sustainability

MDPI

Review

Ransomware Detection, Avoidance, and Mitigation Scheme: A Review and Future Directions

Adhirath Kapoor [1], Ankur Gupta [1], Rajesh Gupta [2], Sudeep Tanwar [2,*], Gulshan Sharma [3] and Innocent E. Davidson [3,*]

[1] Model Institute of Engineering and Technology (Autonomous), Jammu 181122, India; adhirathlrkapoor@gmail.com (A.K.); ankurgupta@mietjammu.in (A.G.)
[2] Department of Computer Science and Engineering, Institute of Technology, Nirma University, Ahmedabad 382481, India; 18ftvphde31@nirmauni.ac.in
[3] Department of Electrical Power Engineering, Steve Biko Campus, Durban University of Technology, Durban 4001, South Africa; gulshanS1@dut.ac.za
* Correspondence: sudeep.tanwar@nirmauni.ac.in (S.T.); innocentD@dut.ac.za (I.E.D.)

Abstract: Ransomware attacks have emerged as a major cyber-security threat wherein user data is encrypted upon system infection. Latest Ransomware strands using advanced obfuscation techniques along with offline C2 Server capabilities are hitting Individual users and big corporations alike. This problem has caused business disruption and, of course, financial loss. Since there is no such consolidated framework that can classify, detect and mitigate Ransomware attacks in one go, we are motivated to present Detection Avoidance Mitigation (DAM), a theoretical framework to review and classify techniques, tools, and strategies to detect, avoid and mitigate Ransomware. We have thoroughly investigated different scenarios and compared already existing state of the art review research against ours. The case study of the infamous Djvu Ransomware is incorporated to illustrate the modus-operandi of the latest Ransomware strands, including some suggestions to contain its spread.

Keywords: Ransomware; cryptography; WannaCry; Djvu; malware; Ransomware detection

Citation: Kapoor, A.; Gupta, A.; Gupta, R.; Tanwar, S.; Sharma, G.; Davidson, I.E. Ransomware Detection, Avoidance, and Mitigation Scheme: A Review and Future Directions. *Sustainability* **2022**, *14*, 8. https://doi.org/10.3390/su14010008

Academic Editor: Anna Visvizi

Received: 18 November 2021
Accepted: 17 December 2021
Published: 21 December 2021

1. Introduction

Increased connectivity and digitization have facilitated cyber-criminals in designing and launching large-scale cyber-attacks targeting individuals and corporations worldwide. While individual naivete and lack of awareness enable these attacks to bypass basic security mechanisms, security vulnerabilities in the IT systems of small and large corporations are increasingly being exploited to cause business disruptions. The cyber-attack canvas keeps expanding rapidly as cyber-criminals consistently circumvent security provisions designed and deployed by organizations. Increasingly, the target of the attacks is data that is critical to individuals and organizations alike. Threat actors are cashing in on opportunities that can help them seize control of valuable data to demand a ransom from the data owner. Ransomware is a form of malware that infects a computer or multiple computers over a network, encrypting files and folders, rendering them unusable. Users are then prompted for a ransom typically to be paid in cryptocurrency. Ransomware is not a new threat, but its use is surging and causing heavy financial losses all over the world [1]. It is a major challenge for cyber-security analysts and Reverse Engineers as typical Ransomware is not detected by anti-virus software due to its polymorphic nature.

According to [2], almost 51% of the organizations worldwide were hit by highly sophisticated Ransomware attacks in 2020. These attacks were using advanced command and control servers, making them challenging to reverse engineer. Among all the countries studied in the report, India was affected the most by the deadly Ransomware attacks, with almost eighty-two percent of organizations being hit by Ransomware. Netwalker is

one of the newest and dangerous Ransomware strands [3]. Its popularity is the method of propagation, using phishing emails related to COVID-19, thus luring the victim to download the attachments resulting in the execution of the portable binaries and system infection. In February 2021, the latest Ransomware strand, Zeoticus 2.0, successor to the infamous strand Zeoticus was released. Zeoticus 2.0 has raised the stakes since it is now proving extremely hard to control and mitigate. It can execute completely offline without requiring any command and control server. For receiving the Ransom payment, Zeoticus uses highly secure and encrypted Proton mail accounts to evade tracing.

