Computer Science Review 36 (2020) 100233

Contents lists available at ScienceDirect

Computer Science Review

journal homepage: www.elsevier.com/locate/cosrev

Review article

I2CE3: A dedicated and separated attack chain for ransomware offenses as the most infamous cyber extortion

Masoudeh Keshavarzi *, Hamid Reza Ghaffary

Department of Computer Engineering, Islamic Azad University of Ferdows Branch, Iran

ARTICLE INFO

Article history:
Received 22 April 2019
Received in revised form 15 September 2019
Accepted 24 February 2020
Available online 29 February 2020

Keywords:
Attack chain
Ransomware
Cryptocurrency
Cryptovirology
DGA
Doxware

ABSTRACT

"All of your files have been encrypted!", "Your device has been locked!", and so on are the sentences that these days are often seen in the cyber world. Motivated by recent promotions of technology, ransomware attack has soared saliently in terms of volume, versatility, and intricacy. This attack has initiated a lucrative trade by holding users' resources, whether data or non-data, hostage and demanding to pay ransom for release them. Furthermore, it has begun to camouflage other malware in many cyber-attacks. As a result, designing approaches to vanquish such threat should be taken into account. Understanding attack cycle and having an exhaustive taxonomy of ransomware, specially associated technologies, can assist to develop security measures at the various parts of attack flow. This paper has provided a comprehensive taxonomy of ransomware and digital extortion threats. A discrete and dedicated attack chain called I2CE3 has been proposed for ransomware regardless of its subcategories. The proposed chain offers six consecutive phases that ransomware species go through to triumph in attack. Afterwards, the present work has elaborated the role of all technologies involved in each phase. Finally, based on the proffered chain, performed studies and security solutions have been considered and segregated.

Contents

1. Introduction ... 2
2. Taxonomy of extortion-based attacks ... 3
   2.1. Rogue security software ... 3
   2.2. Ransomware ... 4
   2.3. Leakware (Doxware) ... 5
3. I2CE3: Ransomware attack chain ... 5
   3.1. Infection phase ... 5
   3.2. Installation phase ... 6
   3.3. Communication phase ... 6
   3.4. Execution phase ... 7
   3.5. Extortion phase ... 7
   3.6. Emancipation phase ... 8
4. Case study ... 8
5. Role of involved technologies ... 8
6. Defensive approaches based on attack chain ... 12
   6.1. Defense at the infection phase ... 12
   6.2. Defense at the installation phase ... 12
   6.3. Defense at the communication phase ... 14
   6.4. Defense at the execution phase ... 14
   6.5. Defense at the extortion phase ... 15
   6.6. Defense at the emancipation phase ... 15
7. Conclusion and open challenges ... 16
   Declaration of competing interest ... 16

* Corresponding author.
E-mail addresses: Masoudeh_k@yahoo.com (M. Keshavarzi), keshavarzighafari@gmail.com (H.R. Ghaffary).

https://doi.org/10.1016/j.cosrev.2020.100233
1574-0137/

References 16

1. Introduction

Ransomware is forthcoming one of the most perilous cyber threats facing both individuals and organizations. According to Kaspersky Lab ICS CERT [1], 2017 has been a tough year in terms of destructive attacks. One of the main global threats to users was ransomware. In 2017, FBI's Internet Crime Complaint Center (IC3) received 1783 complaints identified as ransomware with adjusted losses of over $2.3 million [2]. Moreover, Verizon Enterprise has specified ransomware the most dominant sort of malware in 2018 Data Breach Investigations Report (DBIR) [3].

Ransomware, as its name implies, is a malware that extorts them by taking users' resources hostage. This exaction is done based on victim's fear of losing digital assets or denying access to them. The concept of ransomware or extortion-based malware was first formally introduced by Dr. Joseph Popp in 1989, with releasing "AIDS Information Trojan" [4]. AIDS Trojan was distributed via infected diskettes with a fabricated cover of "PC Cyborg Corporation" to the victims. It attacked users by encrypting and interfusing their file names and demanding payment of US$189 to recover files. The AIDS modus operandi was to replace AUTOEXEC.BAT file with malicious instructions, whereby the victim machine was rendered unusable at the 90th boot up of the system. Despite the fact that AIDS Trojan used sophisticated techniques, it had several flaws. One weakness was that this Trojan leveraged symmetric cryptography and embedded the key into the malware itself. Following that, Adam Young and Moti Yung [5] proposed the idea of using asymmetric cryptography (and even better, the hybrid) for the high-survivable viruses. The authors employed public-key encryption in the cryptovirological attacks and demonstrated that it was essential to such threats. One-Half virus, LZR virus, AIDS Info Trojan, and KOH virus are the malware samples that were investigated in their research paper. Nowadays, this method is applied to the cryptographic ransomware greatly.

Despite a long latency, ransomware has resurged, and its intensity and diversity have peaked over the last few years. Since 2012, ransomware scams and its business model have thriven again. CryptoLocker, reported in 2013, was a sort of cryptographic ransomware which identified to be trailblazer in the lucrative crypto ransomware industry. It infected more than 250,000 systems in less than four months and its revenue reached over $3 million [6–8]. With the introduction of ransomware-as-a-service (RaaS) and untraceable payment systems, this trade has become more serious in the underground market. The emergence of RaaS has provided a sketch of developing and improving new ransomware variants to every cybercriminal even without needed skills. The outbreak of attacks like WannaCry, Petya, and NotPetya has gained much fame and attention in 2017. According to the reports, the average amount requested as ransom is typically between $300 and $700 for individuals, and ranges from $10,000 to $17,000 for enterprises [9,10]. It is estimated that by 2019, the proceeds of the cybercrime will reach $2 trillion [8]. Ransomware has involved not only servers and personal computers, but also all computational systems including smart phones, IoT devices, ICS/SCADA, and many others, as shown in Fig. 1 [1,11–15]. Therefore, coping with it is one of the security requirements of any organization.

Detection of ransomware families remains a challenging task, due to the evolution of technologies and ongoing enhancement of employed techniques, which play critical roles on. Hence, having a self-inclusive view of involved components can be effective in presenting security solutions against ransomware attacks and circumventing new variants of them. Although the studies have been conducted to diagnose and analyze some of ransomware specious, only a small number have addressed ransomware categorization. Table 1 summarizes the review papers presented in this research area. The Ref. [16] proposes an intrusion kill chain. It is the only research work mentioned here that does not specifically address ransomware. Compared to those dealing with categorization, this article differs by providing a comprehensive taxonomy which covers all new types of extortion attacks. Although the paper [9] is the closest to our work, it only investigates the success factors of the attack and classifies ransomware based on severity, platform, and target. In addition to providing a comprehensive taxonomy covering the newer threats, our research perusal will also examine all the technologies that are the primary actors in ransomware attack. On the other hand, having an overview of the attack flow assists to design a multilayer security system, especially in preventing threats such as ransomware. To the best of our knowledge, this paper is the first that suggests a separated and dedicated chain for ransomware, regardless of its subcategories. The segmentation of the attack steps allows investigator to deeper explore the problem of ransomware from a global and regulated perspective. Subsequently, we review performed studies and segregate defensive solutions based on the proposed attack cycle. This classification will lead to better organization of research efforts.

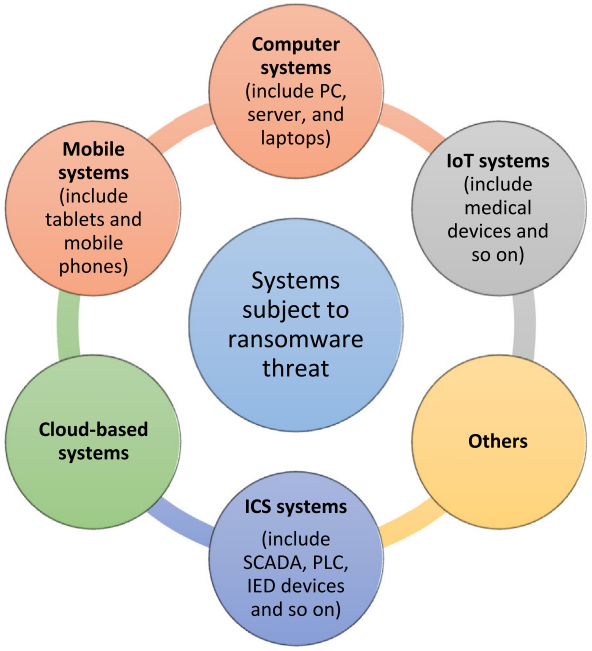

Fig. 1. Target of ransomware attacks.

The rest of the paper is organized as follows. Section 2 surveys ransomware attacks, and provides an exhaustive taxonomy of all fear-based threats. In Section 3, we propose a parting scheme for ransomware attack chain and elaborate each phase in details. Section 4 provides an application of this proposed chain to a real case study. Section 5 focuses on the role of involved technologies. After examining and classifying the defensive approaches based on suggested attack cycle in Section 6, we conclude this paper in Section 7 and present some of the existing open challenges.

Table 1
Related survey papers.

Reference	Topic	Introducing attack chain	Introducing taxonomy	Purpose
[9]	Ransomware	–	✓	The authors classify ransomware from three perspectives (severity, platform, and target). They focus on success factors of ransomware and review the existing studies in the field.
[13]	Ransomware	–	✓	The authors discuss the rise of ransomware attacks and security concerns in the Internet of Things (IoT). They categorize ransomware into three basic types (crypto, locker, and hybrid). This article provides a comprehensive description of ransomware intrusion methods and remedies for IoT devices
[16]	APT	Intrusion kill chain (IKC), Also known as cyber kill chain (CKC)	–	Since the evolution of Advanced Persistent Threat (APT) necessitates an intelligence-based model, the authors propose a kill chain model to describe phases of intrusions, map adversary kill chain indicators to defender course of action, and identify patterns that link individual intrusions into broader campaigns.
[17]	Ransomware	–	–	This article explores the transition from the early-day scams to extortion implemented by current ransomware. It studies prominent examples of ransomware over time along with their characteristics and infection methods.
[18]	Ransomware	–	✓	This is one of the first studies to review ransomware. Suggested taxonomy is only based on the severity of the threat. However, due to the absence of various families at the time of its publication, the proposed categorization does not cover many new types of ransomware.
[19]	Ransomware	–	✓	This research work analyzes the evolution of key management in ransomware and classifies crypto-ransomware attacks accordingly.
Current article	Ransomware	Ransomware attack chain (I2CE3)	✓	Since identifying the category to which ransomware belongs can be very effective in providing defensive and remedial solutions, this article presents taxonomy of extortion-based attacks. It is also the first time that a dedicated attack chain has been proposed for such threats, and several case studies have been conducted on this basis. Finally, a structured categorization of related studies has been performed based on the proposed chain that highlights the attack indicators in each phase.

2. Taxonomy of extortion-based attacks

Ransomware is a cyber-threat which blocks users access to their resource, whether data or non-data, with the intent of extortion. It has been the most predominant cyberattack since 2005. This malicious software has initiated a lucrative trade among cyber criminals. With the continuous evolution and sophistication of ransomware families, security researchers have begun to introduce a range of taxonomies to facilitate the comprehension of ransomware attacks and implement appropriate countermeasures with the minimum loss of digital assets. Cyberattacks can all be classified in several ways in order to better grasp their functionality and posed threat level. Luo and Liao [18] categorized ransomware based on threat severity. They distinguished bluff ransomware from real ones. Then, according to their proposed method, real ransomware was divided into simple attack and encryption with different key lengths. The taxonomy proffered by Ahmadian et al. [20] merely classified ransomware into non-cryptographic and cryptographic, and did not address all of the extortion-based attacks. Al-rimy et al. [9] classify ransomware from three perspectives, namely severity, platform, and target. Their severity-based approach isolates this threat into scareware and detrimental ransomware. They further categorize later into locker and crypto-ransomware. Bajpai et al. [19] address ransomware taxonomy from the key management standpoint. Given the popularity of extortion attacks and the increasing spread of new species, the lack of a comprehensive classification that covers all extortionist attacks still remains felt. We present a hierarchical and coherent taxonomy of ransomware as a subclass from malware that covers all of the fear-based threats, as shown in Fig. 2.

In general, malware refers to any malicious code employed by an adversary to execute her/his evil intentions on a system without authorization and knowledge of its owner [21,22]. Ransomware is a sort of malware that can fall into the subset of scareware category. However, in some open literatures, scareware is maintained as a type of ransomware. We put ransomware under the subcategory of scareware attacks, because it takes advantage people's fear for its illicit and profitable purposes. Scareware is a form of malware that, by scaring people with imaginary or real threats, forces them to do special activity. Typically, all scareware attacks can be called extortion-based threats. In the same sense, we separate the scareware into three categories, as will be described below.

