Survey On Ransomware Evolution, Prevention, And Mitigation

Mousab Hamad, Derar Eleyan.

Abstract: Ransomware transformed into a form of criminal business. malware that takes over a victim's machine or data unusable. it is booming so fast all the world, it is a dangerous threat to users' and corporates' data file. Ransomware encrypts files on an infected computer and holds the key to decrypt the files until the victim pays a ransom (this is why it is called ransomware). Ransomware is causing losses financially from hundreds of millions of dollars annually. Every year passes we observe a new version of this destructive malware. And the new versions have new technologies to bypass the defenders. In this paper, we present a brief history of ransomware, the best methods to prevent the infection, how to detect it, and how to recover from this infection. This monster has estimated financial damage of $1 billion. The fact that many Internet users appear to have no awareness of ransomware and do how to awake and protect themselves, they think that with a highly automated tool like it they won't be targeted because they are normal users in Cyberspace.

Index Terms: Ransomware, Malware, Automated Virus, Cyberspace

I. INTRODUCTION

Ransomware, in other words, called crypto infection, has gotten critical consideration among internet scientists over the most recent couple of years. offenders utilize this malware to take individuals' private data. The payment or request can be digital money or requests to buy from assigned stores [1]. Ransomware is built and developed to disrupt access to the data or even access to the machine itself. The attackers then exploit the victim for the recovery of the equipment or data. Ransomware displays a screen containing a message about the terms of the ransom (ransom note), and in our days. Some ransomware would go to the extent of displaying on this screen some Child pornography and highlight the threatening to the victim's life. These scary techniques are the facilitation that criminals use to make paying felt easier. [2] As known as Internet play like a double-edged sword and here the Internet and new technologies like cloud computing and digital currency such as Bitcoin and Ethereum provide the best ground for offenders especially those who are developing ransomware. The amount of money the perpetrator receives as ransom is between $300 and $700 for people and between $10,000 and $17,000 for companies [4]. According to the FBI's Cyber Crime Complaint Center, between April 2014 and June 2015, ransomware attacks caused an estimated $ 18 million in damage [5]. In many situations, the only way to retrieve the files which are is to pay the ransom even though it is not recommended. In general, [6] mentioned two types of ransomware: Locky and Crypto, Crypto ransomware uses encryption technologies to lock chosen files from user access; this is much more difficult to overcome and the harm can be permanent. Crypto ransomware is also the most common form used by cybercriminals. On the other hand, Locky ransomware locks the whole device from the user's entry point, but it is normally easy to resolve. The third form of ransomware called scareware. The third type was not considered as a type of ransomware but some researchers did count it as one.

- *Mousab Hamad, Applied Computing Department, Faculty of Applied Science, Palestine Technical University Kadoorie, Tulkarem, Palestine.*
- *Derar Eleyan, Associate Professor in Information Systems, Applied Computing Department, Faculty of Applied*
- *Science, Palestine Technical University Kadoorie, Tulkarem, Palestine*

The scareware attempts to persuade the victim to buy antivirus which if it is not a fake one. It should remove the virus. All of these are included in the display message. The antivirus is non-functional malware too [7,8]. Some security mechanisms can detect ransomware based on its Activities such as File System Activities, Registry Activities, Control Management Unit, Network Operation, and Lock mechanism [9,10]. Options of heal from ransomware might not always be present because some encryption is too much Hard to crack without a decryption key even though Defense companies are consistent Develop and release an anti-ransomware program and Tools for decryption in response to the threat [10,12]. Detecting the malware early in the event of an attack is one of the important things to make the damages less than the target of the offender for both Businesses and individuals [9,10]. If anyone determined to pay the ransom. That does not inflect him from contacting the FBI. In all situations, the FBI supports all victims to report their incidents especially if it is ransomware. In 2019, the IC3 received 2,047 complaints identified as ransomware with adjusted losses of over $8.9 million [37]. In this paper, the evolution of ransomware attacks stated to enterprises and individuals is stated. and recommend Prevention strategies and describing the best practices. We elaborate on the financial impact of the different categories of ransomware information systems and recommend mitigation strategies. The remainder of the paper is structured as follows: Section II introduces the literature review. Section III consists of detection and prevention techniques of the ransomware. Section IV discusses the ransomware lifecycle. Section V discusses the mitigation strategies and best recovering methods. The Related works are discussed in Section VI. and the conclusion is described in Section VII.

II. LITERATURE REVIEW

1. Ransomware Evolution

Ransomware isn't a new idea, the first ransomware that showed up in 1989 was named the PC CYBORG (Helps) Trojan. Joseph Popp evolved the first ransomware program in 1989, with the name of the bad diseases in that time. 'AIDS' (PC Cyborg) which was treated and considered as a Trojan. Floppy discs were used to spread this Trojan. Once the floppy disc is inserted into the machine, the AIDS program encrypted

the files on the C: drive and then asked for $189 to pay to a PO Box in Panama. AIDS ransomware has a lot of weaknesses:

1) The reachable victims' number is low.
2) The infection method is not reliable (floppy disc used).
3) The encryption method was weak and easily reversed.
4) The payment method was easy to detect. [3]

As mentioned in [3] There has been an explosion in ransomware in recent years, which has now spread around the globe, blindly infecting victims, where it quickly encrypts data, making companies and individuals locked out of their machines. The Growing ransomware has seen a 600 percent rise in the number of ransomware families such as Cerber, Locky, and CryptoWall, and many more.

Figure 1 shows the timeline of ransomware attacks (2005-2020). For the next of this section an overview of the most important attacks with new technologies.