The history of Ransomware dates back to the late 1980s. The first Ransomware named Acquired Immunodeficiency Syndrome (AIDS) Trojan, was released via a floppy disk. The AIDS Trojan contained a program that would count the number of times a computer system was started, and once this count reached the number 90, all of the files would be encrypted. The only way to be able to use them again was to pay a ransom amount of $189 [4]. During the early days, Ransomware authors attacked victims to showcase their technical prowess. It was not until the early 2000s when cyber-criminals began to exploit users for financial gains as data gained primacy. In 2004, a Ransomware strand named GPCode was released. GPCode infected Windows Machines via e-mail attachments. It used a 660-Bit RSA key to encrypt files and folders [5,6]. Since then, Ransomware families like WannaCry, Cerber, Petya, etc., have evolved and caused monetary damage worth billions of dollars. Figure 1 depicts a timeline of the prevalence of Ransomware families.

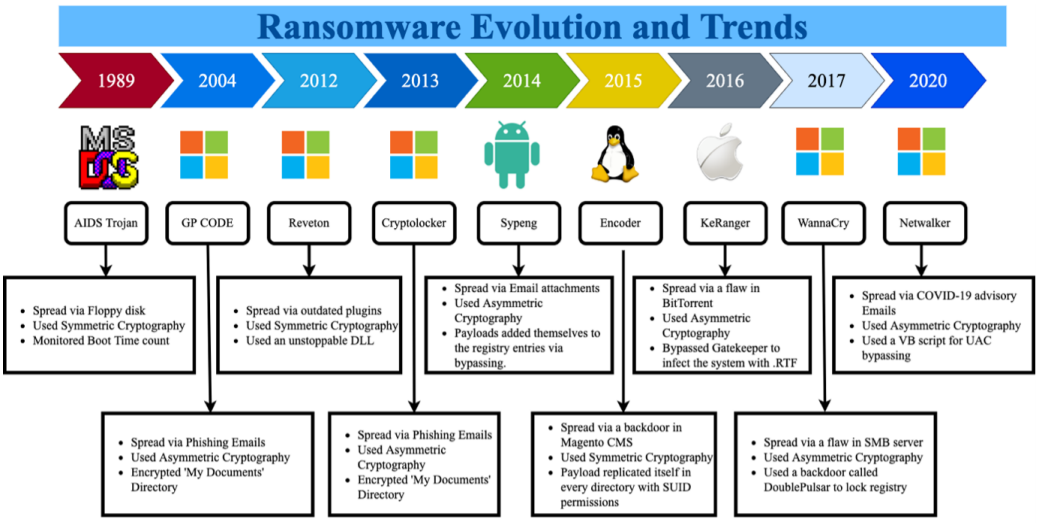

Figure 1. Ransomware timeline and trends.

1.1. Motivation of the Study

The motivation of this study is as follows:

- There is a sudden surge in extremely dangerous Ransomware attacks that have crippled most businesses and individuals alike. Ransomware poses a high threat and needs to be tackled at a global level.
- The existing literature contains solutions for mitigating either specific Ransomware or proposes generic solutions. A comprehensive analysis encompassing issues in securing individual users and corporations is lacking.
- Ransomware avoidance techniques are the most effective and need specialized focus as mitigation and recovery from Ransomware is increasingly complex.

1.2. Research Contributions

In this article, we make the following contributions:

- We present DAM, a theoretical framework to review and classify the tools, techniques, and strategies to detect, avoid and mitigate Ransomware.

- We put forward a continuum for the avoidance of Ransomware. This continuum can be adopted by different organizations ranging from critical deployments to small-scale organizations.
- Finally, we present a case study on one of the recent Ransomware strands, Djvu, where we discuss the technical aspects related to Djvu and then apply the DAM framework to consider potential containment/response strategies.

Table 1 maps the contributions to the sections they are discussed in.

Table 1. Mapping of research contributions with respective sections.

Research Contributions	Reference Section Numbers
Contribution 1	Section 4
Contribution 2	Section 4.2
Contribution 3	Section 5
Contribution 4	Section 6

1.3. Paper Organization

The research article is organized as follows: Section 2 presents the background. Section 3 discusses the state-of-the-art technologies and presents a comparative analysis of different survey articles with ours. Section 4 presents the DAM framework for classification and analysis of defense techniques against Ransomware. Section 5 provides some ideas for avoiding Ransomware infection and mitigating its impact. Section 6 presents a comprehensive case study of DJVU, while Section 7 concludes the paper. The complete structure of the paper is explained by Figure 2 while Table 2 defines all the acronyms to be used throughout the article.