2.1. Rogue security software

The rogue security software was one of the most known and common scareware. It is a deceitful program that pretends to be anti-spyware or legitimate system utility, but in fact being

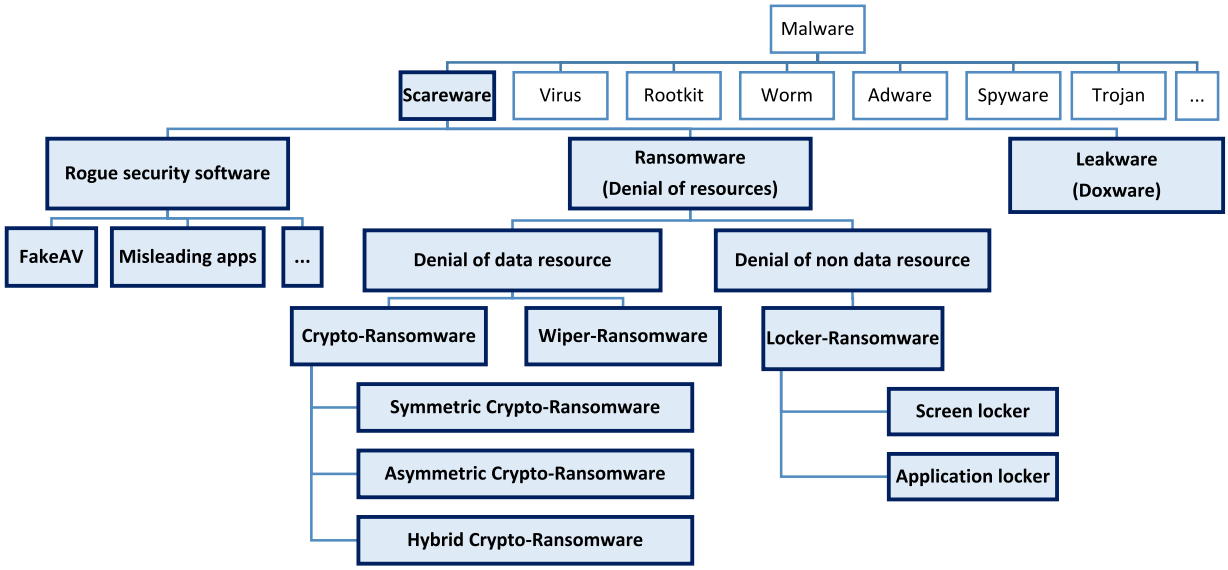

Fig. 2. Proposed taxonomy of the extortion-based attacks.

malicious software itself. This sort of scareware pretends it has reconnoitered potential malicious items or illegal content on the victim machine. Main difference between rogue utility and classical ransomware is that rogue software does not typically deny access to the resources and damage the victim device. More often than not, they would appear as a troublesome application in the background and continuously notice the users about bogus security alarms for the reasons that convince them to buy proposed security solution. Fake anti-virus (FakeAV) is one of the prevalent rogue software that has been capitalized so far. FakeAV informs the users that there is malicious code on their system and claims they are indispensable to purchase its own software. But in fact, the solution offered by the group behind fakeAV does nothing more than remove the malware itself. Most of the time, the rogue application's purpose is to get money from victims or start a more serious attack.

2.2. Ransomware

The advent of ransomware has brought about a dramatic change in scareware industry. This class of malware by taking user's resources hostage and demanding ransom for release them, in forms of paying money, purchasing software, or doing a special task, has made a lucrative business model among the other attacks. The key feature that distinguishes ransomware from other types of scareware is to confiscate the victim's device or valuable data and prevent user from accessing them. Depending on the seized resource, we divide ransomware into two classes: denial of data resource, and denial of non-data resource. To the best of our knowledge, this is the first taxonomy that covers all types of ransomware, and puts each one in its own category.

Denial of data resource (DoDR). The most valuable asset in computer system is data. This class of ransomware blocks access to the data resources (files) and requires victims to pay a ransom, if they want to get back access to their data. Crypto-Ransomware is the most prevalent of this category. Although cryptography has been known as a purely protective technology from unauthorized access, Crypto-Ransomware uses this technique offensively in order to encrypt the precious data, and demands a ransom for exchange the encryption key. One could say, AIDS Info Trojan is the first discovered and documented Crypto-Ransomware. This attack was not so prosperous, because the decryption key could be extracted from the code of the Trojan. Hence, the idea of using asymmetric key and hybrid methods was made [5,23,24]. Therefore, according to the encryption mechanism, Crypto-Ransomware can be split into three groups; symmetric, asymmetric, and hybrid.

In symmetric crypto-ransomware, the same key is used for both encryption and decryption. One of the key strengths of this approach is the speed of its operation, which results in improved performance in ransomware attacks. However, the inapt manner of managing the key will expose it. In asymmetric crypto-ransomware, different keys are used for encryption and decryption. Using of asymmetric cryptosystem (also known as public key encryption) allows a slightly stronger form of cryptoviral attacks. It involves a private key that is known only for the owner of malware. After encrypting data with public key, victims require the private key in order to decrypt and return their files. The benefits of this cryptographic method can be cited as robustness and almost unbreakable. The main disadvantage of this approach is its slowness, which is cumbersome in cyberattacks. Finally, hybrid mechanism combines symmetric and asymmetric cryptography in order to acquire the best of both methods. In hybrid strategy, asymmetric cryptography is employed to securely encrypt the session key, which is the symmetric cipher used by ransomware to encrypt data [5,19]. For example, TorrentLocker is a sample that adopts RSA and AES algorithms. The random generated AES key is encrypted by RSA. As an another instance, one could indicate a variant of Gpcode that encrypts data using a unique AES-256 secret key and re-encrypt this key by a 1024-bit RSA public key [25,26]. CTB-Locker (Curve-Tor-Bitcoin-Locker) also is placed in the hybrid crypto-ransomware class that employs a combination of AES and Elliptic Curve Cryptography (ECC). Apart from the cryptography algorithm, cybercriminals can utilize both standard (e.g., CryptoAPI provided by Windows platform) and custom cryptosystem during the attacks.

Although Crypto-Ransomware is the most popular and successful class of denial of data resources, it is not the only one. Any of malware that deny the users from accessing their resources until they make a payment or do an activity is considered as a ransomware. Wiper is another category of the DoDR ransomware. Albeit, the wiper can be classified by itself as a separated group of the malware with the aim of destroying critical files, it is observed in the several extortion-based attacks. Hence, we have identified it as a subset of DoDR ransomware. The conventional wiper

intends to destruction rather than financial gain. Shamoon and StoneDrill are notorious families belong to the classical wiper [3, 27].

Principally, the majority of Wiper-Ransomware has a capability to modify and overwrite the Master Boot Record (MBR) – which is responsible for loading operating system – with their own malicious code in order to render the system useless, after deleting data resource. Though, this functionality can be existence in other families of ransomware. There are multiple data destruction methodologies so that data is rendered unusable. In case of Crypto-Ransomware, unauthorized data encryption is applied for the purpose. But, the Wiper category utilizes either unauthorized data replacement or data encryption (of course, without any decryption key). As a matter of fact, the Wiper class needs lower effort. Notwithstanding the predefined structure of Wiper-Ransomware, some of the Crypto-Ransomware attacks inadvertently can fall into this category due to the existence bugs in their implementation. WannaCry is a sample of data destruction attacks in 2017. It used a combination of AES and RSA for encrypting files and generated a unique Bitcoin wallet address for each victim. However, due to a race condition bug this code did not execute correctly. The adversaries were unable to identify which of the victims had paid. Subsequently, the victims lacked any chances to regain access to their files [28]. In addition to WannaCry, Petya, PetWrap, NotPetya, AnonPop, Ordinypt, and MBR-ONI has appeared as destructive attacks [3,29,30] that we would place them under the Wiper-Ransomware class in our proposed taxonomy. For example, Ordinypt is a strain of Wiper-Ransomware that replaces the contents of files with random data and requests a ransom of 0.12 Bitcoin (600 Euro) [30].

Denial of non-data resource (DoNR). The second category of ransomware prevents victims from accessing the device or system utilities, but leaves the user's data intact. Data may seem inaccessible at first glance, but the main difference with the previous group (i.e., DoDR) is that the data will not be tampered with or destroyed. Therefore, it makes DoNR less effective at extorting victims compared with its counterpart. The most famous, and at the time of writing this article, perhaps the only identified class belonging to DoNR is Locker-Ransomware, which uses locking mechanisms against victims. Since Locker-Ransomware attacks, similar to rogue security software, do not have a fatal threat to the devices and do not destroy the data, they must use social engineering techniques to convince and force the victims to pay ransom. IoT devices, especially in the health and emergency sectors, are attractive targets for this type of attack [13,31]. As the targets of ransomware are shown in Fig. 1, Locker-Ransomware category aims more mobile, IoT, and ICS devices than computer systems or cloud storage that contain valuable data stored. Depending on blocked non-data resource, Locker-Ransomware attacks are split into subclasses. These resources can comprise operating system, application, services, user interfaces, and other utilities. For example, Trojan.Ransomlock.G [15] locks the user's screen and displays a full screen ransom note that covers the entire desktop. Also, the first variant of DeriaLock was only a screen locker and requested a payment. Lockdroid and many variants of its target Android platforms and employ a range of psychological tricks to persuade victims into paying the ransom [9,15,32]. Reveton is another sample of Locker-Ransomware that locks the screen and leaves files intact. It also disables Task Manager and pretends to be a message from law enforcement authority that has spotted illicit activities in the victim's machine. Some other strains of Locker-Ransomware tend to lock browser. Most of browser lockers are cross-platform and client-side. Browlock is a sample of them [15].

2.3. Leakware (Doxware)

The extortion-based threats have attained new levels of menace. Another category of scareware or fear-based attacks is Leakware (also known as Doxware). It is a new evolution of digital hijacking and cyber blackmailing. Doxing in the word means the publishment of confidential and personal information on the Internet. Doxware utilizes the mechanisms of spyware and info stealer, and in some cases, it combines them with ransomware methodologies, such as cryptography or locking. Primarily, instead of denying user's access to the resources (mostly private and valuable data), Leakware makes them visible to everybody unless the victim pays the ransom off.

This concept was first formally posed by Adam Young through the introduction of crypto virus with a novel feature in 2003 [33]. Game theory was engaged as an integral part of the attack itself that was launched on the host. It was used to analyze the effectiveness of proposed attack. Since 2017, the threat has become more noxious. In general, Leakware is more dangerous than all breeds of ransomware, as backup strategies cannot mitigate the damage caused by it. What makes the Leakware worse and more persistent than other extortion-based attacks, is that even if the victim pays the ransom, she/he may still be threatened because a copy of the data is in the hands of adversaries. Apparently, Charger (with EnergyRescue as the app's name) [34] is a battery saving application for Android platforms. It thieves the user's SMS message and contact list, and locks the device. Then, it blackmails the victim by threatening to sell her/his personal information on the black market.

3. I2CE3: Ransomware attack chain

Ransomware attack and its species are growing at a remarkable rate. Its ability to impress individuals and organizations, a little risk and cost to the attackers, not having to find a buyer for stolen data (like info stealers), the capability to deploy across numerous devices, and thereby impose bigger ransoms, has made ransomware an interesting phenomenon from the perspective of adversaries [3]. To tackle such cyber threat efficiently, it is required to comprehend the steps of attack. The separation of the attack process allows researchers and security professionals to have a common contract, whereby they can convey their ideas and discuss the problem of identifying and halting threat at each stage of the attack continuum.

The ransomware attack begins at the moment which the malicious payload is delivered via one of the infection vectors to the victim machine. A successful ransomware attack after taking control of the device prohibits users from accessing it or the data stored on it. Preventive actions principally include encryption and locking. Next step is leaving a ransom note and informing the user that her/his resources have been held hostage. To outlasting in the cyber world, ransomware campaigns should pledge to set free hostages (e.g., by decrypting data resources or unlocking non-data resources), after receiving the ransom. Otherwise, ransomware campaign will soon lose its reputation among the victims. This is all that happens in different ransomware categories. Accordingly, we provide an attack cycle that covers all sorts of ransomware, irrespective of the methodology used to capture the resource. Fig. 3 expounds each of the stages as the attack is proceeding.

3.1. Infection phase

All of the ransomware attacks commence at the moment that the malicious code is delivered to the victim. This job is accomplished via infection vectors in the first section of attack chain,

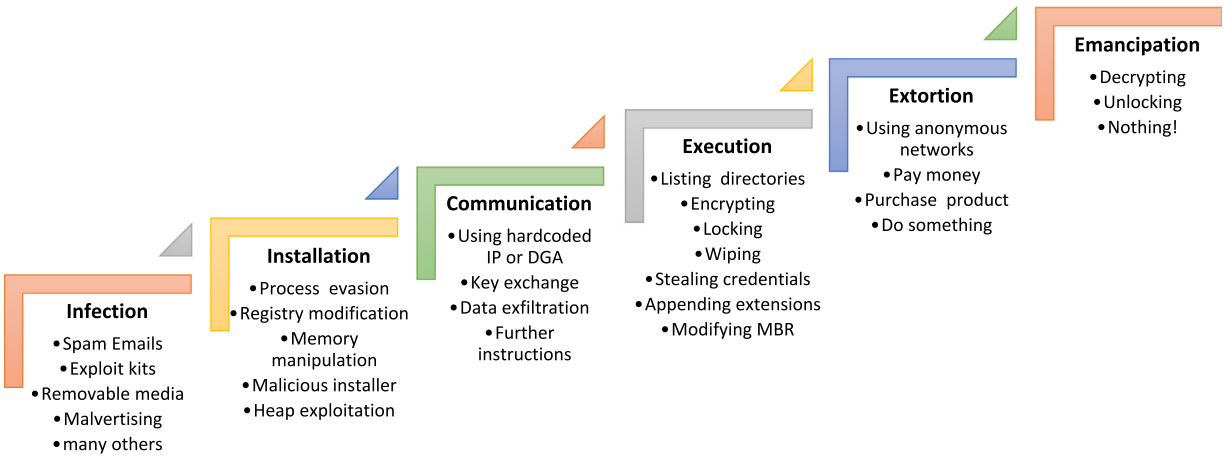

Fig. 3. Proposed attack chain (I2CE3) for all types of ransomware.

which is infection phase. Although, there are multiple infection vectors, ransomware attacks mostly employ spam phishing emails and exploit kits. The spam emails contain either malicious attachments (e.g., a Microsoft Office document inclusive of macro, a PDF file with JavaScript) or a link to a compromised website. The first vector needs user interaction to click and download malice payload whereas later does not. Notwithstanding exploit kits are zero-day in the nature, the adversaries prefer to deliver ransomware via phishing emails and social engineering techniques. In case of mobile ransomware, one of the most common infection vectors is the download of malicious app from untrusted sites or from app stores which do not have the necessary security controls. Charger [34] and Lockdroid are the samples of this group.