In 2005, criminals launched a ransomware attack (Gpcoder) that used symmetric encryption. Then after one year, according to [13-15] criminals developed a stronger encryption method called asymmetric encryption. Asymmetric encryption utilizes two numerically related encryption keys (public and private keys). The public key is utilized to scramble information, and information can't be utilized to encode, so the public key can be traded or shared with no information on the private key [15]. The private key is utilized for information encryption just and will be covered up until the payoff is paid [16]. RSA encryption(Rivest–Shamir–Adleman) was used for the first time in the ransomware industry in 2006. Archievus uses RSA Asymmetric encryption with the RSA algorithm. It encrypted the directory of 'My Document' and to get access to it the victim needed to buy an item from specific Web sites. In 2010, WinLock showed up as Locky ransomware, which bolted and forestalled admittance to the tainted gadget (known as a Storage). WinLock shows pornographic pictures until casualties send a $10 premium-rate SMS to get an open code. it was spread by another ransomware worm that imitated the Windows Item notice and gave casualties a global number to call to include a six-digit code. The call would be rerouted through a nation with high worldwide telephone rates, and the individual would be kept waiting while the charges racked up. In 2010 ten individuals answerable for Winlock were captured in Moscow, the pack had been inactivity for about a year and supposedly procured over $16 million from this SMS plot. After 2 years Reveton Appeared, in other words as stated in [16] it is also having the name of Trojan: W32/Reveton. It takes control of the victim machine [16,18]. It uses the RSA-2048 algorithm so it uses Asymmetric Encryption, it makes new instances in services to get the communication with the C&C server of the offender [16,18,19]. And it for sure encrypts the victim's files and displays a message to pay the ransom on the of the machine. The display message for the payment includes police enforcement warning with webcam footage and this creates some illusion that the victim did something wrong, so the victim will get scared. CryptoLocker happened from 5 September 2013 to 2014. This attack utilized a Trojan that focused on computers running Microsoft Windows. It proliferated through infected mail attachments and an existing Gameover ZeuS botnet. When enacted, it encrypts particular types of files stored on local and mounted network drives using RSA Asymmetric cryptography, with the private key put away as it were on the malware's control servers. CryptoLocker utilized Advanced Encryption Standard (AES)-256 file encryption and used 2048 bit RSA for their C&C on the TOR systems. This malware shows a message which offered to decrypt the data if payment happens by an expressed due date. The payment can be either with bitcoin or a pre-paid cash voucher [20]. In the middle of 2013, the first Locky Ransomware to android has just appeared as fake antivirus, it started by scanning users' documents and display files that are infected with malware by performing a fake scan.it also depends on adware added to it. This adware does not stop showing until the user chooses the option to lock his phone. The victim can not do a factory reset because this ransomware modifies the OS setting [19]. In 2014 SimpLocker the first Crypto-Ransomware to Android has just arrived, it goes under the legitimate apps which are used extremely by teenagers as they do not have enough awareness about how to distinguish between the legitimate and illegitimate apps. It scans those file extension JPEG, PDF, DOCS, AVI, and MP4 to encrypt them using AES. It uses Extensible Messaging and Presence Protocol(XMPP) to send information about the victim's device to the C&C server [19]. Imagine using TOR for doing any money transaction. That happened in 2014 with CryptoDefnese which include TOR-based Bitcoin for ransom payment to make the trace process so hard. Even though CryptoDefnese uses TOR but it has a weakness due to using of Windows' built-in encryption. The private key could be obtained from Windows API.

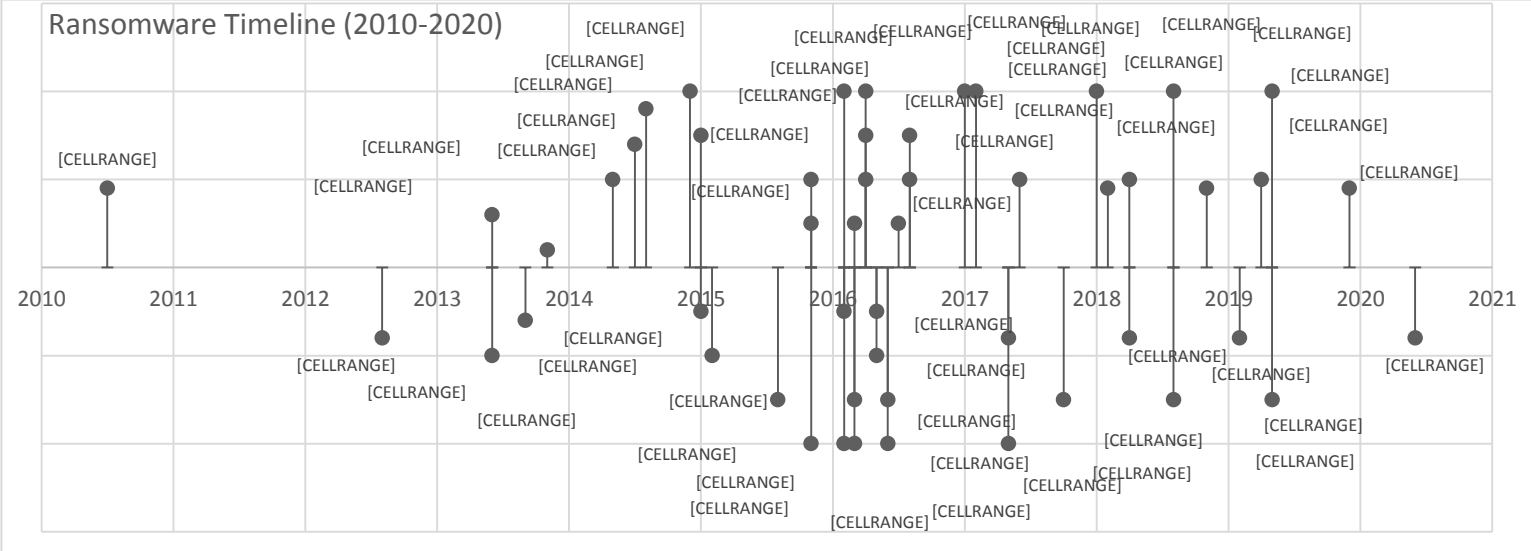

Figure 1. *Ransomware Timeline*

In March 2016 Samas attacks were considered with the endorsement of the previous technology like TOR C&C, payment via Bitcoin, and the AES file encryption. Sama's developers were interested in attacking organizations, they did not care about individual targets or broad campaigns. Samas included a real-time communication channel so the offenders may contact their casualties [12,21]. Petya (prevalent in 2016) could be a takeoff from the standard encryption configuration. It was chosen to offend the system's low-level memory configuration by maliciously overriding the essential boot record and after that encrypting the master record table [12]. It encrypts the essential record table (MFT) after restarting the tainted system, so o master boot registration (MBR) is not possible [22]. As a result, by locking the MBR, the infected system will eventually become useless, so you will not be able to access your files or even the operating system on the drive, as it is necessary to identify the MBR as a port on a hard disk and the location of the files. In March 2016 the first ransomware-as-a-service (RaaS) was revealed by the name of Cerber. In RaaS there is a license belong to the attacker over the internet with the help of a developer, and this developer shared the ransom with the attacker. As mentioned in [24] for about 40% cut the developer can sign-up as Cerber copartner and he will have any Cerber ransomware he wants. An attacker usually does not share his ransom with anyone. so the majority of ransomware doesn't use this service. The advantage of this service as in any partnership the needed work for the attacks is less than the normal ones. Cerber uses AES encryption similar to other ransomware attacks [3]. Jigsaw was born in April 2016. it spreads with traditional ways like email attachments and spam ones. It affects registry entry this gives it the ability to be the first ransomware that deletes files during the attack to encourage payment and would delete a thousand files each time it is restarted. On the other hand previous ransomware attacks made false threats to delete files. It used AES encryption similar to other ransomware [3,23]. in May of 2017 the most widespread ransomware happened, WannaCry haunted in all continents and with over 150 countries infected with it.it has no discriminate nature of the attack. It attacked everything including universities, the transport sector, the health sector, etc. [25].