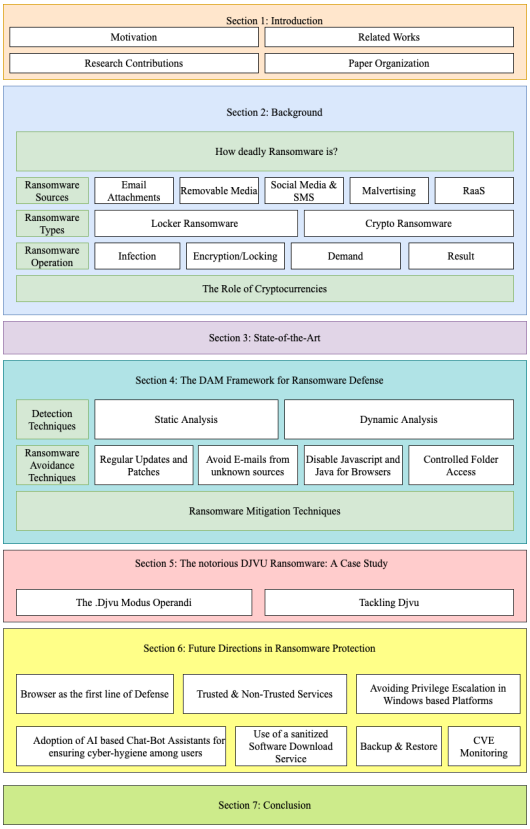

Figure 2. Structure of the article.

Table 2. Acronyms.

AES	Advanced Encryption Standard
AIDS	Auto Immune Deficiency Syndrome
AOL	America Online
ASCII	American Source Code for Information Interchange
BBC	British Broadcasting Corporation
C2C	Command & Control
CTB	Curve Tor Bit-locker
DAM	Detect Avoid Mitigate
DLL	Dynamic Link Library
DNS	Domain Name Service
IOC	Indicators of Compromise
IT	Information Technology
MBR	Master Boot Record
ML	Machine Learning
MSN	Microsoft Network
P2P	Peer-to-Peer
PC	Personal Computer
PDF	Portable Document Format
RaaS	Ransomware as a Service
RSA	Rivest Shamir Adleman
SDN	Software Defined Networking
SMB	Server Message Block
TCP	Transmission Control Protocol
TOR	The Onion Routing
URL	Uniform Resource Locator
UTM	Unified Threat Management

2. Background

2.1. How Deadly the Ransomware Is?

Ransomware is considered one of the most dangerous variants of malware. This is primarily because it doesn't even require much user interaction for privilege escalation. Even the usage of industry-standard tools and technologies have not been able to contain the wrath of Ransomware. Once Ransomware infects the device, it becomes impossible for the victim to access the files. Due to the ransom being paid using cryptocurrency, there is no way to track the perpetrators of the Ransomware attacks. Figure 3 illustrates the monetary damage caused by Ransomware in the year 2020 as compared to its predecessors [7,8].

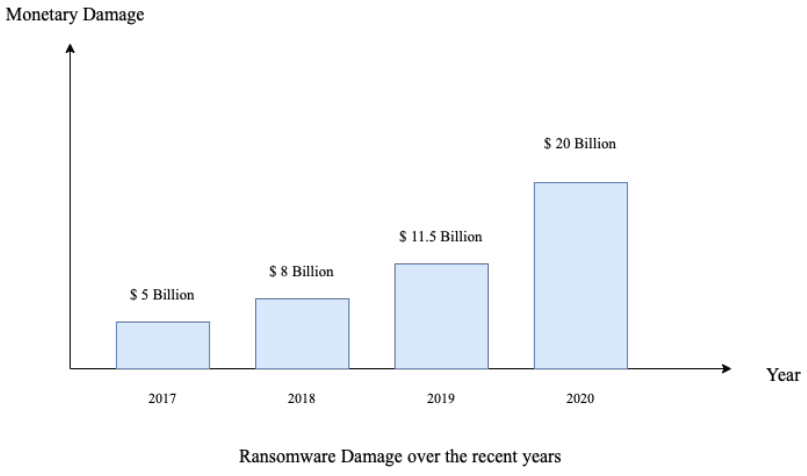

Figure 3. Ransomware damage over the recent years.

2.2. Ransomware Sources

Ransomware propagates primarily due to a lack of Cyber-hygiene at the individual level. Cyber-hygiene refers to all aspects of online safety [9] including browsing behavior, availability and consistent updating of antivirus software, installing third-party software, and user awareness. Cyber-hygiene must be practiced for keeping Ransomware and other strands of malware away. Despite improving security standards and protocols, Ransomware families have managed to penetrate the defense systems of organizations, governments, and individual users. Some of the main sources of Ransomware include:

2.2.1. Email Attachments

Email attachments usually contain Portable Document Format (PDF) documents, voicemails, images, e-invites, etc. These attachments using various steganographic techniques contain embedded malicious files. Ransomware perpetrators use techniques that make an email look like it was sent from a trusted and known sender. There are various tools available through which attackers with no technical knowledge can craft malicious emails.