The first known ransomware, AIDS Trojan, used the infected diskettes in order to deliver malware to the victims [4,5,23]. With the extension of botnets and their prosperity in sending massive amounts of spam emails, the rate of adopting spam emails has been raised for distributing malware to as many users as possible. CryptoLocker used Gameover ZeuS botnet to spread through spam emails to many of its victims [7]. Likewise, CryptoWall, Cerber, Jaff, and Locky are other successful ransomware which are delivered via spam emails. Nevertheless, the trail of several exploit kits is sensible in the distribution of ransomware. According to the reports, Angler, Neutrino, Magnitude, Nuclear, and RIG are the exploit kits which have employed as delivery methods in some of ransomware families such as CryptXXX, CryptoWall, Cerber, and Locky [35].

Although most ransomware variants spread through mentioned infection vectors, there are species that operate on self-propagation manner. For the reason, a new epoch of "crypto-worms" is expected to emerge in the cyber extortion attacks. This concept will be more eminent as spam campaigns become less efficient. WannaCry is more malignant than other common ransomware due to its self-propagation characteristic that uses it to exploit critical vulnerabilities in the infection phase [28]. Before the outbreak of WannaCry, ZCryptor had exhibited this behavior and adopted worm-like infection vector on the Windows platform [35].

3.2. Installation phase

The malicious payload mostly is downloaded via droppers. After the malcode is delivered to the victim machine through aforementioned vectors, ransomware enters the installation phase. At this point, ransomware must install itself on the system and take control of the device, without attracting the attention of security software. To this end, ransomware utilizes a variety of techniques. One of the procedures that cannot be easily recognized by signature-based security tools is code injection. Process Hollowing is a code injection technique that has been used by malware to hide itself. For example, TorrentLocker employed this technique for injecting malicious code into the legitimate Windows process [36]. It utilizes explorer.exe as its hollow process. Similarly, CryptoWall and GlobeImposter are other samples that leverage Process Hollowing to perform their activity from a seemingly legal process [36,37]. Process Doppelgänging is a novel and very sneaky technique for cross-process injection. This technique is somewhat similar to Process Hollowing and assists to bypass most of modern security systems. Process Doppelgänging takes advantage of NTFS transaction in order to mask the loading of executable. It is considered as a fileless attack, because the malicious code is not stored on the disk. SynAck is the first ransomware family to adopt Process Doppelgänging which evades real-time file scanning [38].

Another deceptive method for evading antivirus solutions during installation is to hide malware in the installer package. Recently, the wave of new malicious Nullsoft Scriptable Install System (NSIS) installers adopted by ransomware campaigns has been observed. It tries to appear as normal as possible with the inclusion of non-malicious components. In the newer version of NSIS installers, Nullsoft installation script is responsible for loading the encrypted malicious payload into the memory, decrypting it, and executing its code area. NSIS has been seen in the installers that drop the infamous ransomware families, such as Cerber, Locky, CryptoWall, Wadhrama, and CTB-Locker [39]. In many samples of Crypto-Ransomware or Wiper-Ransomware to make sure that there is no way to recover encrypted data resource, volume shadow copies will be deleted using the vssadmin.exe tool [36]. Also, some changes are made by ransomware on the system to persist between system reboots and place into startup, depending on the platform.

3.3. Communication phase

Once the installation of ransomware is completed, it starts to amass the victim's information. This information, which is later exfiltrated, includes the victim's IP address, location, operating system, version of browser and its plugins, security tools installed on the device, and so on. Some of ransomware families require an initial communication with the main malefactors in order to execute their further actions. In communication phase, ransomware will attempt to establish a connection with its command and control (C&C or C2) server. This behavior occurs frequently in

many other types of malware. But in ransomware attacks, especially in case of Crypto-Ransomware, this communication is accomplished mostly with the intention of exchanging encryption key and receiving required instructions to keep on attacking.

The connection to the C&C server is made either through IP address or domain name. Since the hardcoded IP and domain names in the malware itself were detected by analytical techniques and resulted in the attack being defeated, the attackers began to use tricks to resist and anonymize their communications. To conceal the adversary's location and achieve anonymity, cybercriminals behind ransomware have adopted systems providing anonymous network communications, such as The Onion Router (Tor) and the Invisible Internet Project (I2P) [15]. Another most recently used tricks is domain generation algorithms (DGAs) that produces the domain names for C&C operations with multiple levels of redirection to enhance obfuscation and reduce the probability of takedown [15,40]. In this mechanism, an embedded code in the malware binary is used to create a seed for generating pseudo-random domains. Then, ransomware issues DNS queries in order to look up the potential registered domains for communicating with the C&C server [40].

In the case of mobile ransomware attacks, most of them leverage simple HTTP/S connections to communicate with the C&C server. New variant of Simplocker has been spotted that uses Extensible Messaging and Presence Protocol (XMPP) to bypass security measures. It adopts this legitimate messaging relay server in order to contact to the C&C server. As a result, its communication looks normal and makes it difficult to trace C&C traffic. Also, all communications over XMPP can be encrypted using Transport Layer Security (TLS) [32]. Communication phase is very crucial in some of ransomware families. For example, CryptoLocker attempts to find an active C&C server and connect to it though DGA-generated domains. If the connection is failed, the malicious behavior is not triggered and the sample does not arrive into the execution stage [20,25]. TorrentLocker is another example that will not encrypt files if it fails to connect to its command server [36]. In contrast, the ransomware species, such as Bart and a new version of RAA, do not need to connect to the C&C server for their nefarious operations and data encryption.

3.4. Execution phase

As noted in the taxonomy section, the main distinction of ransomware from other fear-based attacks is to impede users' access to the digital resources (whether data or non-data). This goal is achieved through a variety of mechanisms, including encryption, locking, or deletion. In the Crypto-Ransomware and Wiper categories, a step is required to search for important files that should be attacked. The traverse strategy varies for different types of ransomware. The search process can be as simple as seeking files with specific extensions to more complex procedures that consider the last accessed files or the entropy of the files. Some samples of ransomware adopt Windows's volume management functions such as GetLogicalDrives and GetDriveType to find network drives to perform destructive actions and encrypt the contents of target files stored on them [25,41,42]. After enumerating all directories, depending on the cryptography algorithm or the strategy used, the malicious operation begins on data resources. Only files that are matched with predefined extensions (or conditions) are encrypted or manipulated.

In the vast majority of Crypto-Ransomware families that employed fast symmetric cryptography algorithms, the key schedule is pre-computed. It results in that the entire key schedule to reside in memory during the whole of encryption process [43]. In the case of asymmetric and hybrid crypto-ransomware, the key required for encryption is delivered to the victim machine in the communication phase. However, in some variants, this key will be generated on the victim machine and sent back to the C&C server. After tampering selected files, depending on the type of ransomware, a new special extension will be appended to the end of affected files name. Some species not only encrypt the contents of files and render them unusable, but also alter the filenames. This will make the victim unable to correctly estimate the amount of damage.

Crypto-Ransomware families can leverage a variety of cryptographic algorithms along with standard or customized cryptosystems. For instance, RansomCrypt after running on a machine, begins to iterate all files and encrypt them using standard TEA algorithm, a simple block cipher [44]. Other families like Locky and CryptoLocker may utilize more sophisticated block ciphers, such as AES, along with another algorithm to encrypt the content of target files. In the species belonging to the Wiper category, the contents of target files may be overwritten with junk data in this phase. In the denial of non-data resource attacks, targeted resources are identified and limited by locking mechanisms. In this attack, instead of manipulating data resource, the device itself or some applications will be useless. Many kinds of ransomware belonging to this category leverage a full-screen window on the victim machine and restrict the user's access to this page in different ways. This will be done by creating a virtual desktop, changing registry entries, or killing some processes.

Although theft of information is not part of the predefined ransomware aspirations, some strains have this capability. This thievery may be carried out either with the purpose of espionage or with the aim of lateral movement. For instance, Petya steals credentials from the compromised machine and uses them to spread itself to the other devices. Alternatively, SamSam, the most notable sample of targeted ransomware, also has this functionality [35]. Recent variants of Cerber have the feature in the form of Bitcoin wallet-stealing [35]. In addition, there are also tremendous features in many species. For example, HDDCryptor leverages a utility tool for extracting credentials from the last session to reach the previously accessed network drives, which are not currently mounted [41]. Ultimately, after performing any malicious actions, many ransomware families tamper the MBR and replace it with their own bootloader to display ransom note.

3.5. Extortion phase

Different from many other types of malware, ransomware often informs victims that they have been affected by a specific attack, and to be rid of it, they must follow the instructions. Instead of finding the right and avid buyers for stolen valuable data in the underground market, it directly extorts money from users by preventing them from accessing to the device or data. In this stage, a ransom note is displayed typically in the language based on the geolocation of victim's machine IP address (in the forms of background image, HTML file, text file, and so on). The ransom note contains required instructions about how to make payment and how to return data or device to the original state. In many ransomware families, the text content of ransom note is hardcoded in the malware binary itself. Other variants may download it from the C&C server on first communication. Only the user-specific information and necessary Tor links will be added later to the ransom demand.

Similar to all fear-based attacks, social engineering techniques are most used in this section to persuade victims to pay a ransom. To do this, many Crypto-Ransomware and Wiper-Ransomware families specify a deadline that if the payment is not made by that time, the private key (necessary key for decryption) will be permanently destroyed or the requested amount will be doubled. In addition, most Crypto-Ransomware offers a free decryption

service for a few numbers of infected files in order to ensure the victim to pay ransom. In many ransomware families, after displaying a ransom page, the hollowed process gets killed by itself.

AIDS Trojan, the first documented ransomware, demanded victims to make a payment via international money order or cashier's check, sent to a P.O. box in Panama [4,15]. Nowadays, there are so many payment methods that are all anonymous or pseudo-anonymous. And this is one of the reasons for the growth of this lucrative attack among the cybercriminals. Payment methods range from wire transfer and online voucher-based payment systems to the use of a variety of popular cryptocurrencies. For example, earlier versions of CryptoLocker provided different options including cashU, Ukash, paysafecard, Green Dot MoneyPak (USA only), and Bitcoin for payment to the victims [15, 42]. Although in the newer versions, only MoneyPak and Bitcoin are offered. Given Bitcoin's popularity as a cryptocurrency, its pseudo-anonymity and almost decentralization, and the possibility of having multiple Bitcoin addresses independent of users' real identities, the use of Bitcoin has become widespread in felonious activities, especially in the digital extortion attacks such as ransomware [36,45–48]. In addition to the availability of Bitcoin in all geographical areas, another advantage is the irreversibility of transactions.

Financial motive is no longer only adversaries' incentive. Many ransomware attacks are emerging for political purposes, spying, sabotaging, or camouflaging other types of malware. For instance, Unit 42 research group from Palo Alto Networks [49] has spotted a new strain of ransomware called RanRan with a political motive instead of a monetary payment. It targets Middle Eastern organizations and extorts them by forcing victims to post a seditious political statement against a Middle Eastern political leader (the victim's country leader). Rensenware is another example of Crypto-Ransomware with non-monetary incentive that looks more like a joke. In order to decrypt files, it asks the victim to get needed score in the TH12 $\sim$ Undefined Fantastic Object, a shooting game specified in the ransom note. To illustrate the motivations behind the ransomware scams, we divide the requested ransom into two main groups, monetary and non-monetary.

3.6. Emancipation phase

The condition to survive in the business world is to fulfill the obligations. Illegal cyber trade is also no exception. The hackers behind ransomware must release the taken hostage resources after receiving the ransom from the victim so that they can continue to earn money in subsequent attacks. Some ransomware variants pay much attention to this principle, as they even provide online chat services or other facilities to victims in order to ensure the integrity of the resource emancipation process, and if there is any problem they can help.