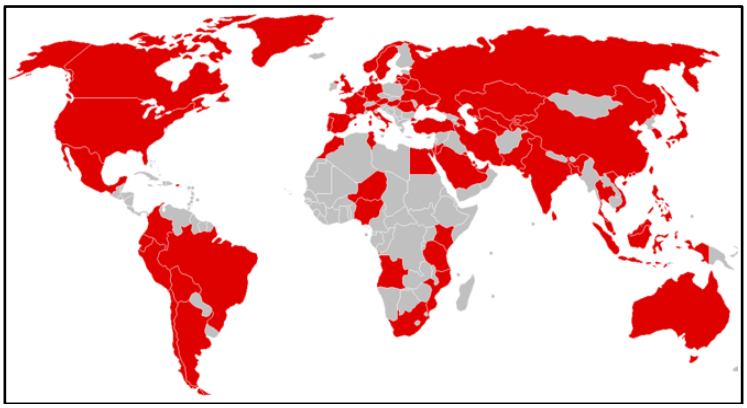

Figure 2*. Distribution of initial WannaCry attacks [25]*

Figure 2 below shows the distribution of reported WannaCry attacks the world over. What made it effective is the best distribution mechanisms used which are called infection mechanisms and beside it the robust encryption methods employed. A resilient encryption [26].

The Samsam ransomware appeared in the early months of 2017. It attacks Erie County Medical Center (ECMC) And the victims of this assault were six-thousand personal computers [28,29]. unlike the common spam email infection vector. It depends upon the physical devices in the network like the router or the firewall, it takes advantage of the lapses in it [30,31]. As studies say according to [29,31] Samsam targets and exploit in specific the default passwords for the web-server and the remote desktop protocols vulnerabilities. with zero actual shots, it severely damaged the service and major city in the United States and this was the run-down of the "Silent Battle" [27,31]. As mentioned in [27,31] Atlanta was not the only place of this cyber-war. This ransomware almost cost 900K dollars as stated in [31,32]. REvil ransomware was reported in 2019. It does encrypt the infected machine's data but not just that it also deletes all shadow copy backups so the recovery would be so hard to be accomplished [32,33]. It began the attacks in Oracle Weblogic system, it also attacked the clients of VPN big companies like Pulse and Fortinet [32,34]. Sodinkibi the other name of REvil the payments of its' ransom recorded till now as stated in shaming website and it is about 6 million USD. The most recent ransomware was

reported in the middle of 2020. As the previous ransomware, the reports indicate it is propagated through email attachments according to [36]. It targets vast sorts of file extensions. Once it encrypts the victims' machine it adds its' file extensions "hALioS". This new mentality that cyber-c
riminals are considering as the new threat to most companies, individuals, and even the government. Developing this ransomware more and more by using the previous version and adding the new technology to it to make it robust. On the other hand, there have been huge decryption softwares made by the anti-virus like MacAfee, Kaspersky employed to reduce the danger and the damage done by ransomware. Thanks to poor coding implementation, weak randomization and various other mistakes by the but still with extended families of the ransomware, there are more than 60 ones [32]. Ransomware is now a robust encryption program with a hidden C&C.

2. FINANCIAL IMPACT OF RANSOMWARE

Previously, individual users used to be the most likely victims of ransomware attacks. But in 2016, a dramatic shift to enterprises occurred, where 42% of all ransomware infections are reported and blocked by Symantec targeted enterprises [3]. This due to different reasons, one of the main reasons is the propagation of the malware among many computers that are contacted to the enterprise network and asking for a ransom for a single infection [31]. Recently, the number of attacks targeting individual users decreased a lot. In the other hand, from 2016 to 2020 an unexpected number of ransomware infection targeting enterprises and companies which were reported by Symantec [3]. This is because of different reasons, the widespread malware within companies [31]. The ransom pay can be maximized depending on different things, like the values of the attached files, how much trust there is between the criminals in respecting their word, and the ability of those victims to pay. The next figure represents the losses caused by the ransomware that were reported to the FBI during the period 2012-2019. Besides that, the FBI ICR report mentioned that those numbers are just reported to the FBI agent. Those losses are the direct losses without the losses due to stopping businesses, wages, files, types of equipment.

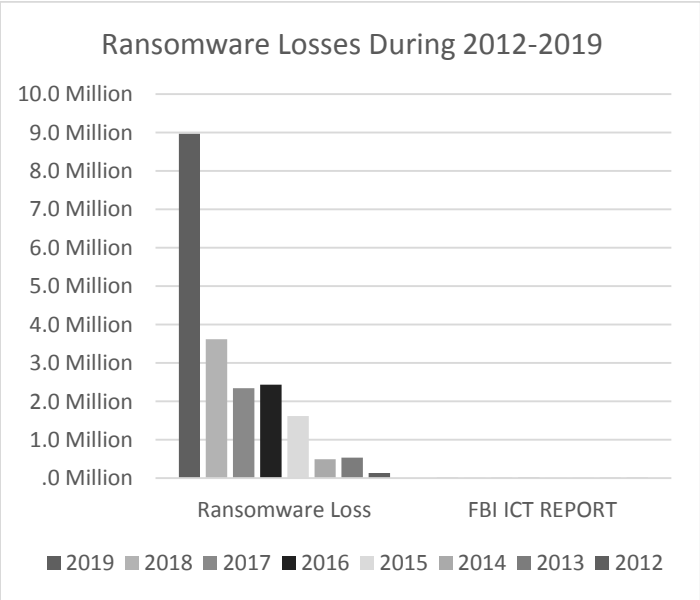

Figure 3. *Ransomware Losses According to [37]*

At the end of 2013, Cryptolocker ransom payments of four Bitcoin addresses were studied and investigated by ZDnet which is a business technology news company. The findings of this company led to getting more than 40 thousand transactions to those addresses through the period from 15 October to 18 December, those 40k bitcoins equalized in that time 27 million [3,44] the FBI's Internet Crime Complaint Centre recorded significant increases in ransomware infections. According to [45] FBI said that "It estimated the market value of ransomware to be $200 m annually". CryptoWall had 1000 reported attacks [3]. CryptoWall total losses are estimated to $18 m. Fluctuation in the Bitcoin exchange rate caused the variety in the change of ransom paid [3]. CryptoWall variation of the ransom was depending on the victim and the country he lives in [3,45]. "Popcorn ransomware allowed victims to decrypt their files for free if they infected two other people with the ransomware" [48]. Ransomware has a high gainful rate. It has a kind of flexibility when it comes to victim nature. At the beginning of the ransomware, all the payments were unintelligent with fixed pricing to all people. But that does not persuade victims. The new families of ransomware offered the new smart demands. It applies pricing based on the victims' ability to pay [3].

