamburg, Germany, 27–30 August 2018; pp. 40–48.

36. Al-rimy, B.A.S.; Maarof, M.A.; Shaid, S.Z.M. A 0-day aware Crypto-ransomware early Behavioral Detection Framework. In Proceedings of the International Conference of Reliable Information and Communication Technology, Johor Bahru, Malaysia, 23–24 April 2017; Springer: Berlin/Heidelberg, Germany, 2017; pp. 758–766.
37. Zhang, H.; Xiao, X.; Mercaldo, F.; Ni, S.; Martinelli, F.; Sangaiah, A.K. Classification of Ransomware Families with Machine Learning based on N-gram of Opcodes. *Future Gener. Comput. Syst.* **2019**, *90*, 211–221. [CrossRef]
38. Cimitile, A.; Mercaldo, F.; Nardone, V.; Santone, A.; Visaggio, C.A. Talos: No more Ransomware Victims with Formal Methods. *Int. J. Inf. Secur.* **2018**, *17*, 719–738. [CrossRef]
39. Huang, D.Y.; Aliapoulios, M.M.; Li, V.G.; Invernizzi, L.; Bursztein, E.; McRoberts, K.; Levin, J.; Levchenko, K.; Snoeren, A.C.; McCoy, D. Tracking Ransomware End-to-end. In Proceedings of the 2018 IEEE Symposium on Security and Privacy (SP), San Francisco, CA, USA, 20–24 May 2018; pp. 618–631.
40. Cohen, A.; Nissim, N. Trusted Detection of Ransomware in a Private Cloud using Machine Learning Methods leveraging Meta-features from Volatile Memory. *Expert Syst. Appl.* **2018**, *102*, 158–178. [CrossRef]
41. Homayoun, S.; Dehghantanha, A.; Ahmadzadeh, M.; Hashemi, S.; Khayami, R.; Choo, K.K.R.; Newton, D.E. DRTHIS: Deep Ransomware Threat Hunting and Intelligence System at the Fog Layer. *Future Gener. Comput. Syst.* **2019**, *90*, 94–104. [CrossRef]
42. Wang, Z.; Liu, C.; Qiu, J.; Tian, Z.; Cui, X.; Su, S. Automatically Traceback RDP-Based Targeted Ransomware Attacks. *Wirel. Commun. Mob. Comput.* **2018**, *2018*. [CrossRef]
43. 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.* **2018**, *74*, 144–166. [CrossRef]
44. El-Kosairy, A.; Azer, M.A. Intrusion and Ransomware Detection System. In Proceedings of the 2018 1st International Conference on Computer Applications & Information Security (ICCAIS), Riyadh, Saudi Arabia, 4–6 April 2018; pp. 1–7.
45. Kim, D.Y.; Choi, G.Y.; Lee, J.H. White list-based Ransomware Real-time Detection and Prevention for User Device Protection. In Proceedings of the 2018 IEEE International Conference on Consumer Electronics (ICCE), Las Vegas, NV, USA, 12–14 January 2018; pp. 1–5.
46. Honda, T.; Mukaiyama, K.; Shirai, T.; Ohki, T.; Nishigaki, M. Ransomware Detection Considering User's Document Editing. In Proceedings of the 2018 IEEE 32nd International Conference on Advanced Information Networking and Applications (AINA), Pedagogical University of Cracow, Cracow, Poland, 16–18 May 2018; pp. 907–914. [CrossRef]
47. Saleem, J.; Adebisi, B.; Ande, R.; Hammoudeh, M. A State of the Art Survey-impact of Cyber Attacks on SME's. In Proceedings of the International Conference on Future Networks and Distributed Systems (ICFNDS), Cambridge, UK, 19–20 July 2017; Art. No. 52, ISBN 978-1-4503-4844-7.
48. RAMSES. RAMSES: Internet Forensic Platform for Tracking the Money Flow of Financially-motivated Malware. 2016. Available online: https://ramses2020.eu (accessed on 5 January 2019).