2.2.2. Removable Media

Removable Media is not considered as an entry portal for Ransomware by many. However, Tischer et al. [10] conducted a survey, revealing that people are really intrigued by what might be there in a random Universal Serial Bus (USB) drives lying at a public place. A lot of Organizations that did not disable USB ports have been hit by Ransomware via this mode [11].

2.2.3. Malvertising

Malvertising [12] is the organized practice of infecting the advertising infrastructure that websites use for displaying online advertisements. Malvertising has proved to be another popular technique for infecting systems with Ransomware. It has infected systems even via browsing trusted sites like British Broadcasting Corporation (BBC) News, America Online (AOL) and Microsoft Network (MSN) [13]. It tricks the browser into downloading malicious file extensions automatically. Exploit rootkits like Angler, Magnitude and Nuclear are then able to help the attacker gain access to the victim's device [14,15].

2.2.4. Social Media & SMS

This type of Ransomware propagation falls under the category of Social Engineering, where the victim is lured into clicking links that they should not. Attackers use the technique of Uniform Resource Locator (URL) shortening in order to add obscurity to the original link. Users with poor Cyber-hygiene are lured into clicking these links. Sometimes, users also receive SMS messages that depict urgency and force them into clicking those links [16].

2.2.5. Ransomware as a Service

Like other hosting services on the Dark Web that offer anonymity, Ransomware-as-a-Service (RaaS) has emerged as a marketplace exclusively for attackers with insufficient programming skills to easily propagate Ransomware. The RaaS service providers either take a cut from the buyer or charge service usage fees.

2.3. Ransomware Types

There are mainly two prevalent types of Ransomware, known as Crypto Ransomware and Locker Ransomware.

2.3.1. Crypto Ransomware

Crypto Ransomware uses encryption algorithms to encrypt the victims' data using two approaches. In case of a Symmetric Algorithm, there is just one key that is used for

both encryption and decryption. The second algorithm which is more prevalent is the Asymmetric Algorithm through which the data is encrypted using a public key and the victim can only get their data back when they pay for the decryption key [17]. Over the years, attackers have made it difficult for reverse engineers trying to decrypt the data without paying the ransom. Attackers now use a combination of both symmetric and asymmetric algorithms to make the decryption process more challenging. Victim's data is encrypted using a symmetric algorithm due to its speed [18,19]. Then, the key used is encrypted using the public key possessed by the malicious actor [20].

2.3.2. Locker Ransomware

As the name indicates, Locker Ransomware locks the device instead of encrypting the files and folders. Upon being infected, the victim's device is prevented from bring accessed. The data inside is untouched. This type of Ransomware is less effective than Crypto Ransomware, because the data can still be accessed by moving the storage device to another computer [21].

2.4. Ransomware Operation

The various phases of Ransomware operation as shown in Figure 4 are detailed below:

2.4.1. Infection

The first stage is the spread of the Ransomware to the victim's device. As discussed in the earlier section, there are multiple sources through which Ransomware finds an infection vector. In this stage, the strategy of the Attacker is to get their Ransomware downloaded on the victim's machine. This stage is heavily dependent on the victim's activities and overall Cyber-hygiene. If the potential victim is cyber-aware [22], then it is highly possible that the Ransomware won't be able to infect the system.

2.4.2. Encryption/Locking

Upon infection, the Ransomware starts performing its programmed sequence of actions depending on its type. A very strong property of recent Ransomware strands is that it contacts a central command-and-control (C2C) server through which process of automation for the attacker becomes simple. The C2C Server also acts as a repository through which different victims can download their decryption keys after making the payment. After the first stage, the cryptographic keys are generated on either the victim's Personal Computer (PC) or in the C2C server. The attacker then proceeds to lock the files and folders or can straight away alter the master boot record so that the victim is unable to access their device.

2.4.3. Demand

During the third stage, a message starts getting displayed on the screen, which demands a ransom amount from the victim, so that they can get the access back to their system. The attacker provides a Bitcoin address for the payment of ransom. This increases the difficulty for law enforcement agencies to trace the payment back to the attacker.