In the Crypto-Ransomware attacks, after paying the ransom, a link to a victim-specific decryption tool is sent to the infected user. TorrentLocker, CTB-Locker, and TeslaCrypt are the sample ransomware families that act in this way and provide decrypting tools when the payment is completed [36]. However, there are some categories that are not able to recover victim's resources after receiving a ransom, deliberately or because of a bug in the ransomware design. In Section 2, we put this type of ransomware in the Wiper-Ransomware category. For example, WannaCry can be pointed out, which due to the technical details in the code, was not able to identify which victim had paid the ransom [3,28]. Therefore, according to the reports, those who paid the ransom in this kind of attack never received a decryption key to recover files. The same applies to NotPetya. Even if the victim agrees to pay, NotPetya will erase the Salsa20 stream cipher key, needed for decryption [3]. But with all this, there is no guarantee of the proper release of resources for a variety of reasons, including connection impairment, bugs in the ransomware code, or unpredictable malicious intentions of its authors.

4. Case study

To illustrate the applicability of I2CE3 chain, a case study of several different ransomware families has been conducted. This study shows that different ransomware samples, regardless of which subcategory they belong to, have similar indicators in each phase of the attack. Figs. 4 and 5 depict the process of TorrentLocker and Koler attack based on I2CE3 six steps, respectively.

Table 2 presents the indicators extracted from some other ransomware samples (including Crypto and Wiper-Ransomware) at each stage of the I2CE3 chain.

5. Role of involved technologies

Motivated by recent promotions of technology, ransomware attacks have increased saliently in terms of volume, versatility, and intricacy. Understanding how ransomware variants operate and what technologies are contained in the flow of attack allows us to better perceive how to surpass and defeat them. It is evident that comprehending the characteristics of infection vectors, delivery of malicious payload, and features of network traffic with C&C servers to receive instructions will aid the security teams to be aware of what to anticipate, and to adopt proper countermeasures to prevent or minimize the detriment inflicted by ransomware at that point. In following we summarize some of involved components in this cyber threat and explore each of them. However, there are a few actors that might be omitted or out of the reach of the paper.

Role of cryptography. Ransomware employs an assortment of techniques to block users' access to their resource. The most common and interesting techniques is cryptography. Traditionally, cryptography is a serviceable technology to information security on the fly. It is defensive in nature, and provides privacy, authentication, and security to users. But, this technology can be misused against security. The idea of Cryptovirology was first posed by Adam Young and Moti Yung [5,23,50], which is the offensive utilization of cryptography. Cryptovirology is the area of scientific study that focuses on the combination of cryptography and malicious software. Survivable virus, or today's Crypto-Ransomware, adopts this technology to take data hostage. As long as the victim has not paid the ransom, the decryption key is not delivered to her/him.

A variety of symmetric and asymmetric encryption algorithms are used for this purpose as described in Section 2.2. In order to achieve acceptable speed, high performance, and robustness, most ransomware attacks use hybrid methods. Many ransomware belonging to this category, generally use a fast symmetric algorithm like AES to encrypt files and then employ a public key algorithm, such as RSA and ECC, to cipher the secret key. ECC applies a relatively shorter encryption key than RSA. As a result, it is faster and requires less computing power than RSA with the same key length. The proof of this concept is the equivalent strength of the 160-bit ECC and RSA with a key size of 1024 bits. In contrast, implementation of RSA is easier than ECC and, the probability of error is lower due to lack of complexity. AES, the symmetric block cipher which adopts the shared secret key for encryption and decryption, is one of the most commonly used algorithms in ransomware attacks. This algorithm has been deployed in different modes in the various strains of ransomware.

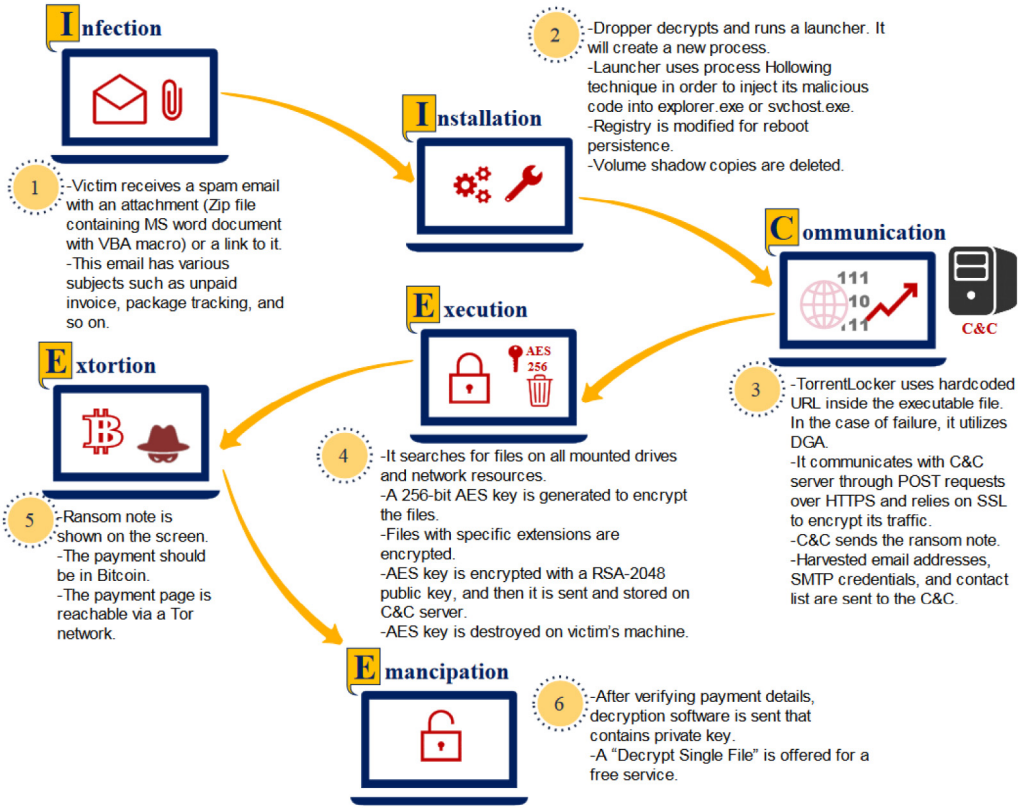

Fig. 4. TorrentLocker attack based on the I2CE3 chain.

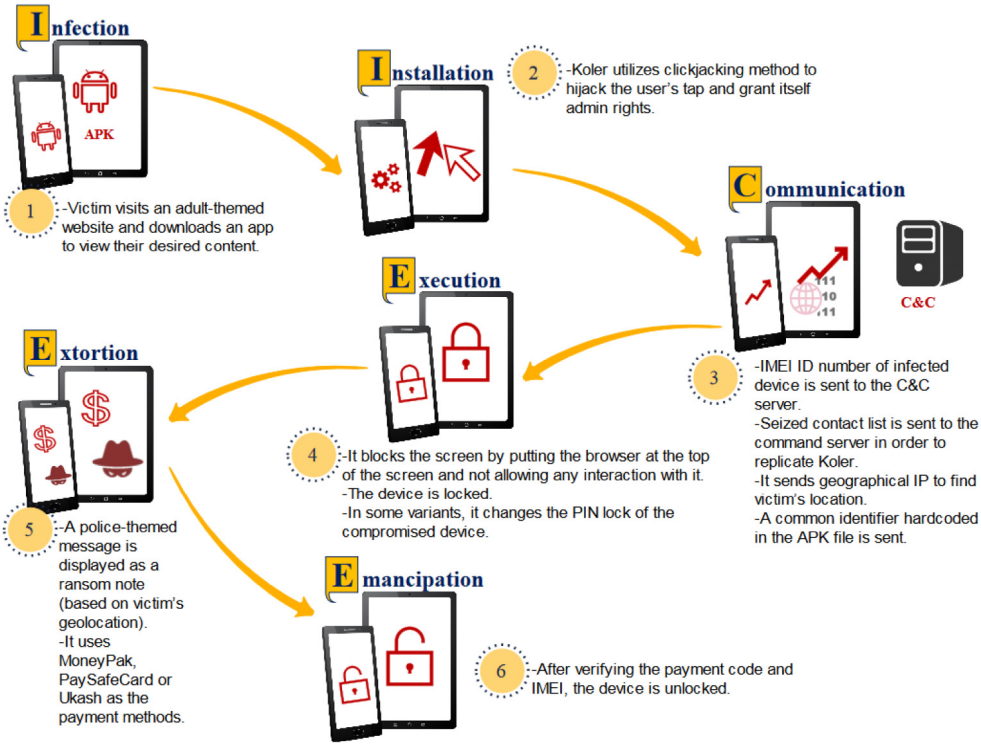

Fig. 5. Koler attack based on the I2CE3 chain.

For example, early versions of TorrentLocker adopted AES algorithm in CTR (Counter) mode to encrypt data resources. However, due to an error resulting in easy decryption, later versions replaced the mode of operation from CTR to CBC (Cipher Block Chaining) [36,51,52]. TeslaCrypt uses AES and leverages CBC as its mode of operation. Petya and NotPetya, which are included in the Wiper-Ransomware category according to our proposed classification, utilize stream cipher Salsa20 for disk encryption.

Table 2
Indicators extracted from some ransomware samples based on I2CE3.

Ransomware samples	Indicators involved in the					
	Infection phase	Installation phase	Communication phase	Execution phase	Extortion phase	Emancipation phase
Cerber	-Spam email -Exploit kit -Malvertising	-Malicious NSIS installer -Code injection -Deleting volume shadow copies -Registry modification for persistence	-Minimal network activity -Using DGA -Transmitting statistics	-Encrypting -Listing directories -Stealing Bitcoin wallet	-Pay money (Bitcoin) -Tor	-Decrypting
WannaCry	-Vulnerability exploitation -Self-propagating	-Deleting volume shadow copies -Registry modification	-Using hardcoded URL	-Encrypting -Listing directories -Enumerating RDP session	-Pay money (Bitcoin) -Tor	-Nothing
CryptoLocker	-Spam email -Vulnerability exploitation	-Code injection -Deleting volume shadow copies	-Using DGA -Key exchange -Transmitting statistics	-Encrypting -Listing directories -Stealing contacts -Modifying MBR	-Pay money (cashU, Ukash, MoneyPak, and Bitcoin)	-Decrypting
Locky	-Spam email -Exploit kit	-Malicious NSIS installer -Deleting volume shadow copies	-Using hardcoded URL -Using DGA -Key exchange -Transmitting statistics	-Encrypting -Listing directories	-Pay money (Bitcoin) -Tor	-Decrypting
Petya	-A malicious update of an accountability software (M.E.Doc) -Vulnerability exploitation	-Process evasion -Installing backdoor -Privilege escalation	—	-Installing its own custom OS -Encrypting file system during boot disk -Listing directories -Stealing credentials -Modifying MBR	-Pay money (Bitcoin)	-Nothing

The general availability of cryptographic libraries and the easy use of them is one of the key factors in the rapid growth of noxious ransomware attacks in recent years. In addition to the role of encryption in Crypto and Wiper-Ransomware groups, this technology is also used to secure the communication between ransomware and its C&C server [52]. Since many ransomware families get the encryption key when they communicate with the C&C server, it is very important to secure C&C communication for success. Encryption techniques make difficult to detect malicious C&C communication at the network level. The gangs behind ransomware attacks use miscellaneous methods to secure C&C channel. For instance, CryptoWall version 3.0 performs communication with its command center over the I2P network, whereas previous versions leveraged Tor to obfuscate C&C communications [51]. Onion routing – one of the anonymous communication items which is usually offered in most ransomware attacks – also uses the cryptography technology. It utilizes multiple and nested encryption processes in order to achieve privacy.

Role of social engineering. Social engineering has always been a popular tool in the hands of scammers. In the early 2000s, it became more aggressive in cyberattacks [22]. According to our proposed six-step chain for ransomware attack, social engineering techniques play a vital role in the infection and extortion phases. Typically, social engineering is employed in the ransomware attack by stimulating user's emotions, such as curiosity, fear, urgency, and so on to perform an action. Given the progress and complexity of security measures, it is possible to say that social engineering techniques are the easiest way to propagate malware. As mentioned before, one of the major vectors of pollution which requires user interaction is spam email. Most ransomware attacks are initiated by enticing victims into visiting a malicious webpage or opening an infected attachment in the phishing email through social engineering techniques. To this end, many ransomware spam campaigns are disguised as routine correspondence, such as invoices and delivery notification [35]. Locky, one of the most notorious ransomware in 2016 used this method to disseminate and stir up users to receive malicious attachment.

The main psychological factor for blackmail in scareware attacks is fear. Various ransomware families also leverage social engineering strategies to take advantage of the people's fear in the extortion phase. Many ransom notes contain countdown timer, which means that criminal groups will increase the amount of ransom exponentially or, in some cases, will eliminate a number of files forever after the expiry date. In addition, the specified deadline will lead to discouraging victims from seeking therapeutic solutions and making mistakes in their decision-making. These menacing tricks will be more effective in companies and organizations such as hospitals, where "time" plays a crucial role, so that most victims consider themselves forced to pay ransom. WannaCry, SamSam, Defray, and BitPaymer are examples of this case.

Role of botnet. Spam botnets are one of the main pillars of cybercrime attacks on a large scale. Given that spam phishing email is one of the major infection vectors, the issue of spam-sending botnets must be considered as one of the key actors involved in distributing ransomware. In brief, botnets are a network of hundreds to millions of compromised machines so-called zombie under the command of a botmaster. Botnet-based spam campaigns by programming a large number of distributed bots are able to transmit tens of thousands of spam emails to many users in a short time interval [53]. Botnets have always played a palmary role in many cyberattacks, including DDoS, banking Trojans, money mule spamming, ransomware, and crypto miners.