2. INFECTION FACTORS AND FACILITATORS

2.1 Facilitators

Ransomware got many enablers due to lifestyle changes and technology improvements this leads to an extend widespread with ransomware attacks both in the number of attacks and types of them [38]. The most common enablers are:

2.1.1Encryption

Encryption was invented in the past to achieve one of the most concepts of information security which is confidentiality [38,40]. These days there is a huge use of internet in general, computer and other technologies in specific, Nevertheless, there is a high opportunity of catching the data in its' way between the sender and the receiver. The concept of confidentiality implied by encryption is to ensure that the data is only can be read by authorized people [38]. This technology has proven to be a double-edged sword.-As stated in [38] the "Symmetrical encryption uses one key for both encryption and decryption process". Its advantage is the encryption process can be quickly completed. However, its downside is that it is less secure. According to [38] the Asymmetrical encryption can be defined as "Asymmetrical encryption uses one key for encryption, called the public key, and another key for decryption called private key". The encryption process is slower but more secure. Hybrid encryption combines both symmetrical encryption and asymmetrical encryption [38].

2.1.2Cyber Currency

Cyber Currency did guarantee privacy for the remitter in any transaction. the recipient's address remains unknown even for the authority [38,40]. So in terms of ransomware, this currency solves a big problem for the offenders. When the victim decides to file a complaint to track the account of the perpetrator it would be so hard to get it. In addition to that, all this occurred in a legitimate action and there is a lot of online stores that deal with it these days [38,40]. Cyber Currency is built on Blockchain theory. Which is based on asymmetric encryption just like the RSA algorithm and one-way has

function, which makes it so strong to break it through mathematical operations [38,40].

2.1.3Ransomware Accessibility
RaaS exists this makes it easy to obtain the Ransomware codes. Besides, there are some free development kits, such as TOX, Hidden Tear, and Torlocker, which reduces obstacles or even delete them for joining the ransomware industry [38,39].

2.2 Infection Factors:
These days, the Internet has a penetration rate of 63.2% (4.9 billion users) worldwide [3,58]. Which is considered a fertile environment for cyber-criminals [3]. The most common method used to widespread the ransomware is phishing and spam emails. There are many factors of proliferation and the most important ones are [18,14]:

2.2.1 Phishing or SPAM e-mails: Spam emails can be defined as emails that contain an attachment with very know words for the filename 'invoice', 'internal' [18,60] in malware. Files are masked as .pdf with a fake icon, to convince the users that it is a normal file, whenever the malware is downloaded it pull out the ransomware. This is so close to IRC, P2P.

2.2.2 Exploit kits: In this method, the advertising network has hustler advertisements (Ads) grouted to it, those are put when there is a large audience [18]. The hustler AD redirects users to the attacker's website, which usually exploits using an exploit kit like Magnitude, Angler, Neutrino, and Nuclear [59] the vulnerability in the browser, using an exploit kit [18] to enable the drive-by-download of ransomware.

2.2.3 Downloader and Trojan Botnets: This is happened by letting users download legitimate with a hidden functionality malware without any notice from the victim. This is can be adventing through software-hosting websites [18].

III. RANSOMWARE ATTACK SCENARIO

The scenario of successful ransomware can be divide as shown in figure 4 below into five processes:

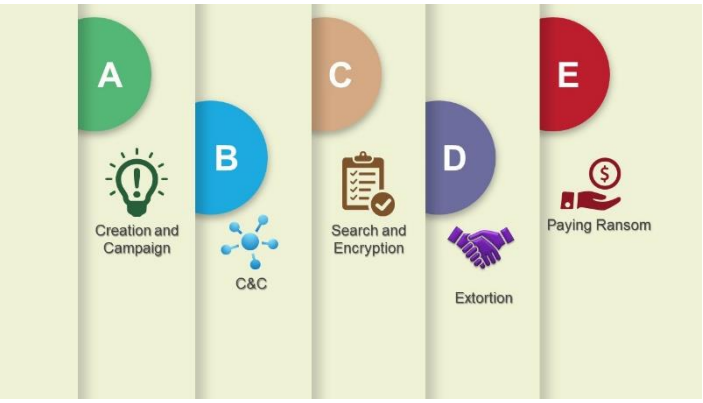

Figure 4. *Successful Ransomware Attack Process [6]*

A. Creation and Campaign:
Programming codes to build the malware that will work as the ransomware is the meaning of creation. Creators or developers need to be so much familiar with all kinds of new technology in anything that will make files hard to recover or even more secure with the ransom payments [6]. The campaign can be defined by what is the ways that will make the victim download the ransomware. In other words, the infection factors that Are needed to put this inside the targeted machine. For enterprise targets, they put security defenders in front of their physical and virtual entrances. Social engineering or the infection method to use has to be highly sophisticated and studied [6].

B. C&C:
Once ransomware reaches the victims' machine, it starts the command and control with the offender servers. It starts generating the encryption and if it is a Locky ransomware it starts reaching the admin settings for that purpose [6].

C. Search and Encryption:
After the encryption key is generated with C&C, the ransomware begins to search for important files depending on their extensions [6]. When all the important and valuable file extensions have been distinguished, the ransomware starts encrypting the files and it can do this process through different topologies: symmetrical encryption, asymmetrical encryption, and hybrid encryption [6].

D. Extortion:
The semi-final step of this process is displaying the ransom note. This note contains the mode of payment, the type of infection, and finally the deadline, after it the ransomware will being deleting the encrypted files [6].