2.4.4. Result

After the third stage, it is up to the user to either pay the ransom amount or not. There are three outcomes that result at this stage. If the victim decides to pay the ransom, then they will be provided with a decryption key to unlock access back to their devices. Another outcome can result when the victim has strong technical skills or can take the help of reverse engineers to reverse the Ransomware operations and get the files back. The third outcome results from the situation when the victim is unable to pay the ransom. This results in permanent damage and complete loss of data.

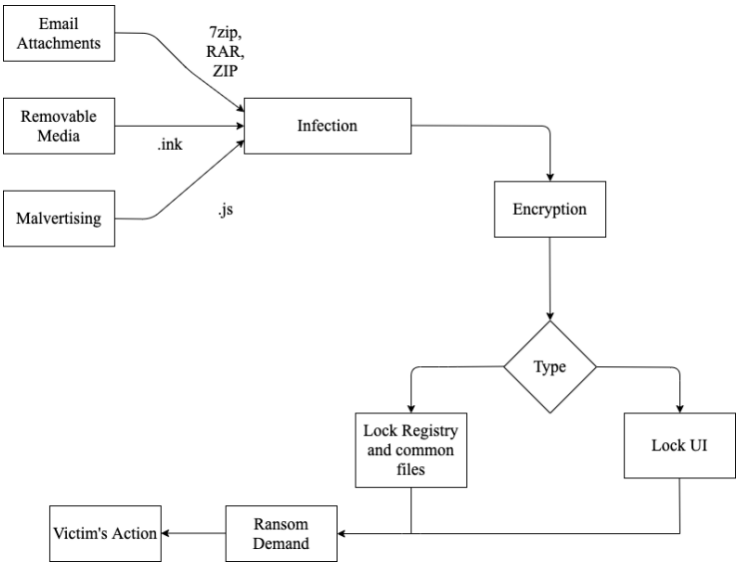

Figure 4. Typical Ransomware sequence of operations.

2.5. The Role of Cryptocurrencies

In the early days of Ransomware, attackers would demand money in the form of direct bank deposit or via money transfer agencies. These methods of payment could be traced back to the attacker. Since emergence of cryptocurrencies, Ransomware attacks have exploded. This is majorly due to the fact that cryptocurrencies introduce the concept of anonymity. Cryptocurrencies facilitate the creation of strong Ransomware which, instead of deploying a direct one-to-one payment method, used a third-party payment gateway so that the risk of being traced is minimized. The first ever Ransomware that proved to be really strong in terms of maintaining anonymity & use of a well-built encryption algorithm was CTB Locker. CTB locker stood for Curve, The Onion Routing (TOR) and Bitcoin locker. It used elliptic curve cryptography to encrypt the data, TOR Protocol for anonymous means of communication between the victim and the attacker and Bitcoin as a payment method for paying the ransom in a way that the transfer wouldn't be traced [23]. Usually, when a cryptocurrency is set up as a payment method, an attacker passively watches the blockchain, an enabler for cryptocurrencies to check if the ransom amount has been paid or not. Once, the payment is made, the process of sending the decryption key to the victim can be initiated via automation. This puts the theory of anonymity and un-traceability into practice. Cryptocurrencies also play a very important role in distribution of Ransomware via the dark web. Script Kiddies make use of platforms like RaaS to buy customized strands from exploit developers. Evidence suggests that most of the Ransomware families such as WannaCry have been successful because of the un-traceability provided to cyber-criminals by cryptocurrencies.

3. State-of-the-Art

Researchers, cyber-security firms and government agencies have researched all aspects of Ransomware propagation, operation and devising effective combat techniques. Although, a few of them were adopted by organizations and governments; most of the frameworks have not proved successful in practice. This is due to the fact that security is multi-dimensional encompassing network security, data security, application security and finally individual Cyber-hygiene practices [24]. It is therefore extremely challenging to design blanket security solutions. Several works have reviewed the impact of Ransomware and summarized techniques to counter its threat. Since, our work is focused on summarizing the existing detection, avoidance and mitigation techniques while providing insights to improve countermeasures, a comparative analysis with existing review papers is provided in Table 3.

Table 3. Comparative analysis of the proposed survey with the state-of-the-art surveys on Ransomware detection, avoidance, and mitigation.