The architecture of botnets varies from simple client–server models to peer-to-peer designs. CryptoLocker, one of the worst and most infamous ransomware in 2013, has been using Gameover ZeuS botnet to be released to its victims [7]. ZeuS was a peer-to-peer botnet that employed Cutwail spam botnet to transmit massive amount of seductive phishing emails. It was mostly used for financial crimes. Necurs, one of the largest known botnets in history with many infected bots, was mounted by ransomware distribution campaigns in order to send spam

emails to several million users. It has been involved in many cybercrime offenses, from launching DDoS attacks to distributing malware. The Necurs's track has been discovered in the spread of ransomware, including Locky, Jaff, GlobeImposter, and Scarab [35,37]. Reportedly, Necurs botnet has earned a lot of revenue from the delivery of malware like Locky ransomware and Dridex banking Trojan. However, after a significant interruption, its revitalization has turned towards more sophisticated frauds such as pump-and-dump stock scams.

Kelihos was another marvelous botnet that offered "spam as a service" to its customers [54]. It was leveraged for disseminating some ransomware families, including Troldesh (also known as Shade), Wildfire, CryptFlle2, and MarsJoke. The usage of botnet in ransomware attacks can be much more dangerous than what has been seen so far. Virobot was the latest known ransomware in terms of novel use of botnet technology at the time of writing this article. Virobot, identified by Trend Micro as RANSOM_VIBOROT.THIAHAH [55], is a new strain with both ransomware and botnet capabilities. It means that once Virobot hits a device, in addition to encryption, the infected machine becomes part of a spammer botnet to send the ransomware itself to more victims.

Role of anonymous networks. One of the uses of anonymous networks is their usage in digital extortion attacks. There are many reasons for employing anonymous network technology in the cybercrime. The most prominent of them is the lack of traceability by law enforcement agencies and authorities. The use of anonymity in communications neutralizes the embedded blacklisting strategies in many security tools. This technology is clearly evident in the three phases (i.e., communication, extortion, and emancipation) of the proposed I2CE3 chain. Many ransomware families leverage a variety of anonymous networks like Tor and I2P to communicate with C&C server for bypassing network traffic inspections. Tor is an overlay network that provides anonymous communication between entities over TCP. It employs a set of volunteer machines to direct Internet traffic. The anonymity of communication parties is usually achieved through the onion routing. In the onion network, the messages are encapsulated into layers of encryption. However, this technique may be defeated by methods such as timing analysis. I2P is another example that provides an anonymous peer-to-peer communication through end-to-end encryption. It employs garlic routing for this purpose. CryptoWall version 3.0 is a typical ransomware that utilizes I2P in order to establish connection with its command center [51].

Underground markets mainly utilize anonymous networks in combination with cryptocurrencies like Bitcoin to trade and smuggle goods. Basically, the criminals behind ransomware provide victims with hidden service URLs on the ransom note that need to install applications like Tor Browser or use services like Tor2web in order to access them (for paying ransom and releasing hostage resources). This kind of communication prevents eavesdropping of network traffic. For example, in phases of extortion and emancipation after completing file encryption, CTB-Locker will perform all communications over Tor. This is usually done via multiple proxy websites, which act as relays to the Tor hidden service [36]. TeslaCrypt displays a ransom note to the victim in which instructions are provided to access Tor hidden service and how to pay ransom in Bitcoin. Similarly, Cerber ransomware provides the user with a list of Tor2web gateways for payment [56].

Role of DGA. C&C servers are a vital part of many ransomware families that play the coordinating role of the attack elements. The vast majority of ransomware species have to communicate with their C&C server in order to carry out devastating acts, or after receiving ransom, to clean up the victim's machine and release the resources. The C&C server address can be hardcoded in the forms of IP addresses or domain names inside the malware binary itself, which can be easily detected and blocked through static analysis. In many cases, the durability of the attack depends on the availability of the command center and the receipt of instructions from it. Ransomware campaigns leverage various techniques to bypass security systems to prevent their C&C servers from taking down. This is where DGAs come into play as a secret mechanism for communicating with C&C servers. Applying this technology will make it harder to turn off C&C servers at least until the algorithm is completely reverse engineered.

Domain generation algorithms periodically produce a large number of pseudo-random domains based on a seed value over a short period of time. These domains are often gibberish strings that are appended to a top level domain (TLD). Generated pseudo-random domains are divided into six distinct groups according to their structural layout by [40]. The bot herders, who handle C&C servers, register one or a few of the generated domain names. Ransomware sends DNS queries to the generated domains to resolve and connect to the one that is registered. Hence, several NXDomain responses may be made due to these queries [56,57]. The number of domain names varies depending on the structure and design of DGA. For example, Gameover ZeuS generates 1000 unique domains per day [40,42]. This method helps to fortify attacks against blacklisting strategies and signature-based techniques. Although there are still weak points in this technology, the use of dynamic seeds in ransomware species that communicate with C&C via DGA mechanism helps to strengthen their command servers against sinkholing approaches.

Role of cryptocurrency. Ransomware is one of the swiftest evolving industries for the reason that it offers a way to make money with requiring little skill or effort. However, in the current era, cybercriminals are no longer solely motivated with financial incentives, but also by political motives. Thus, the ransom demanded by the adversary may be either monetary or non-monetary depending on the purpose of the attack. Cybercriminal groups need to secure financial transactions to ensure the success of the attack. Therefore, they tend to use global and decentralized monetary systems rather than fiat currency. Digital currency and blockchain technology have created monetizing opportunities for cybercrimes by eliminating intermediaries and providing anonymity.

Today, cryptocurrency has become a hot topic in computer security forums, as its footprint has been seen in many attacks such as ransomware, crypto miners, and phishing scams. Cryptocurrencies are fueling the success of ransomware attacks due to their almost untraceable nature. With the appearance of Bitcoin in 2009 as the first decentralized cryptocurrency, a revolution was sparked in the world of underground economies, and the attention of cybercriminals was drawn to this new way of transferring money. Bitcoin is a peer-to-peer cryptocurrency that employs a publicly available shared transaction ledger, known as the blockchain [7,47]. In the majority of ransomware attacks, such as WannaCry, payment is made with Bitcoin. One of the difficulties of digital currency to use in cyberattacks is the fluctuation of the market, which leads the criminal groups not to know exactly how much they demand from their victims. Hence, some ransomware families like Scarab add negotiation capabilities over the amount of ransom in the extortion phase [58]. In addition to Bitcoin, which is one of the most widely used payment methods for ransomware attacks, other cryptocurrencies like Monero are becoming more and more popular among offenders. This kind of cryptocurrency has additional security and privacy features that prevent transactions from being tracked. For example, Kirk ransomware utilizes Monero as a ransom payment option.

Role of RaaS. Over the past few years, ransomware threats have soared dramatically. One of the reasons for this progress is the

concept of ransomware-as-a-service, called RaaS. The emergence of RaaS platforms has equipped any of users with malevolent intent for creating their own ransomware variants, even sans previous knowledge. In this way, the main authors of ransomware focus on the development and promotion of malicious code and delegate its propagation to affiliates [15]. By dint of easy access to RaaS, cybercriminals can comfortably move to the website providing RaaS and only by little effort build their own ransomware variant. The RaaS provider groups pocket a portion of ransom revenue for every successful infection.

RaaS provides good monetizing opportunities for the owners of botnets or those who have access to many computers in any way. Tox and Shark are examples of RaaS platforms. Operators of such platforms mainly use anonymous networks such as Tor to offer their services. Also, many notorious ransomware families, like Cerber, leveraged this business model to spread widely among users and gain more profit. So RaaS can be considered as one of the factors behind the success of ransomware attacks [9].

6. Defensive approaches based on attack chain

Cybersecurity threats are constantly evolving and offenders are looking novel ways to bypass protective systems. Over the past few years, the cyber world has witnessed a variety of ransomware attacks with intimidating trends. This kind of malware has rapidly become one of the most pernicious cybersecurity threats facing individuals and enterprises around the world. Different ransomware families engage a variety of techniques to eschew from circumvented by security monitoring systems. As the outcome of a ransomware attack is almost irreversible, prevention methods and/or detection in early stages must be in preference. Defense against ransomware attacks is somewhat similar to repelling procedures in the other cyberattacks. These signature or anomaly-based approaches are either deployed as a traffic monitor in the network or as an endpoint protection solution in the host. Since in practice there are limitations in signature-based strategies, especially with respect to remarkable growth of ransomware variants and employment of anti-forensic techniques such as packing and obfuscation, behavioral detection approaches have attracted much consideration in the cybersecurity scope. As a result, behavior-based solutions are more effective due to their capabilities to offer detailed characteristics and recognize zero-day attacks. However, these techniques also suffer from restrictions including high rate of false positive, noticeable consumption of resources, and difficulty of implementation.

Typically, defensive approaches include analysis, detection, prevention, and recovery. Here, we will categorize and investigate the state-of-the-art defensive research efforts against ransomware from the view point of our proposed I2CE3 attack chain. Table 3 summarizes some of these studies, which are described in the following sections.

6.1. Defense at the infection phase

The most operative strategy for circumventing any attack relies on preventing that in the first place. Understanding how various strains of ransomware infect devices is crucial for counteract such threats. Because most ransomware species are being delivered through malicious attachments or links included in phishing spam emails, analyzing and protecting emails is an essential subject. The investigation of spam emails and their malicious contents can collaborate on the analysis of ransomware variants and assist to recognize that in the first place, before infecting system. Malicious attachments which lead to infection and ransomware release are mainly in the format of MS Office, pdf, or Zip files. Solutions such as disabling macros in Microsoft Office documents for users who are willing to take advantage of full functionalities will not be desirable. Also, these solutions do not have generalization to other types of files containing malicious payload.

As adversaries use social engineering techniques to succeed in the infection phase, educating users is a clear strategy that is recommended in most literatures. However, some research efforts have technically addressed the issue of detecting spam emails and malicious content. Many studies in the field of detecting spam emails and phishing sites can also be extended to ransomware attacks [79–81]. [82] focuses on mobile phishing attacks and defense mechanisms against them, and offers a comprehensive taxonomy of suggested strategies. In order to detect malicious email, a novel set of general descriptive features is presented in [83]. The authors leveraged machine learning methods on their proposed features, which were extracted from the email components, and evaluated Random Forest as the best classifier in their results. Rudd et al. [84] utilized machine learning methods to distinguish malicious email attachments from benign ones. They employed two classifiers (i.e., deep neural networks and gradient boosted decision tree ensembles) on their provided dataset. The method presented by them examines two types of attachments; Zip archives and Microsoft Office documents. Another solution that can be used in the infection phase is spam trap, which is in the honeypot category [85].

Infection vectors in Android ransomware families mainly include malicious apps offered as legitimate programs in app stores and malicious landing pages linked in SMS or other media to the users. Although mobile ransomware inflicts less damage than its counterparts, they should be considered a serious threat due to the widespread use of mobile devices. Alzahrani et al. [59] introduced RanDroid, an automated lightweight approach to identify Android ransomware species. RanDroid is designed for inspecting APK files before installing them on the users' devices. It leverages both static and dynamic analysis to extract information, such as the appearance of locking screens and threatening strings, from APKs. In the case of ransomware variants, which employ worm-style propagation methods, limiting access on network shares can be a cure. Also, as mentioned earlier, another common method for delivering ransomware is exploit kit. Exploit kits are toolkits that automate the exploitation of vulnerabilities. Using exploits donates a facility to the attackers that they will not require user interaction and social engineering. In such cases, updating the operating system and applications and refusing to install unnecessary programs or obsolete plugins can be very helpful.

6.2. Defense at the installation phase

Regardless of what the infection vector is, the malicious payload is delivered to the victim's system, either as an executable binary or as a script or macros embedded in the file, and needs to be installed to continue the attack process. The best defense strategies in this stage are file and process monitoring at the endpoint. However, these approaches are applied with a slight change in the execution phase. Static and dynamic analyses are two main methods for examining file and producing dataset of signatures related to benign and mal code. Static analysis is a fast way to investigate files and detect potentially malicious code. Since static approaches do not actually run the code, they are unable to identify ransomware families, which engage sophisticated techniques. Furthermore, like other malware, most ransomware species utilize obfuscation and packing techniques to thwart static analysis and bypass security systems. Hence, dynamic analysis method (also known as behavior analysis) comes into play. The dynamic techniques by executing code in a controlled environment will be able to observe its behavior and

Table 3
Classification of research related to defense against ransomware based on attack chain.

Reference	Defense at infection	Defense at installation	Defense at communication	Defense at execution	Defense at extortion	Defense at emancipation
Young et al. [5]				✓		
Liao et al. [7]					✓	
Ahmadian et al. [20]			✓			
Kharraz et al. [25]				✓	✓	
Kharraz et al. [26]				✓		✓
Continella et al. [43]		✓		✓		✓
Xu et al. [44]		✓				
[46–48]					✓	
Antonakakis et al. [57]			✓			
Alzahrani et al. [59]	✓					
Lestringant et al. [60]		✓				
Andronio et al. [61]	✓	✓	✓			
Mercaldo et al. [62]		✓				
Sgandurra et al. [63]		✓		✓		
[64–68]		✓				
Cabaj et al. [69]			✓			
Almashhadani et al. [70]			✓			
Scaife et al. [71]				✓		
Gómez et al. [72]				✓		
Spagnuolo et al. [73]					✓	
Lee et al. [74]	✓					✓
[75–78]						✓

capabilities. For this purpose, techniques such as sandboxing are used to create signatures for new and unknown ransomware. These analytic tools will help to monitor and scrutinize processes, registry modifications, and network activity, which are the main pillars of the ransomware installation phase.