E. Paying Ransom.

IV. DETECTION AND PREVENTION TECHNIQUES V.

1. Ransomware Detection Methods:

1.1 Machine Learning
Machine Learning is just a way of using mathematical operations to predict outcomes or decide to do something as a reaction to some incident [38,41]. The most important thing in this science is finding the cleaned training data with the best suitable algorithm to make outcomes as good as possible.ML has two sides like everything in the world, the good side when using the best algorithm, the output will be predicted precisely, this science can't become dumb. However, in process of finding the algorithm, there is a possibility to enter a spiral of trial and error. In addition to that to be cautious is necessary to not let overfitting happened [38,41].

1.2 Honeypot
Honeypot involves luring the offender with trap files. When the trap files are infected, the ransomware can be specified [38]. The advantage of this technique it does not need processing power or upholding the system, the weakness of it, the ransomware is supposed to attack the trap files but there is not warrant that it is going to do that so to know the behavior of ransomware is necessary here [38].

1.3 Statistic
The statistic is used to analyze the characteristics of anything [38]. Employing this detection mechanism is a tedious

undertaking. In practice, this technique involves the evaluation of ransomware by examining code one without executing it [38,42]. On the opposite side the dynamic analysis includes the testing operation but in a controlled environment to prevent outside infection (e.g., sandbox, virtual machine, emulator, etc.) [42].

1.4 Monitoring Techniques for Detection

1.4.1 Monitoring for known file extensions:

According to [43] it is a useful method for detecting suspicious activity, by monitoring file activity so that both real-time and historical records are uploaded to network file shares. This still can be effective although the file extensions are a lot these days.

1.4.2 Monitoring for an increase in file renames:

this technique is not that common, when ransomware strike it will change huge file names while data is being encrypted at that moment [43].

1.4.3 Client-based anti-ransomware agents:

anti-ransomware agents monitor the windows registry for text strings known to be connected and related to ransomware [43]. They run in the background and deny endeavors of ransomware to encrypt data [43].

2. Prevention of Ransomware:

In this section, there are some good ways on how to interdict the ransomware attack and to reduce the risk of infected machines []. Most of them are basics things of the security for any malware, not just the ransomware.

1. Backup the important files regularly and in a consistent way and always have a presence of backup off-site.it is so necessary to encrypt the backed up data to restore it by authorized people.
2. Don't stay logged in as an administrator any longer than needed [49].
3. Be Cautious while you are opening unsolicited attachments.
4. For Ransomware attacks to be deployed, cybercriminals compromise their accounts and submit fake links to as many people as possible [50].
5. Email filtering is a must thing to do to deter the infection. Symantec provides services with a security cloud [51,54] which helps in blocking malicious emails before targeting.
6. Ensure the firewall is configured correctly and properly in the system [51,53].

VI. MITIGATION STRATEGIES AND RECOVERY

A. Mitigation Strategies:

When new ransomware came up with new technology or family and target any victim for the first time. The certain thing in this situation is that most decryptors or services will not recover the encrypted files. But mitigation strategies are capable of doing something. even though the system gets infected the backup can bring the files within hours if it is not damaged too [14]. The ransomware creators are aware of backup performance so they did improve a new type that runs vssadmin.exe and delete the shadow volume copies of the host. Due to that, it is necessary to secure backups through layers of security [14]. The source verification needs to be done for any edit of the backup file servers. The importance of this strategy came out from non-sensible continuous backup of entire data. In simple words, the data that can be replaced smoothly is affordable if it is encrypted. But the data that is related to results if is encrypted the whole operation needs to be restarted [13,57]. If anything wrong happens to those files they will affect so many users within the system. The categorizing can be done physically or logically under different policies [13].

B. Data Recovery

The last five years have witnessed a significant and clear development of ransomware attacks that are based on extortion, and these attacks continue to the present time, especially during the Coronavirus pandemic [3,55]." Do not pay the ransom", that the first advice to take but when all other ways to recover data fail, because dealing with criminals is hard to recover data. There is a need for social engineering techniques to deal with offenders for recovering all important needed data [3]. There are some decrypting tools and services. The robust encryption algorithm is considered when the cyber-criminal built his ransomware. If the victim does not have a backup system for the first data can not be retrieved. Some investigations have found the keys that are used to decrypt and reverse the ransomware. MacAfee and Kaspersky developed incorporation with other security vendors and law enforcement a tool called 'Shade Ransomware Decryption' which had great success in facing Shade ransomware. Some companies offer data decryption but these services depend on public available keys. AVG also provides free decrypt tools for limited types of ransomware [3,56].

VII. RELATED WORKS

This research contains the study of a lot of papers that are connecting about a ransomware attack, evolution, and anything related to it. The following table contains an overview of the publications, the publishers, positive and negative aspect

Ref	Year	Title	Overview	Limitations /Future Direction
[1]	2014	Awareness Education as the Key to Ransomware Prevention	This research paper talks about ransomware attacks and the methodologies of this attack. It gave the awareness as the best ransomware prevention techniques	Most of the information is out of date. It does not have a lot of documented reliable scientific information.
[2]	2015	Cutting the Gordian Knot: A Look Under the Hood of Ransomware Attacks	This experimental paper started with a complete overview of ransomware evolution then it went deep into the ransomware attack practically.	It does not have any obvious limitations.