Researcher	Contribution	Pros	Cons
Aurangzeb et al. [25]	Evaluated attack methodologies for Windows Based Ransomware families.	The authors discussed all possible exploit vectors and kits used in creation of Windows based Ransomware families.	They did not specifically propose any technical solutions required to counter Ransomware.
Tailor et al. [26]	Analyzed different encryption techniques used by modern Ransomware strands so as to develop better detection strategies.	The authors presented a comprehensive overview of different encryption techniques used by both Locker and Crypto Ransomware families.	Techniques proposed by the authors could include some implementation based details for effective detection of Ransomware.
Tandon et al. [27]	Explained the modus-operandi and architecture of typical Ransomware attacks.	The authors gave a detailed view of MS-017 exploit and how it eventually used Double Pulsar to cause the spread of WannaCry.	Discussions are presented in the context of a single Ransomware. Broad-based countermeasure strategies not provided.
Genç et al. [28]	Discussed the current Ransomware mitigation strategies and evaluated their effectiveness.	The authors explained the latest ransomware strands which can be generated using rootkits in addition to Ransomware of things.	Novel mitigation strategies for obfuscated Ransomware strands not suggested.
Oz et al. [29]	The authors summarized all the different Ransomware families based on the exploits that helped them propagate.	The tables and the summaries presented by the authors can be adopted by researchers to create new mitigation frameworks.	The authors did not discuss the solutions with respect to the latest families that use offline encryption techniques.
Kok et al. [30]	The authors' research was focused on finding out the effectiveness of preexisting detection techniques and thus highlighted the requirement of an ML based solution to create better detection techniques.	The authors explained the Ransomware lifecycle in a novel manner and mapped it to the different techniques to find out their effectiveness.	The authors outlined an ML based solution using linear regression but did not technically explain its effectiveness over existing solutions.
The proposed survey	The authors discuss all possible Ransomware propagation techniques and put forth a Ransomware avoidance Continuum that can be adopted by organizations and individuals alike.	The authors presented a good overview of the adversary methodologies and performed a case study of one of the recent Ransomware strands, Djvu. Novel suggestions are put forth to contain the spread of Ransomware.	-

4. The DAM Framework for Ransomware Defense

We propose the DAM framework to classify potential defense techniques, tools and strategies for countering the menace of Ransomware.

4.1. Detection Techniques

Various Ransomware detection techniques have been proposed by both academic researchers and industrial security experts. Some of them are currently in use as well. These techniques mostly work via static or dynamic analysis of the executable suspected to be Ransomware. Static analysis of an executable is performed through examination of the code without actually running the executable. Static analysis of a binary consists of static linking, locating American Source Code Information Interchange (ASCII) strings, packer detection and memory relocation. Dynamic analysis is performed after execution of the suspected Ransomware. During its execution, the actions and system calls made by the suspected file are recorded and based on this information, a final report is generated.

4.1.1. Static Analysis

Subedi et al. [31] proposed a methodology that would utilize static analysis as an approach to detect Ransomware. The approach followed by the researchers contained a framework that would first reverse engineer the PE file using assembly language and then subsequently apply Dynamic Linkable Library (DLL) and function call extraction on the PE file. The Framework was developed as a tool called CRSTATIC. They analyzed forty-

three Ransomware Samples with CRSTATIC using different parameters. This work was able to differentiate between Ransomware and Normal Programs via a Cosine similarity graph based on assembly instructions. Although, relatively new, CRSTATIC cannot detect the latest ransomware families which deploy signature evasion techniques. Despite its drawbacks, CRSTATIC used pre-parse, a lightweight parser that could detect malicious PE files with respect to different parameters like relocations and byte read operations. CRSTATIC was not able to detect Locker Ransomware families.

Zheng et al. [32] devised a tool called GreatEatlon for detecting Android Ransomware. This tool was created by combining the features present in Heldroid [33], APKTool and other open source analysis tools. GreatEatlon used four stages to identify the presence of Ransomware on an Android Device. The first stage was to follow the code flows of an executable suspected to be a Ransomware. Any Ransomware's first line of action is to find the files it wants to encrypt. GreatEatlon was easily able to identify the path of Ransomware by utilizing an extension of FlowDroid [34], a state-of-the-art technique used for analyzing code flows of Android applications. GreatEatlon then passed the Executable through the second stage in which DeviceAdmin APIs were inspected when the executable was allowed to run. If the APIs were misused by the executable to escalate its privileges, then it would be flagged as malicious. Last two stages deployed static and manual analysis techniques to finally identify the behavior of the suspected executable file.