Continella et al. [43] addressed code injection problem and provided how to cope with it. Their proposed mechanism considers both the short and long history of each process and the entire system. Detecting the encryption function inside the binary code is another solution that can be used in the installation phase and engaged as a complementary method to the security tools. Lestringant et al. [60] suggested an approach to automatically recognize cryptographic primitives inside binary code. Their method is based on Data Flow Graph (DFG) isomorphism. Since DFGs are a natural way of displaying dependencies between operations, they are deserved to be used in the identification of the cryptographic algorithm. In the proposed approach, first of all, the DFG is constructed corresponding to the input binary code. Then this DFG is normalized using rewrite rules. Finally, subgraphs in the DFG which are isomorphic with the signature of a given cryptographic algorithm are searched. Given that the last two stages are computationally intensive, in order to achieve acceptable performance, binary code must be fragmented and used as input. Xu et al. [44] introduced CryptoHunt, which is able to recognize commonly used cryptographic functions including TEA, AES, RC4, MD5, and RSA inside the binary code, even under various obfuscation conditions. They proposed a technique called bit-precise symbolic loop mapping for this purpose. HelDroid developed by Andronio et al. [61], targets to detect mobile ransomware on the Android devices. It is based on static analysis and considers the behavior of ransomware at the application layer. The authors applied a text classifier based on NLP features to identify threatening phrases. The diagnostic power of the suggested method depends on the training dataset. Mercaldo et al. [62] developed a detection approach based on formal methods to recognize ransomware code instructions in Android platform. Their methodology identifies ransomware families through the application's Bytecode, instead of source code. For this reason, it is independent of the source programming language and obfuscation tricks. The authors reused existing sophisticated model checkers to avoid performance degradation. EldeRan [63] was presented as a machine learning approach to analyze ransomware attacks dynamically and classify them. For this purpose, it monitors applications' early activities during in their installation phase. In this framework, the most relevant dynamic features of ransomware are identified through the Mutual Information (MI) criterion. EldeRan leverages Regularized Logistic Regression classifier due to its speed, easy to train, and update capabilities in order to distinguish ransomware from goodware. Researchers in [64] suggested a method based on structural entropy and fuzzy logic algorithms in order to discriminate between Android ransomware and legitimate mobile application. They performed their analysis directly on the executable files. The approach presented in [65] was the latest work in the field of detection ransomware during the installation phase at the time of writing this article, which was provided to overcome the weakness of dynamic strategies. Zhang et al. [65] perform ransomware classification based on static analysis. They do this by transforming the opcode sequences of ransomware samples into N-gram sequences and then calculating TF-IDF for each to select feature N-grams. The authors employed five machine learning algorithms to build classification models and applied their models on 1787 ransomware samples from eight families. They declare their proposed methodology attains high accuracy in both binary and multi-classifications.

[66] utilized sequential pattern mining technique to identify and extract best features of crypto-ransomware programs in order to classify and distinguish them from benign applications. The applied dataset by them involved logs of Dynamic Link Libraries (DLL), registry, and file system activities. These logs were collected from the first 10 s of running ransomware and benign programs. Finally, they leveraged classification algorithms including J48, Random Forest, Bagging, and MLP to evaluate usefulness of their selected features. Also, Homayoun et al. [67] presented a system called DRTHIS, deployable on the fog layer, to detect

ransomware and identify their respective families. They utilized and compared two deep learning techniques, namely Long Short-Term Memory (LSTM) and Convolutional Neural Network (CNN) for classification. They again used the sequence of operations performed by both ransomware and benign application instances in the first 10 s of implementation. Another research work has proposed by Rhode et al. [68], which is able to predict the harmfulness of the file within the first 5 s of its execution. They have employed a recurrent neural network (RNN) model to predict malicious behavior. Author's argument for using machine activity features as the model inputs instead of using API calls is that the API calls are vulnerable against tampering and cause mistakes in the classification of samples by neural networks. They also state that RNN models outperform other machine learning classifiers and are more resistant to overfitting. Although the last three approaches can be deployed in the execution phase, we mention them in this section. Because the former merely focuses on feature extraction and classification problem, and the latter takes into account the reduction of dynamic detection time and use of neural networks, both of which can be run in the sandbox environment. The first part of the work presented in [26], that is, an abstract description of the behavior of a large class of current ransomware attacks can also be implemented in this phase.

6.3. Defense at the communication phase

Many cyberattacks need to communicate with their command center in order to complete the attack process, propagate and infect more devices, or exfiltrate the victim's information. Ransomware is no exception. In many of ransomware families employing asymmetric cryptography, since the key pair is generated only after a successful connection with C&C server, if communication is disturbed by security measures or never established, the attack will not arrive at the destructive execution phase. Accordingly, deploying a defensive approach at this stage can be effective in preventing further damage. Identifying malicious C&C communications is not a new topic and has been considered for a long time. Some ransomware campaigns use the hardcoded IP addresses or domain names in the binary itself for communications that can be easily discovered by static analytical tools. This list of domain and IP addresses known as malicious can be used in network signature-based monitoring systems. Therefore, in order to evade network security tools, many ransomware strains employ DGA to establish channels and communicate with C&C server. This tactic neutralizes blacklisting and signature-based approaches in the network. As a result, the discovery and recognition of DGA traffic and the use of techniques such as machine learning, information retrieval, and data mining will help to design more effective solutions to combat ransomware attacks in the communication phase.

The distinction of malicious C&C traffic from legal traffic has long been studied, especially in the context of botnet recognition. The solution presented in [57] addresses the issue of detecting randomly generated domains by DGA without the need for malware reverse engineering. The insight behind this method is that the queries made by malware or bot will lead to Non-Existent Domain (NXDomain) responses. Ahmadian et al. [20] proposed an approach to recognize DNS requests issued by the DGA in ransomware families that apply this method to discover and connect to the live C&C server. The authors leveraged Markov chain to detect gibberish queries. They claim that their proposed framework is able to identify ransomware species which use DGA for communicating with command center and exchanging public key. Also, the work presented by Andronio et al. [61] could be extended to this phase. This means that they use an approach to detect the process of capturing the threatening text from C&C server, where such a text is not embedded in the ransomware payload. Cabaj et al. [69] presented a Software-Defined Networking (SDN)-based system for detecting Crypto-Ransomware. Their method was exclusively inspired by their observations on the traffic characteristics of two ransomware families, namely CryptoWall and Locky. They argue that analyzing the sequence of HTTP messages and their respective content size is enough to recognize such threats. Almashhadani et al. [70] investigated network traffic of crypto ransomware, using Locky as a case study. After a behavioral analysis, they proposed a network-based classification method to detect attack.

6.4. Defense at the execution phase

Although the defense in the execution phase is somewhat late, it may be argued that the most practical defense solutions for previously unknown ransomware families are deployed in this stage. DoDR ransomware requires files' read and write operations to encrypt or tamper their content. One of the most effective and commonly used methods for defending ransomware in the execution phase is to monitor file system activity by various approaches, including hooking the System Service Descriptor Table (SSDT). Also, in Crypto-Ransomware class, a defense strategy is to take advantage flaws in the design and implementation of cryptography algorithms. In the case of using symmetric cryptography, since the key remains in the victim's machine until the user is online and the key is sent back to the C&C server, memory forensic tools can be leveraged for memory dump. Another security measure at this stage is the review of folder-listing operations that are common in ransomware families. However, file system scanners also exhibit this behavior. Monitoring and protecting the Master File Table (MFT), which contains information about all stored files and directories on the NTFS volume, is one of the defense strategies in the execution phase. Due to the manipulation of the MBR in digital extortion attacks, especially in the Locker-Ransomware category, observing MBR changes is also suggested at this stage.

Controlling and restricting access to cryptographic tools suggested by Young et al. [5] may be the first countermeasure that has been proposed in extortion attacks which focuses on the execution phase for defense. However, this method is unable to detect ransomware instances that employ embedded encryption methods inside their own. As mentioned, in the execution stage, ransomware avidly traverse the file system in order to seek the target files. Continella et al. [43] proposed ShieldFS, an add-on driver that protects the Windows native file system against ransomware threats. It makes a set of adaptive models containing more than 1.7 billion I/O request packets (IRPs) produced by distinct benign applications, and updates it by monitoring the low-level file system activity over time. The proposed approach combines this information with data, such as write entropy, timestamp, and so on in order to distinguish ransomware from goodware. Any process that violates such models will be detected as malicious and its operation will be rolled back. Moreover, ShieldFS looks for indicators that illustrate the use of symmetric cryptographic primitives. To this end, it investigates the memory of potentially mal processes for traces of the typical block cipher key schedules. Kharraz et al. [25] stated that by looking at I/O requests and protecting MFT in NTFS file system, it is possible to detect and prevent a significant number of new ransomware attacks. In another effort, the authors designed a dynamic analysis system called UNVEIL [86] that was able to analyze, recognize, and model the behavior of ransomware attacks. Their techniques are based on monitoring file system accesses and examining dissimilarity scores of screenshots taken before, during, and after the execution of ransomware. The file

system monitoring component in UNVEIL has direct access to data buffers involved in I/O requests. It observes file system I/O activity through the Windows Filesystem Minifilter Driver instead of using hooking techniques. In the case of Locker-Ransomware category, authors leveraged an open source OCR engine to extract threatening text (common in ransom note) from screenshots. However, UNVEIL was not an endpoint solution, and was designed with the aim of analyzing and modeling ransomware attacks. Kharraz et al. [26] proposed Redemption as an endpoint security solution that was able to distinguish malicious accesses to the file system from benign ones. According to the authors, it requires minimal editing in the OS.

Given that some types of ransomware employ their own encryption function, it is not adequate to only supervise calls to standard cryptographic libraries. Hence, Scaife et al. [71] proposed a data-centric approach called CryptoDrop to detect and stop ransomware attacks that tend to manipulate files. Instead of monitoring programs, CryptoDrop inspects user data for suspicious changes. The authors utilized three primary indicators to recognize these malicious changes; file type changes, similarity measurement using hash function, and Shannon Entropy. Kim et al. [87] proposed a white list-based ransomware detection method. They applied an access control policy to the file operation procedure. The whitelist contains records of application usage patterns and does not need to be updated by a trust party. Their proposed scheme consists of file monitoring component in the kernel mode, an access control component in the user mode, and an access control DB. Their method only focuses on document and system files. The authors in [72] introduced an approach based on honeyfiles to detect and frustrate ransomware attacks. As soon as the honeyfiles deployed around the target environment are read by the malicious process, the proposed tool called R-Locker blocks the attack.

6.5. Defense at the extortion phase

The gangs behind ransomware attacks not only look for secure and untraceable, but also easy payment and exchange methods for victims. The most prominent digital currency used in cybercrime is Bitcoin. However, the footprint of Monero has also been seen in Internet attacks, especially crypto miners. Assenting victims to pay ransom demands can assist to fortify hackers behind ransomware, whilst there is no guarantee of recovering data and repeating this attack on the same victim. While many of the destructive operations have been carried out before the extortion phase and access to resources has been prevented, this stage can also provide an opportunity for defense.

Most studies on defending in the extortion phase focus on analyzing and categorizing Bitcoin transactions. For example, Liao et al. [7] considered the issue of analyzing Bitcoin transactions by examining the ransom payment timestamps, in the case of CryptoLocker. Huang et al. [48] performed an end-to-end analysis of a large portion of ransomware ecosystem, including its revenue, affiliate schemes, and infrastructures. They tracked financial transactions of several ransomware families from the moment a victim acquires Bitcoin until the ransomware operators cash it out. Spagnuolo et al. [73] presented a modular framework called BitIodine that was able to parse the blockchain and cluster addresses belonging to a same entity. They released this framework to build Bitcoin forensic tools. The authors paid special attention to the visualization of information extracted from the Bitcoin network. Also, a study by Kharraz et al. [25] enounces that Bitcoin addresses used for malicious purposes share similar transaction records, including short duration of activity, small amounts of founds, small transaction records, and so on. In fact, they differentiate and categorize the addresses based on the transaction history. A study by Conti et al. [46] highlighted the economic impact of ransomware attacks in terms of Bitcoin payment. The authors also provided a framework for identifying, collecting, and analyzing Bitcoin addresses managed by the same user. They released a dataset containing the identified Bitcoin addresses belonging to the ransomware attacks. In [47], a data-driven method for identifying and collecting information on Bitcoin transactions associated with illegal activity is presented based on the footprint of the public Bitcoin blockchain. The authors implemented this method on the GraphSense, an open-source cryptocurrency analytics platform, and employed it for empirical analysis of transactions related to 35 ransomware families.