49. CYBECO. Supporting Cyberinsurance from a Behavioural Choice Perspective. 2017. Available online: https://www.cybeco.eu/ (accessed on 9 January 2019).
50. Pillai, A.; Kadikar, R.; Vasanthi, M.; Amutha, B. Analysis of AES-CBC Encryption for Interpreting Crypto-Wall Ransomware. In Proceedings of the 2018 International Conference on Communication and Signal Processing, Chennai, India, 3–5 April 2018; pp. 599–604, ISBN 978-1-5386-3522-3.
51. Gonzalez, D.; Hayajneh, T. Detection and Prevention of Crypto-Ransomware. In Proceedings of the 2017 IEEE 8th Annual Ubiquitous Computing, Electronics and Mobile Communication Conference, New York, NY, USA, 19–21 October 2017; pp. 472–478, ISBN 978-1-5386-1105-0.
52. Richardson, R.; North, M. Ransomware: Evolution, Mitigation and Prevention. *Int. Manag. Rev.* **2017**, *13*, 10–21.
53. Mehmood, S. Enterprise Survival Guide for Ransomware Attacks. SANS Information Security Training | Cyber Certifications | Research. 2016. Available online: www.sans.org (accessed on 24 October 2018).
54. TechNet, M. Microsoft Protection Center: Security Tips to Protect Against Ransomware. Technical Report, Last Revision 2017. Available online: https://social.technet.microsoft.com/wiki/contents/articles/29787.microsoft-protection-center-security-tips-to-protect-against-ransomware.aspx (accessed on 30 January 2019).

55. Frenz, C.; Diaz, C. Anti-Ransomware Guide. Technical Report; OWASP Anti-Ransomware Guide Project, Version 1.7. 2018. Available online: https://www.owasp.org/index.php/OWASP_Anti-Ransomware_Guide_Project (accessed on 30 January 2019).
56. Ahmadian, M.M.; Shahriari, H.R.; Ghaffarian, S.M. Connection-Monitor & Connection-Breaker: A Novel Approach for Prevention and Detection of High Survivable Ransomwares. In Proceedings of the 2015 12th International Iranian Society of Cryptology Conference on Information Security and Cryptology, Iran, Rasht, 8–10 September 2015; pp. 79–84.
57. cuckoosandbox. Automated Malware Analysis. Available online: https://cuckoosandbox.org/ (accessed on 12 December 2018).
58. Cabaj, K.; Mazurczyk, W. Using Software-defined Networking for Ransomware Mitigation: The Case of Cryptowall. *IEEE Netw.* **2016**, *30*, 14–20. [CrossRef]
59. Pletinckx, S.; Trap, C.; Doerr, C. Malware Coordination using the Blockchain: An Analysis of the Cerber Ransomware. In Proceedings of the 2018 IEEE Conference on Communications and Network Security, Beijing, China, 30 May–1 June 2018; pp. 1–9.
60. Kharraz, A.; Robertson, W.; Balzarotti, D.; Bilge, L.; Kirda, E. Cutting the Gordian Knot: A Look under the Hood of Ransomware Attacks. In Proceedings of the International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment, Milan, Italy, 9–10 July 2015; pp. 3–24.
61. Hu, F.; Hao, Q.; Bao, K. A Survey on Software-defined Network and Openflow: From Concept to Implementation. *IEEE Commun. Surv. Tutorials* **2014**, *16*, 2181–2206. [CrossRef]
62. Mijumbi, R.; Serrat, J.; Gorricho, J.L.; Bouten, N.; De Turck, F.; Boutaba, R. Network Function Virtualization: State-of-the-art and Research Challenges. *IEEE Commun. Surv. Tutorials* **2016**, *18*, 236–262. [CrossRef]
63. Imran, A.; Zoha, A.; Abu-Dayya, A. Challenges in 5G: How to Empower SON with Big Data for enabling 5G. *IEEE Netw.* **2014**, *28*, 27–33. [CrossRef]