Hsiao et al. [35] conducted reverse engineering experiments on the infamous WannaCry Ransomware to understand how the malicious binary works. The mode of analysis used by the authors was Static analysis. IDA Pro [36] was used for reverse engineering to understand the inner working of the Ransomware. The PE file which was initially used for the first stage of Ransomware operation converted itself into different formats in the subsequent stages. First, the PE file is delivered through the Eternal Blue exploit [37] which then uses a Windows API to embed itself. In the next phase, two services, mssecsvc.exe and tasksche.exe are responsible for further propagation by altering the environment settings. The third stage is responsible for the overall encryption of the victim's data where taskche.exe loads the encryption .dll in the device's memory. The last stage is maintained by C2C servers for tracing the payments and the course of infection.

4.1.2. Dynamic Analysis

Sgandurra et al. [38] tested 542 different samples of Ransomware families through EldeRan, a hybrid approach comprising of machine learning techniques and dynamic code analysis. EldeRan tested application samples against a set of parameters that would be able to identify if the sample is a Ransomware during the infection phase. EldeRan successfully analyzed Windows API calls, Registry Key operations, file and directory operations, dropped files and embedded strings. The next component of EldeRan involved the Machine Learning approach that comprised of feature selection that could distinguish Ransomware from a regular software via Mutual information criteria [39] and classification that used Regularized logistic regression. Overall, EldeRan achieved a great success rate in detection of new Ransomware families.

Maimó et al. [40] were the first authors to discuss the impact of Ransomware on Clinical environments. The first ever Ransomware to target the medical industry was WannaCry. Upon its outbreak, all the NHS operations were put to a halt and most of the appointments and surgeries were canceled. They devised a ML based technique compatible with Integrated Clinical Environment (ICE) architecture that could detect the presence of a Ransomware before it could even start propagating. Their technique was able to detect the changes in network traffic when the Ransomware was being run. These patterns were then fed to a probabilistic supervised Ransomware classifier to finally extract complex features of the sample being run. The solution proposed had four main components. The first module monitored traffic patterns resulting from a live sample. The next module required human supervision for generating a suitable dataset that would be fed to the ML algorithms for detection and classification of Ransomware. The third module identified the

anomalous patterns and labeled them. The last module focused on mitigation techniques through the aid of Rule based ML models.

Kao et al. [41] conducted another reverse engineering experiment on WannaCry Ransomware through Dynamic mode of analysis. In this case, WannaCry sample was run on the system and its interactions with processes, file system, registry and network activity were recorded. The authors used a tool named YARA to record the signature of the sample. To carry out behavioral analysis dynamically, SysInternals Suite and Wireshark were made use of. WannaCry being a multi-stage Ransomware uses a process to load the tasksche.exe file that in turn launches different processes.

When a ransomware attack occurs, it is really important to detect it as early as possible because in this case, every second is significant as early detection results in a lesser degree of damage. Morato et al. [42] devised an algorithm called REDFISH which claimed to detect the presence of ransomware in an organizational setting way before all the frameworks till date through analysis of network traffic. The authors used around 19 ransomware families to test their algorithm. This algorithm was designed to tackle ransomware strands that were created to encrypt files and folders present in shared networking drives in Network Attached Storage. After carefully evaluating all the environments where Ransomware can persist, the authors found out that existence of SMB in a network indicated a possible habitat where Ransomware can dwell in. They used a network traffic inspection device to analyse the behaviour of incoming and outgoing traffic. They analysed the usage of SMB based commands very closely to look for anomalies in the traffic. The authors ran several tests on the algorithm and reported that REDFISH can detect ransomware within 20 s. The authors stated that although REDFISH proved to be fast but the strands were still able to lock 10 to 15 files before being detected. We believe REDFISH is a feasible algorithm for organizational settings and can be easily deployed because of its minimal impact on the server resources. Also, the network inspection device used by REDFISH stays out of the production network, so any malware which also has the ability to launch reverse shells for an attacker would not be able to deactivate the detection mechanism [43]. However, in the modern scenarios where ransomware is highly stealthy in nature, this algorithm can fail. Recently, there is a surge of Ransomware strands that use Microsoft Word and Excel based documents to deliver themselves onto the victims' machines. VBA and Excel macros can obfuscate PowerShell code within their streams so that when they are passed through antivirus scans, they are deemed to be benign. We strongly believe that in cases like these, REDFISH will not be able to detect the ransomware strands within the stipulated time frame.

Chen et al. [44] created an automated early detection tool with a novel feature of pattern extraction. Their tool was able to capture new strands and samples through the sandbox and was able to prepare an automated analytic report. The report was able to present the most unique patterns and behavioural paths followed by different ransomware families. For experimentation and validation, the authors used seven ransomware families. Through the results of experimentation, the authors were able to find out the efficiency of each of the algorithms used for pattern extraction. In order to unsheathe the features of different ransomware families, they used TF-IDF, ET and LDA to automate the whole process. The tool developed by the authors can be used in medium to large enterprises as it can easily handle large log data and detect ransomware before other industry standard solutions. The approach used by the authors focused on calculating the time efficiency of different algorithms but they did not compare their tool with other frameworks and algorithms in effect. Also, the algorithms used require training before they can make intelligent decisions. The algorithms will not work well for the latest strands like Darkside [45].