6.6. Defense at the emancipation phase

Identifying ransomware family via information included in the ransom note left on the victim's machine or by analysis methods can be useful for unlocking or decrypting affected files. Because, some of ransomware variants already have been discovered by third-party security companies and released their countermeasures. Therefore, all studies that have identified ransomware families can also be used at this phase. When a victim gives a ransom to regain access to the resources, she/he creates this feeling in other criminal gangs that target her/him in the same or different ways for similar extortion attacks [10]. A needless solution of paying ransom is having a faultless backup plan. In addition to defensive solutions, having a backup plan to counteract and mitigate effect of ransomware attacks is commodious. Backup files should be maintained in a safe and isolated location that is not open to the influence of ransomware threats. Because some of ransomware families have begun to target backup files as a part of their execution phase. Inspecting the accuracy of backups and recovering files from them in a testbed should be considered as a part of backup plan.

Continella et al. [43] employed a shadowing mechanism on the write operations in order to recover damaged files. CloudRPS [74] provides users with a backup plan alongside analyzing and preventing ransomware attacks. Subedi et al. [75] suggested RDS3 and implemented it as a ransomware defense strategy. RDS3 provides recovery capability by stealthily backing up data in the spare space of a computing device. In the proposed framework in [26], by mediating requests for access to files and redirecting privileged requests to a protected area, a consistent state of the user's original data is maintained, which leads to provide remedy capabilities. Lee et al. [76] proposed an approach for recovering files and systems infected by ransomware through a backup technique. Their methodology is that when the ransomware calls functions of the cryptographic library, the proposed program is triggered and stores the secret keys in a safe repository. The assumption used in the article is that ransomware writers use ready-made cryptography libraries, such as CNG on the Windows platform. Kolodenker et al. [77] implemented PayBreak as a proactive defense mechanism against Crypto-Ransomware threats. The proposed model monitors programs that invoke cryptographic functions and intercepts calls to such functions. Then by introducing a key escrow mechanism, symmetric session keys are stored securely in a key vault. By providing this capability, PayBreak allows victims to retrieve infected files without paying the ransom. FlashGuard presented in [78] is a ransomware tolerant Solid State Drive (SSD) that provides a firmware-level recovery system. Its designers modified the garbage collection mechanism of the SSD to hold secure the copies of the affected and encrypted data. As a result, it is able to restore all the overwritten pages by traveling back to their previous versions.

7. Conclusion and open challenges

Over the past few years, cybercrime attacks like ransomware, Doxware, and malicious crypto miners have made significant headlines in the wild. Cybercriminals are unremittingly looking for innovative methods in order to conduct digital extortion based on people's fear. Ransomware has been considered as one of the most successful ways of earning money through extortion in the underground market. The worm-style delivery mechanisms have introduced a rapid distribution for ransomware campaigns. Thanks to RaaS business model, the ransomware industry has become more prosperous, and bad guys can easily own customized ransomware without much skill and time. Based on the incremental growth in ransomware industry and rapid return of investment, one expects that ransomware developers will carry on accoutering their own variants with new features and capabilities to extend objective realm and juice up their business. Therefore, developing a protection mechanism against such type of attacks is very important. However, it is almost impossible to design effective defense systems without having a general understanding of these threats.

Although there have been many studies on ransomware, there is still a lack of a comprehensive classification of extortion attacks. In many critical organizations that consider payment as the only option, knowing the type of attack can lead to different decisions. In this paper, we focused on the fear-based attacks, especially ransomware, and provided an exhaustive taxonomy that covers all of the new samples. Another aspect of our research is to propose a six-step specialized attack chain called I2CE3 for such threats. Separating the attack process into different sections and understanding the technologies employed in each phase, in addition to formulating the problem, can help to identify the behavior patterns exhibited by ransomware and provide effective defensive strategies. We believe that the indicators identified at each stage enable security professionals to establish their solutions in accordance with these indicators and to eliminate the attack in the early phases. As the evolution and maturation of ransomware is influenced by the growth of technologies, we mentioned the most important technologies involved in the attack, and described the role of each of them. Finally, we categorized a majority of related work based on proposed chain.

Despite ongoing researches in the field of ransomware, several challenges remain that need to be addressed. One of the major challenges is the lack of a complete database of ransomware instances with representative features, so that articles based on machine learning and statistical techniques can use a common dataset to test their method and compare it with others. This is part of our future research program. Considering the categorization of research studies, it can be seen that there has been a greater focus on providing defensive solutions in the execution phase at the expense of sacrificing a number of files. Due to the irreversible effects of this attack, more work is needed on preventive solutions in the pre-execution phases. Extracting distinctive features at the installation stage is also another interesting topic for research.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

References

[1] Industrial Enterprise and IoT Security Threats: Forecast for 2018, Kaspersky Lab. https://ics-cert.kaspersky.com/reports/2017/11/30/industrial-enterprise-and-iot-security-threats-forecast-for-2018.

[2] 2017 Internet Crime Report, IC3, 2018, https://pdf.ic3.gov/2017_IC3Report.pdf, (Accessed June 2018).

[3] 2018 Data Breach Investigations Report, Verizon, 2018, https://www.verizonenterprise.com/resources/reports/rp_DBIR_2018_Report_execsummary_en_xg.pdf, (Accessed June 2018).

[4] J. Bates, Trojan horse: AIDS information introductory diskette version 2.0, in: E. Wilding, F. Skulason (Eds.), Virus Bulletin, Virus Bulletin Ltd, Oxon, UK, 1990, pp. 3–6.

[5] A.L. Young, M. Yung, Cryptovirology: Extortion-based security threats and countermeasures, in: J. McHugh, G. Dinolt (Eds.), Symposium on Security & Privacy, IEEE Computer Society, Washington, DC, 1996, pp. 129–141.

[6] N. Lee, Cyber warfare: weapon of mass disruption, in: Counterterrorism and Cybersecurity, second ed., Springer, New York, NY, 2013, pp. 99–118.

[7] K. Liao, Z. Zhao, A. Doupe, G.J. Ahn, Behind closed doors: measurement and analysis of cryptolocker ransoms in bitcoin, in: 2016 APWG Symposium on Electronic Crime Research, eCrime, June, 2016, pp. 1–13.

[8] CR. Srinivasan, Hobby hackers to billion-dollar industry: the evolution of ransomware, Comput. Fraud Secur. (11) (2017) 7–9, http://dx.doi.org/10.1016/s1361-3723(17)30081-7.

[9] B.A.S. Al-rimy, M.A. Maarof, S.Z.M. Shaid, Ransomware threat success factors, taxonomy, and countermeasures: a survey and research directions, Comput. Secur. (74) (2018) 144–166, http://dx.doi.org/10.1016/j.cose.2018.01.001.

[10] C. Everett, Ransomware: to pay or not to pay? Comput. Fraud Secur. (4) (2016) 8–12, http://dx.doi.org/10.1016/s1361-3723(16)30036-7.

[11] A. Azmoodeh, A. Dehghantanha, M. Conti, K.K.R. Choo, Detecting crypto-ransomware in IoT networks based on energy consumption footprint, J. Ambient Intell. Human. Comput. (2017) 1–12.

[12] S. Gibbs, Ransomware attack on san Francisco public transit gives everyone a free ride, 2016, https://www.theguardian.com/technology/2016/nov/28/passengers-free-ride-san-francisco-muni-ransomware, (Accessed June 2018).

[13] I. Yaqoob, E. Ahmed, M.H.u. Rehman, A.I.A. Ahmed, M.A. Al-garadi, M. Imran, M. Guizani, The rise of ransomware and emerging security challenges in the internet of things, Comput. Netw. (2017) http://dx.doi.org/10.1016/j.comnet.2017.09.003.

[14] A. Zimba, Z. Wang, H. Chen, Multi-stage crypto ransomware attacks: A new emerging cyber threat to critical infrastructure and industrial control systems, ICT Express (2018) http://dx.doi.org/10.1016/j.icte.2017.12.007.

[15] K. Savage, P. Coogan, H. Lau, The evolution of ransomware, SECURITY RESPONSE, 2015, Symantec Corporation.

[16] E.M. Hutchins, M.J. Cloppert, R.M. Amin, Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains, in: Proceedings of the 6th International Conference on Information Warfare and Security, 2011.

[17] P. O'Kane, S. Sezer, D. Carlin, The evolution of ransomware, IET Netw. 7 (5) (2018) 321–327, http://dx.doi.org/10.1049/iet-net.2017.0207.

[18] X. Luo, Q. Liao, Awareness education as the key to ransomware prevention, Inf. Syst. Secur. (16) (2007) 195–202, http://dx.doi.org/10.1080/10658980701576412.

[19] P. Bajpai, A.K. Sood, R. Enbody, A key-management-based taxonomy for ransomware, in: 2018 APWG Symposium on Electronic Crime Research, eCrime, San Diego, CA, 2018, pp. 1–12.

[20] M.M. Ahmadian, H.R. Shahriari, S.M. Ghaffarian, Connection-monitor & connection-breaker: A novel approach for prevention and detection of high survivable ransomware, in: Paper Presented At the 12th International Iranian Society of Cryptology Conference on Information Security and Cryptology, ISCISC, IEEE, Iran, Rasht, 2015, pp. 79–84, http://dx.doi.org/10.1109/ISCISC.2015.7387902.

[21] A. Pektas, T. Acarman, Classification of malware families based on runtime behaviors, J. Inf. Secur. Appl. (37) (2017) 91–100, http://dx.doi.org/10.1016/j.jisa.2017.10.005.

[22] F. Touchette, The evolution of malware, Netw. Secur. (1) (2016) 11–14, http://dx.doi.org/10.1016/S1353-4858(16)30008-3.

[23] A.L. Young, M. Yung, Cryptovirology: The birth, neglect, and explosion of ransomware, Commun. ACM 60 (7) (2017) 24–26.

[24] A.L. Young, Cryptoviral extortion using Microsoft's crypto API, Int. J. Inf. Secur. 5 (2) (2006) 67–76.

[25] A. Kharraz, W. Robertson, D. Balzarotti, L. Bilge, E. Kirda, Cutting the Gordian knot: A look under the hood of ransomware attacks, in: International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment: 12th International Conference, DIMVA2015, Springer, Milan, Italy, 2015, pp. 3–24.

[26] A. Kharraz, E. Kirda, Redemption: real-time protection against ransomware at end-hosts, in: M. Dacier, M. Bailey, M. Polychronakis, M. Antonakakis (Eds.), RAID 2017, in: LNSC, vol. 10453, Springer, Cham, 2017, pp. 98–119, http://dx.doi.org/10.1007/978-3-319-66332-6-5.

[27] C.N. Gutierrez, E.H. Spafford, S. Bagchi, T. Yurek, Reactive redundancy for data destruction protection (R2D2), Comput. Secur. 74 (2018) 184–201, http://dx.doi.org/10.1016/j.cose.2017.12.012.

[28] Symantec Security Response Team, What you need to know about the WannaCry Ransomware, 2017, https://www.symantec.com/blogs/threat-intelligence/wannacry-ransomware-attack, (Accessed June 2018).

[29] A. Dahan, Night of the devil: Ransomware or wiper? A look into targeted attacks in Japan using MBR-ONI, 2017, https://www.cybereason.com/blog/night-of-the-devil-ransomware-or-wiper-a-look-into-targeted-attacks-in-japan, (Accessed June 2018).

[30] C. Cimpanu, Ordinypt ransomware intentionally destroys files, currently targeting Germany, 2017, https://www.bleepingcomputer.com/news/security/ordinypt-ransomware-intentionally-destroys-files-currently-targeting-germany, (Accessed June 2018).

[31] I. Yaqoob, I.A.T. Hashem, A. Ahmed, S.A. Kazmi, C.S. Hong, Internet of things forensics: Recent advances, taxonomy, requirement, and open challenges, Future Gener. Comput. Syst. 92 (2019) 265–275, http://dx.doi.org/10.1016/j.future.2018.09.058.

[32] Monika P. Zavarsky, D. Lindskog, Experimental analysis of ransomware on windows and android platforms: Evolution and characterization, in: 2nd International Workshop on Future Information Security, Privacy & Forensics for Complex Systems, 2016, pp. 465–472, http://dx.doi.org/10.1016/j.procs.2016.08.072.

[33] A.L. Young, Non-zero sum games and survivable malware, in: IEEE Systems, Man and Cybernetics Society Information Assurance Workshop, 2003, pp. 24–29.

[34] C. Cimpanu, Charger android ransomware reaches google play store, 2017, https://www.bleepingcomputer.com/news/security/charger-android-ransomware-reaches-google-play-store, (Accessed June 2018).

[35] Symantec Security Response Team, 2017, ISTR Ransomware 2017, White Papers, 2017, https://www.symantec.com/security-center/white-papers.

[36] J. Wyke, A. Ajjan, The Current State of Ransomware, Tech. Rep. December, Sophos, 2015, URL https://www.sophos.com/en-us/medialibrary/PDFs/technicalpapers/sophos-current-state-of-ransomware.pdf.

[37] B. Franko, Globeimposter ransomware: Blocked by Ensilo, 2018, https://blog.ensilo.com/globeimposter-ransomware, (Accessed June 2018).

[38] Trend Micro, SynAck ransomware leverages process Doppelgänging for evasion and infection, 2018, https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/synack-ransomware-leverages-process-doppelg-nging-for-evasion-and-infection, (Accessed July 2018).

[39] A. Lelli, Microsoft Malware Protection Center, Ransomware operators are hiding malware deeper in installer packages, 2017, https://cloudblogs.microsoft.com/microsoftsecure/2017/03/15/ransomware-operators-are-hiding-malware-deeper-in-installer-packages, (Accessed June 2018).