[3]	2017	Evolution of ransomware	This review article describes the outline of how the ransomware started in the past till 2017. It mentioned most ransomware families.	It could include the financial impact of the ransomware during evolution. There are no comparisons or reviews of past research.
[6]	2019	Ransomware, Threat and Detection Techniques	This review paper gives a clear understanding of threats and detection practices against ransomware, it also describes a brief history of the ransomware, it contains a survey table of a lot of used paper.	It could have contained little deep details about the ransomware. It could have a good citation style to follow.
[8]	2019	A Review of Ransomware Families and Detection Method	This review paper talks about ransomware families. It also has a timeline for the ransomware attack from the first one to 2016. It has a comparing table between detection methods used for the ransomware	The attack in the period between [2016-2019] could be included. It could have less stressed paragraphs in the literature review.
[9]	2016	Experimental Analysis of Ransomware on Windows and Android Platforms: Evolution and Characterization	This paper illustrates the life span of the android platform. It identifies the ransomware by watching out for the non-regular system registry activity.	It could have the prevent advice for the users in keeping backup offline and online ones for crucial files.
[10]	2016	CryptoLock (and Drop It): Stopping Ransomware Attacks on User Data	There is a lot of ransomware attack used for CryptoDrop detection just like Teslacrypt, CTB-Locker, GP code. Ransomware can be removed by botting and formatting the disk.	CryptoDrop makes the ransomware stopped with a median loss of 10 files.
[12]	2019	Ransomware attacks: detection, prevention, and cure	This research paper talks about phases of ransomware, and how it is prevented, and the cleanup of it	It could talk about the other losses of the organizations. Not just direct ransom.
[13]	2017	The rise of ransomware and emerging security challenges in the Internet of Things	Ransomware and its' relation to the IoT technology. A simple representation of Ransomware evolution. A complete overview of two topics	It could be more refreshment if it is divided into two research, one for the ransomware and the other about the IoT.
[18]	2016	Automated Dynamic Analysis of Ransomware: Benefits, Limitations, and use for Detection	It presents a technique for large-scale malware analysis with feature extraction based on a hashed matrix.	- It could talk about the hashing and how this technology fast and space-efficient way of vectorising features. - It could talk about the Bayesian selection and how this method can give insurance about the low false-negative and low false positive of the signature.
[19]	2019	Ransom Analysis: The Evolution and Investigation of Android Ransomware	It presents the method they are using to investigate the ransomware that hit the android operating system It includes the timeline of the ransomware attacks over android.	It could contain more technical parts of the experiment.
[25]	2017	Demystifying Ransomware Attacks: Reverse Engineering and Dynamic Malware Analysis of WannaCry for Network and Information Security	This paper went deep on how to analyze the encrypted files of WannaCry and if it is possible to reverse and recover those files.	NaN
[26]	2019	WannaCry Ransomware: Analysis of Infection, Persistence, Recovery Prevention, and Propagation Mechanisms	This paper specified exactly the WannaCry infection attack in all different stages and how could it be prevented.	It has no limitation.

[27]	2019	SamSam and the Silent Battle of Atlanta	NaN	NaN
[40]	2019	Ransomware payments in the Bitcoin ecosystem	This paper specified exactly the Bitcoin currency and its relation with the ransomware families. It has a full analysis of the whole process through different operations.	It has no limitation. Just being up to date with new incidents and attacks.

VIII. CONCLUSION

Ransomware is becoming serious and dangerous year after year. A critical analysis of more than 30 ransomware families, we came up to the conclusion that ransomware is costing nations millions of dollars every year. It is using a high level of encryption algorithms. It has a spread with so many methods of different kinds in all kinds of levels. It is now becoming the main source of income for Cybercriminals. The first death incident caused by ransomware and led to the disruption of hospital files in Germany was in 2020. The targets of the ransomware are any entity or person who has access to the Internet. From large enterprises to a kid who just plays Minecraft and wants to get free skins then he gets scammed by some website or email. To summarize there are two prime strategies to prevent this monster, the first one is to have the best awareness of scams and phishing operations. The other is the offline backups of the important files within the system.

Acknowledgment

The authors acknowledge the financial support from Palestine Technical University Kadoorie for publishing this paper.

REFERENCES

[1] Luo and Q. Liao, "Awareness Education as the Key to Ransomware Prevention", Information Systems Security, vol. 16, no. 4, pp. 195-202, 2007. Available: 10.1080/10658980701576412 [Accessed 10 December 2020].Kharraz, W. Robertson, D. Balzarotti, L. Bilge and E. Kirda, "Cutting the Gordian Knot: A Look Under the Hood of Ransomware Attacks", Cutting the Gordian Knot: Detection of Intrusions and Malware, and Vulnerability Assessment, pp. 3-24, 2015. Available: 10.1007/978-3-319-20550-2_1 [Accessed 1 November 2020].

[2] P. O'Kane, S. Sezer and D. Carlin, "Evolution of ransomware", IET Networks, vol. 7, no. 5, pp. 321-327, 2018. Available: 10.1049/iet-net.2017.0207 [Accessed 10 November 2020].Gostev, R. Unuchek, M. Garnaeva, D. Makrushin and A. Ivanov, "IT THREAT EVOLUTION IN Q1 2016", Kaspersky Lab, 2016.

[3] "U.S. Dep't of Justice, I-062315-PSA, Criminals Continue to Defraud and Extort Funds from Victims Using Cryptowall Ransomware Schemes (June 23, 2015), available at https://www.ic3.gov/media/2015/150623.aspx [Accessed 23 November 2020].

[4] S. Kok, A. Abdullah, N. Jhanjhi and M. Supramaniam††, "Ransomware, Threat and Detection Techniques: A Review", IJCSNS International Journal of Computer Science and Network Security, vol. 19, no. 2, pp. 136-146, 2019. [Accessed 25 November 2020].

[5] P. Haas, "Ransomware goes mobile: An analysis of the threats posed by emerging methods", ProQuest LLC, New Jersey, 2015.

[6] H. Chittooparambil, B. Shanmugam, S. Azam, K. Kannoorpatti, M. Jonkman and G. Samy, "A Review of Ransomware Families and Detection Methods", Advances in Intelligent Systems and Computing, pp. 588-597, 2018. Available: 10.1007/978-3-319-99007-1_55 [Accessed 27 November 2020].

[7] Monika, P. Zavarsky and D. Lindskog, "Experimental Analysis of Ransomware on Windows and Android Platforms: Evolution and Characterization", Procedia Computer Science, vol. 94, pp. 465-472, 2016. Available: 10.1016/j.procs.2016.08.072 [Accessed 15 November 2020].

[8] N. Scaife, H. Carter, P. Traynor and K. Butler, "CryptoLock (and Drop It): Stopping Ransomware Attacks on User Data", 2016 IEEE 36th

[9] International Conference on Distributed Computing Systems (ICDCS), 2016. Available: 10.1109/icdcs.2016.46 [Accessed 10 November 2020].

[10] J. Scott and D. Spaniel, "The ICIT Ransomware Report", 2016.

[11] R. Brewer, "Ransomware attacks: detection, prevention and cure", Network Security, vol. 2016, no. 9, pp. 5-9, 2016. Available: 10.1016/s1353-4858(16)30086-1 [Accessed 31 November 2020].Yaqoob et al., "The rise of ransomware and emerging security challenges in the Internet of Things", Computer Networks, vol. 129, pp. 444-458, 2017. Available: 10.1016/j.comnet.2017.09.003 [Accessed 2 December 2020].

[12] S. Maniath, P. Poornachandran and V. Sujadevi, "Survey on Prevention, Mitigation and Containment of Ransomware Attacks", Communications in Computer and Information Science, pp. 39-52, 2019. Available: 10.1007/978-981-13-5826-5_3 [Accessed 10 December 2020].