[40] A.K. Sood, S. Zeadally, A taxonomy of domain-generation algorithms, IEEE Secur. Priv. 14 (4) (2016) 46–53.

[41] S. Hilt, W. Gamazo Sanchez, BkSoD by ransomware: Hddcryptor uses commercial tools to encrypt network shares and lock HDDs, 2016, https://blog.trendmicro.com/trendlabs-security-intelligence/bksod-by-ransomware-hddcryptor-uses-commercial-tools-to-encrypt-network-shares-and-lock-hdds, (Accessed June 2018).

[42] K. Jarvis, SecureWorks Counter Threat Unit™ Threat Intelligence, Cryptolocker ransomware, 2013, https://www.secureworks.com/research/cryptolocker-ransomware, (Accessed June 2018).

[43] A. Continella, A. Guagnelli, G. Zingaro, G. De Pasquale, A. Barenghi, S. Zanero, F. Maggi, ShieldFS: A self-healing ransomware-aware filesystem, in: Proceedings of the 32nd Annual Computer Security Applications Conference, ACSAC, ACM, 2016, pp. 336–347, http://dx.doi.org/10.1145/2991079.2991110.

[44] D. Xu, J. Ming, D. Wu, Cryptographic function detection in obfuscated binaries via bit-precise symbolic loop mapping, in: Proceedings of the 38th IEEE Symposium on Security and Privacy, SP 17, 2017, pp. 921–937.

[45] X. Li, P. Jiang, T. Chen, X. Luo, Q. Wen, A survey on the security of blockchain systems, Future Gener. Comput. Syst. (2017) http://dx.doi.org/10.1016/j.future.2017.08.020.

[46] M. Conti, A. Gangwal, S. Ruj, On the economic significance of ransomware campaigns: A bitcoin transactions perspective, 2018, arXiv:1804.01341v4.

[47] M. Paquet-Clouston, B. Haslhofer, B. Dupont, Ransomware payments in the bitcoin ecosystem, in: 17th Annual Workshop on the Economics of Information Security, WEIS, 2018, arXiv:1804.04080.

[48] D.Y. Huang, M.M. Aliapoulios, V.G. Li, L. Invernizzi, K. McRoberts, E. Bursztein, J. Levin, K. Levchenko, A.C. Snoeren, D. McCoy, Tracking Ransomware End-to-end, in: 39th IEEE Symposium on Security and Privacy, S & P, 2018, pp. 618–631.

[49] R. Falcone, J. Grunzweig, Targeted ransomware attacks middle eastern government organizations for political purposes, 2017, https://researchcenter.paloaltonetworks.com/2017/03/unit42-targeted-ransomware-attacks-middle-eastern-government-organizations-political-purposes, (Accessed June 2018).

[50] A.L. Young, M. Yung, Malicious Cryptography – Exposing Cryptovirology, Wiley Publishing, Inc., 2004.

[51] A. Palisse, H. Le Bouder, J.L. Lanet, C. Le Guernic, A. Legay, Ransomware and the legacy crypto API, in: N. Cuppens, F. Cuppens, J.L. Lanet, A. Legay (Eds.), 11th International Conference on Risks and Security of Internet and Systems, CRiSIS 2016, in: LNCS, vol. 10158, Springer, 2017, pp. 11–28, http://dx.doi.org/10.1007/978-3-319-54876-0-2.

[52] C. Puodzius, How encryption molded crypto-ransomware, 2016, http://www.welivesecurity.com/2016/09/13/how-encryption-molded-crypto-ransomware, (Accessed June 2018).

[53] Y. Xie, F. Yu, K. Achan, R. Panigrahy, G. Hulten, I. Osipkov, Spamming botnets: Signatures and characteristics, in: Proceedings of ACM SIGCOMM, 2008.

[54] A. Arora, M. Gannon, G. Warner, Kelihos Botnet: A never-ending saga, in: Annual ADFSL Conference on Digital Forensics, Security and Law, 2017, pp. 9–26.

[55] Trend Micro, Viro botnet ransomware breaks through, 2018, https://blog.trendmicro.com/trendlabs-security-intelligence/virobot-ransomware-with-botnet-capability-breaks-through, (Accessed September 2018).

[56] S. Pletinckx, C. Trap, C. Doerr, Malware coordination using the blockchain: An analysis of the cerber ransomware, in: 2018 IEEE Conference on Communications and Network Security, CNS, Beijing, 2018, pp. 1–9, http://dx.doi.org/10.1109/CNS.2018.8433199.

[57] M. Antonakakis, R. Perdisci, Y. Nadji, N. Vasiloglou, S. Abu-Nimeh, W. Lee, D. Dagon, From throw-away traffic to bots: Detecting the rise of DGA-based malware, in: Proceedings of the 21st USENIX Conference on Security Symposium, USENIX Association, Berkeley, CA, USA, 2012, pp. 491–506.

[58] A. Higbee, The role of crypto-currency in cybercrime, Comput. Fraud Secur. (7) (2018) 13–15, http://dx.doi.org/10.1016/S1361-3723(18)30064-2.

[59] A. Alzahrani, et al., RanDroid: Structural similarity approach for detecting ransomware applications in android platform, in: 2018 IEEE International Conference on Electro/Information Technology, EIT, Rochester, MI, 2018, pp. 0892–0897, http://dx.doi.org/10.1109/EIT.2018.8500161.

[60] P. Lestringant, F. Guihery, P.A. Fouque, Automated identification of cryptographic primitives in binary code with data flow graph isomorphism, in: Proceedings of the 10th ACM Symposium on Information, Computer and Communications Security, ACM, 2015, pp. 203–214, http://dx.doi.org/10.1145/2714576.2714639.

[61] N. Andronio, S. Zanero, F. Maggi, HelDroid: Dissecting and detecting mobile ransomware, in: Research in Attacks, Intrusions, and Defenses, Springer, 2015, pp. 382–404.

[62] F. Mercaldo, V. Nardone, A. Santone, C.A. Visaggio, Ransomware steals your phone. Formal methods rescue it, in: International Conference on Formal Techniques for Distributed Objects, Components, and Systems, Springer, 2016, pp. 212–221, http://dx.doi.org/10.1007/978-3-319-39570-8_14.

[63] D. Sgandurra, L. Munoz-Gonzalez, R. Mohsen, E.C. Lupu, Automated dynamic analysis of ransomware: Benefits, limitations and use for detection, 2016, arXiv:1609.03020, no. September.

[64] A. Cuzzocrea, F. Martinelli, F. Mercaldo, A novel structural-entropy-based classification technique for supporting android ransomware detection and analysis, in: 2018 IEEE International Conference on Fuzzy Systems, FUZZ-IEEE, Rio de Janeiro, 2018, pp. 1–7, http://dx.doi.org/10.1109/FUZZ-IEEE.2018.8491637.

[65] H. Zhang, X. Xiao, F. Mercaldo, S. Ni, F. Martinelli, A.K. Sangaiah, Classification of ransomware families with machine learning based on N-gram of opcodes, Future Gener. Comput. Syst. 90 (2019) 211–221, http://dx.doi.org/10.1016/j.future.2018.07.052.

[66] S. Homayoun, A. Dehghantanha, M. Ahmadzadeh, S. Hashemi, R. Khayami, Know abnormal find evil: frequent pattern mining for ransomware threat hunting and intelligence, IEEE Trans. Emerg. Top. Comput. (2017) http://dx.doi.org/10.1109/TETC.2017.2756908.

[67] S. Homayoun, A. Dehghantanha, M. Ahmadzadeh, S. Hashemi, R. Khayami, K.R. Choo, D.E. Newton, DRTHIS: Deep ransomware threat hunting and intelligence system at the fog layer, Future Gener. Comput. Syst. 90 (2019) 94–104, http://dx.doi.org/10.1016/j.future.2018.07.045.

[68] M. Rhode, P. Burnap, K. Jones, Early-stage malware prediction using recurrent neural networks, Comput. Secur. 77 (2018) 578–594, http://dx.doi.org/10.1016/j.cose.2018.05.010.

[69] K. Cabaj, M. Gregorczyk, W. Mazurczyk, Software-defined networking-based crypto ransomware detection using HTTP traffic characteristics, Comput. Electr. Eng. 66 (2018) 353–368, http://dx.doi.org/10.1016/j.compeleceng.2017.10.012.

[70] A.O. Almashhadani, M. Kaiiali, S. Sezer, P. O'Kane, A multi-classifier network-based crypto ransomware detection system: A case study of Locky ransomware, IEEE Access 7 (2019) 47053–47067.

[71] N. Scaife, H. Carter, P. Traynor, K.R.B. Butler, CryptoLock (and drop it): Stopping ransomware attacks on user data, in: 2016 IEEE 36th International Conference on Distributed Computing Systems, ICDCS, 2016, pp. 303–312, http://dx.doi.org/10.1109/ICDCS.2016.46.

[72] J.A. Gómez-Hernández, L. Álvarez González, P. García-Teodoro, R-Locker: Thwarting ransomware action through a honeyfile-based approach, Comput. Secur. 73 (2018) 389–398, http://dx.doi.org/10.1016/j.cose.2017.11.019.

[73] M. Spagnuolo, F. Maggi, S. Zanero, Bitiodine: extracting intelligence from the bitcoin network, in: N. Christin, R. Safavi-Naini (Eds.), FC 2014, in: LNCS, vol. 8437, International Financial Cryptography Association, 2014, pp. 457–468, http://dx.doi.org/10.1007/978-3-662-45472-5-29.

[74] J.K. Lee, S.Y. Moon, J.H. Park, CloudRPS: a cloud analysis based enhanced ransomware prevention system, J. Supercomout. 73 (7) (2017) 3065–3084, http://dx.doi.org/10.1007/s11227-016-1825-5.

[75] K.P. Subedi, D.R. Budhathoki, B. Chen, D. Dasgupta, Dasgupta, RDS3: Ransomware defense strategy by using stealthily spare space, in: 2017 IEEE Symposium Series on Computational Intelligence, SSCI, Honolulu, HI, 2017, pp. 1–8, http://dx.doi.org/10.1109/SSCI.2017.8280842.

[76] K. Lee, K. Yim, J.T. Seo, Ransomware prevention technique using key backup, Concurr. Comput.: Pract. Exper. (2017) e4337, http://dx.doi.org/10.1002/cpe.4337.

[77] E. Kolodenker, W. Koch, G. Stringhini, M. Egele, PAYBREAK: Defense against cryptographic ransomware, in: Processing of the ACM on Asia Conference on Computer and Communications Security, Abu Dhabi, United Arab Emirates, 2017, pp. 599–911, http://dx.doi.org/10.1145/3052973.3053035.

[78] J. Huang, J. Xu, X. Xing, P. Liu, M.K. Qureshi, FlashGuard: Leveraging intrinsic flash properties to defend against encryption ransomware, in: Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security, CCS'17, Dallas, TX, USA, 2017, pp. 2231–2244, http://dx.doi.org/10.1145/3133956.3134035.

[79] D. Ranganayakulu, C. Chellappan, Detecting Malicious URLs in E-Mail – An Implementation, in: AASRI Procedia, Vol. 4, 2013, pp. 125–131.

[80] R. Shams, R.E. Mercer, Classifying spam emails using text and readability features, in: 2013 IEEE 13th International Conference on Data Mining, 2013, pp. 657–666, http://dx.doi.org/10.1109/ICDM.2013.131.

[81] A. Singh, S. Batra, Ensemble based spam detection in social IoT using probabilistic data structures, Future Gener. Comput. Syst. 81 (2018) 359–371, http://dx.doi.org/10.1016/j.future.2017.09.072.

[82] D. Goel, A.K. Jain, Mobile phishing attacks and defence mechanisms: State of art and open research challenges, Comput. Secur. 73 (2018) 519–544, http://dx.doi.org/10.1016/j.cose.2017.12.006.

[83] A. Cohen, N. Nissim, Y. Elovici, Novel set of general descriptive features for enhanced detection of malicious emails using machine learning methods, Expert Syst. Appl. 110 (2018) 143–169, http://dx.doi.org/10.1016/j.eswa.2018.05.031.

[84] E.M. Rudd, R. Harang, J. Saxe, MEADE: Towards a malicious email attachment detection engine, in: IEEE Symposium on Technologies for Homeland Security, HST, 2018, arXiv:1804.08162.

[85] I. Jeun, Y. Lee, D. Won, Collecting and filtering out phishing suspicious URLs using spam trap system, in: J.J. Park, et al. (Eds.), Grid and Pervasive Computing, GPC 2013, in: Lecture Notes in Computer Science, vol. 7861, Springer, Berlin, Heidelberg, 2013, pp. 796–802, http://dx.doi.org/10.1007/978-3-642-38027-3_89.

[86] A. Kharraz, S. Arshad, C. Mulliner, W. Robertson, E. Kidra, UNVEIL: A large-scale automated approach to detecting ransomware, in: 25th USENIX Security Symposium, USENIX Security 16, Austin, TX, USENIX Association, 2016, pp. 757–772.

[87] D.Y. Kim, G.Y. Choi, J.H. Lee, White list-based ransomware real-time detection and prevention for user device protection, in: 2018 IEEE International Conference on Consumer Electronics, ICCE.