[13] R. Richardson and K. North, "Ransomware: Evolution, Mitigation and Prevention", International Management Review, vol. 13, no. 1, pp. 10-20, 2017. [Accessed 25 November 2020].Bacani, 2014. [Online]. Available: https://blog.trendmicro.com/trendlabs-security-intelligence/reveton-ransomware-spreads-with-old-tactics-new-infection-method/. [Accessed: 10- Nov- 2020].

[14] L. Constantin, "Widespread exploit kit, ransomware program, and password stealer mixed into dangerous malware cocktail", PCWorld, 2015. [Online]. Available: https://www.pcworld.com/article/3012112/widespread-exploit-kit-password-stealer-and-ransomware-program-mixed-into-dangerous-cocktail.html. [Accessed: 12- Nov- 2020].Sgandurra, L. Muñoz-González, R. Mohsen and E.

Lupu, "Automated Dynamic Analysis of Ransomware: Benefits, Limitations and use for Detection", pp. 2-4, 2016. Available: https://arxiv.org/abs/1609.03020v1. [Accessed 2 November 2020].

[15] S. Sharma, R. Kumar and C. Krishna, "Ransom Analysis: The Evolution and Investigation of Android Ransomware", Proceedings of International Conference on IoT Inclusive Life (ICIIL 2019), NITTTR Chandigarh, India, pp. 33-41, 2020. Available: 10.1007/978-981-15-3020-3_4 [Accessed 11 November 2020].Gonzalez and T. Hayajneh, "Detection and prevention of crypto-ransomware", 2017 IEEE 8th Annual Ubiquitous Computing, Electronics and Mobile Communication Conference (UEMCON), 2017. Available: 10.1109/uemcon.2017.8249052 [Accessed 11 November 2020].

[16] S. Mansfield-Devine, "Ransomware: taking businesses hostage", Network Security, vol. 2016, no. 10, pp. 8-17, 2016. Available: 10.1016/s1353-4858(16)30096-4 [Accessed 13 November 2020].

[17] S. Fayi, "What Petya/NotPetya Ransomware Is and What Its Remidiations Are", Advances in Intelligent Systems and Computing, pp. 93-100, 2018. Available: 10.1007/978-3-319-77028-4_15 [Accessed 15 November 2020].

[18] J. Herrera Silva, L. Barona López, Á. Valdivieso Caraguay and M. Hernández-Álvarez, "A Survey on Situational Awareness of Ransomware Attacks—Detection and Prevention Parameters", Remote Sensing, vol. 11, no. 10, p. 1168, 2019. Available: 10.3390/rs11101168 [Accessed 9 November 2020].

[19] J. PETTERS, "Cerber Ransomware: What You Need to Know | Varonis", Inside Out Security, 2020. [Online]. Available: https://www.varonis.com/blog/cerber-ransomware/. [Accessed: 11- Nov- 2020].Zimba, L. Simukonda and M. Chishimba, "Demystifying Ransomware Attacks: Reverse Engineering and Dynamic Malware Analysis of WannaCry for Network and Information Security", Zambia ICT Journal, vol. 1, no. 1, pp. 35-40, 2017. Available: 10.33260/zictjournal.v1i1.19 [Accessed 9 November 2020].

[20] M. Akbanov, V. Vassilakis and M. Logothetis, "WannaCry Ransomware: Analysis of Infection, Persistence, Recovery Prevention and Propagation Mechanisms", Journal of Telecommunications and Information Technology, vol. 1, pp. 113-124, 2019. Available: 10.26636/jtit.2019.130218 [Accessed 8 November 2020].

[21] K. Kraszewski, "SamSam and the Silent Battle of Atlanta", 2019 11th International Conference on Cyber Conflict (CyCon), 2019. Available: 10.23919/cycon.2019.8757090 [Accessed 28 November 2020].Zimba and M. Chishimba, "Understanding the Evolution of Ransomware: Paradigm Shifts in Attack Structures", International Journal of Computer Network and Information Security, vol. 11, no. 1, pp. 26-39, 2019. Available: 10.5815/ijcnis.2019.01.03 [Accessed 28 November 2020] Wirth, "The Times They Are a-Changin': Part One", Biomedical Instrumentation & Technology, vol. 52, no. 2, pp. 148-152, 2018. Available: 10.2345/0899-8205-52.2.148 [Accessed 24 November 2020].

[22] "SamSam Ransomware Campaigns", Secureworks.com, 2018. [Online]. Available: https://www.secureworks.com/research/samsam-ransomware-campaigns. [Accessed: 28- Nov- 2020].Zimba and M. Chishimba, "On the Economic Impact of Crypto-ransomware Attacks: The State of the Art on Enterprise Systems", European Journal for Security Research, vol. 4, no. 1, pp. 3-31, 2019. Available: 10.1007/s41125-019-00039-8 [Accessed 28 November 2020].

[23] M. Midler, K. O'Meara and A. Parisi, "CURRENT RANSOMWARE THREATS", Carnegie Mellon University, 2020.

[24] J. Schultz, "Sodinokibi ransomware exploits WebLogic Server vulnerability", Blog.talosintelligence.com, 2020. [Online]. Available: https://blog.talosintelligence.com/2019/04/sodinokibi-ransomware-exploits-weblogic.html. [Accessed: 28- Nov- 2020].

[25] L. Tung, "VPN warning: REvil ransomware targets unpatched Pulse Secure VPN servers | ZDNet", ZDNet, 2020. [Online]. Available: https://www.zdnet.com/article/vpn-warning-revil-ransomware-targets-unpatched-pulse-secure-vpn-servers/. [Accessed: 28- Nov- 2020].

[26] G. Hall, "Sodinokibi creators leak and sell data stolen from organizations", 2-spyware.com, 2020. [Online]. Available: https://www.2-spyware.com/sodinokibi-creators-leak-and-sell-data-stolen-from-organizations. [Accessed: 28- Nov- 2020].

[27] "Sekhmet Ransomware - Remove Spyware & Malware with SpyHunter - EnigmaSoft Ltd", Remove Spyware & Malware with SpyHunter - EnigmaSoft Ltd, 2020. [Online]. Available: https://www.enigmasoftware.com/sekhmetransomware-removal/. [Accessed: 23- Nov- 2020].

[28] "2012-2019 INTERNET CRIME REPORT", FBI, 2020.

[29] S. Kok, A. Abdullah, N. Jhanjhi and M. Supramaniam, "Ransomware, Threat and Detection Techniques: A Review", Paper.ijcsns.org, 2019. [Online]. Available: http://paper.ijcsns.org/07_book/201902/20190217.pdf. [Accessed: 29- Nov- 2020].Al-rimy, M. Maarof and S. Shaid, "Ransomware threat success factors, taxonomy, and countermeasures: A survey and research directions", Computers & Security, vol. 74, pp. 144-166, 2018. Available: 10.1016/j.cose.2018.01.001 [Accessed 29 November 2020].

[30] M. Paquet-Clouston, B. Haslhofer and B. Dupont, "Ransomware payments in the Bitcoin ecosystem", Journal of Cybersecurity, vol. 5, no. 1, 2019. Available: 10.1093/cybsec/tyz003 [Accessed 29 November 2020].

[31] S. Kok, A. Abdullah, N. Jhanjhi and M. Supramaniam, "Prevention of Crypto-Ransomware Using a Pre-Encryption Detection Algorithm", Computers, vol. 8, no. 4, p. 79, 2019. Available: 10.3390/computers8040079 [Accessed 29 November 2020].

[32] M. Ahmed, S. Nepal and H. Kim, "MEDUSA: Malware Detection Using Statistical Analysis of System's Behavior", 2018 IEEE 4th International Conference on Collaboration and Internet Computing (CIC), 2018. Available: 10.1109/cic.2018.00044 [Accessed 29 November 2020].

[33] J. Tailor and A. Patel, "A Comprehensive Survey: Ransomware Attacks Prevention, Monitoring and Damage

Control", International Journal of Research and Scientific Innovation (IJRSI), vol., no., pp. 116-121, 2017. Available: https://www.researchgate.net/profile/Ashish_Patel60/publication/321161261_A_Comprehensive_Survey_Ransomware_Attacks_Prevention_Monitoring_and_Damage_Control/links/5a127585aca27287ce2a7ac8/A-Comprehensive-Survey-Ransomware-Attacks-Prevention-Monitoring-and-Damage-Control.pdf. [Accessed 29 November 2020].

[34] FBI: 'Criminals continue to defraud and extort funds from victims using CryptoWall ransomware schemes', (23 June 2015), Alert Number: I-062315- PSA. Available at https://www.ic3.gov/media/2015/150623.aspx, 2015, accessed 21 November 2020

[35] "The secret behind CryptoWall's success", Imperva. Available at www.imperva.com/docs/IMPERVA_HII_CryptoWall_report.pdf, 2016, accessed 21 November 2020

[36] Turkel, D.: 'Victims paid more than $24 million to ransomware criminals in 2015 — and that's just the beginning', Business Insider (7 April 2016). Available at http://uk.businessinsider.com/doj-and-dhs-ransomware-attacksgovernment-2016-4, 2016, accessed 21 November 2020

[37] Hern, A.: 'New nasty ransomware encourages victims to attack other computers', The Guardian (12 December 2016). Available at https://www.theguardian.com/technology/2016/dec/12/new-ransomware-victimspopcorn-time-malware, 2016, accessed 15 November 2020

[38] L. Abrams, "New Scheme: Spread Popcorn Time Ransomware, get chance of free Decryption Key", BleepingComputer, 2016. [Online]. Available: https://www.bleepingcomputer.com/news/security/new-scheme-spread-popcorn-time-ransomware-get-chance-of-free-decryption-key/. [Accessed: 21- Nov- 2020].

[39] P.Y. Networks, "Protecting Your Networks from Ransomware", U.S Government interagency technical guidance document aimed to inform chief information officres and chief information security officers at critical infrastructure entities.,2016.Tripwire, "30 Ransomware Prevention Tips | The State of Security", The State of Security, 2020. [Online]. Available: https://www.tripwire.com/state-of-security/security-data-protection/cyber-security/22-ransomware-prevention-tips/. [Accessed: 30- Nov- 2020].

[40] S. Aurangzeb, M. Aleem, M. Iqbal and M. Islam, "Ransomware: A Survey and Trends", vol. 12, no. 1554-1010, 2020. Available: https://www.researchgate.net/profile/Muhammad_Aleem11/publication/317380115_Ransomware_A_Survey_and_Trends/links/5e19a33ea6fdcc283769077c/Ransomware-A-Survey-and-Trends.pdf. [Accessed 30 November 2020].

[41] M. Kiru and A. Jantan, "The Age of Ransomware", Artificial Intelligence and Security Challenges in Emerging Networks, pp. 1-37, 2019. Available: 10.4018/978-1-5225-7353-1.ch001 [Accessed 30 November 2020].

[42] H. Singh and D. Sittig, "A Socio-technical Approach to Preventing, Mitigating, and Recovering from Ransomware Attacks", Applied Clinical Informatics, vol. 07, no. 02, pp. 624-632, 2016. Available: 10.4338/aci-2016-04-soa-0064 [Accessed 7 December 2020].

[43] Symantec. An ISTR Special Report: Ransomware and Businesses 2016. http://goo.gl/CjH90k, 2020

[44] "Choose your wallet - Bitcoin", Bitcoin.org, 2020. [Online]. Available: https://bitcoin.org/en/choose-your-wallet. [Accessed: 30- Nov- 2020].

[45] "Free Ransomware Decryption Tools | Unlock Your Files | AVG", AVG.com, 2020. [Online]. Available: https://www.avg.com/en-gb/ransomware-decryption-tools. [Accessed: 31- Nov- 2020].

[46] R. Shaikh and M. Sasikumar, "Data Classification for Achieving Security in Cloud Computing", Procedia Computer Science, vol. 45, pp. 493-498, 2015. Available: 10.1016/j.procs.2015.03.087 [Accessed 31 November 2020].

[47] "World Internet Users Statistics and 2020 World Population Stats", Internetworldstats.com, 2020. [Online]. Available: https://internetworldstats.com/stats.htm. [Accessed: 15- Dec- 2020].L. Joseph C. Chen. Evolution of exploit kits - exploring past trends and current improvements. https://www.trendmicro.com/cloudcontent/us/pdfs/security-intelligence/whitepapers/ wp-evolution-of-exploit-kits.pdf, 2015 [Accessed: 15- Dec- 2020].

[48] Cyber Threat Alliance. Lucrative ra Analysis of the cryptowall version 3 threat. http://cyberthreatalliance.org/cryptowallreport. pdf, 2020

[49] SANS ISC InfoSec Forums. Malicious spam with links to cryptowall 3.0 - subject: Domain [name] suspension notice. https://isc.sans.edu/forums/diary/ , 2020

[50] Z. Zorz. Chimera crypto-ransomware is hitting german companies. http://www.netsecurity.org/malware_news.php?id=3141 , 2020