Imtiaz et al. [46] approached the problem of Android Ransomware by using a novel methodology called DeepAMD. DeepAMD used deep ANNs for detecting ransomware before it could exploit other applications on the smartphone. DeepAMD used a dataset to extract features [44] initially for feature selection. The cleansed data resulting from feature extraction was analysed both statically and dynamically to deem the nature of an

application. Overall, DeepAMD proved to be a novel and effective approach for early detection of the most advanced ransomware families. This is because of a good rate of validation of DeepAMD using the latest and updated Android Malware dataset [47]. In addition to detection of Ransomware, DeepAMD can also detect scareware [48] and adware [49] families.

Kok et al. [50] developed a new algorithm called Pre-Encryption Detection Algorithm (PEDA) that was able to detect Crypto Ransomware which is the most dominant type of Ransomware. According to the authors, PEDA could detect almost all crypto Ransomware strands in their pre-encryption stage [51]. PEDA is a hybrid algorithm that first examines a suspicious binary via static analysis through checksum comparison and then dynamically via the usage of an algorithm that monitor pre-encryption [52] APIs. Along with this, PEDA also identified 3 APIs that could locate the presence of Ransomware. The algorithm's success held true for most of the Crypto strands. The only limitation of PEDA is its high dependence on Windows API. So, if PEDA is deployed as the only detection mechanism, it might not be able to detect the latest families.

Al-rimy et al. [53] also created a model for early detection of Crypto Ransomware but through a different approach. The model used two detection modules, one for analysing the behaviour and the second for estimation of anomalies. Fusion of both the results would then give a proper decision on whether the binary is malicious or benign. The authors claimed that this model would certainly be able to detect zero day attacks and advanced persistent threats. Through the results shown in the work, the model performed extremely well in detecting the ransomware strands from a dataset of 12,000 applications. One benefit of using this solution is that it can be used for other ecosystems too because of the extremely low false positive rate.

Figure 5 illustrates the main analysis techniques for detection along with their sub types.

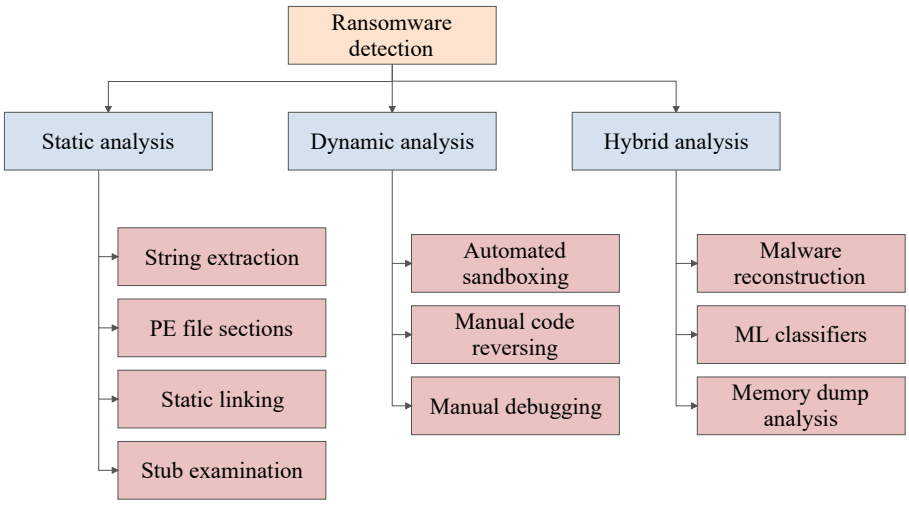

Figure 5. Taxonomy of Ransomware detection techniques.

Table 4 sums up the popular detection techniques used by the researchers along with the mode of analysis used and the samples analyzed.

Ransomware detection techniques have matured in their combat effectiveness against major ransomware attacks. Detection techniques are now hybrid in nature and most of these deploy AI based strategies for improving detection effectiveness. Despite the advancement in the detection techniques, the latest Ransomware families continue to evade them as these techniques are not designed to contain all of the Ransomware strands at once. Solutions for Detection are created mostly to detect a single strand or a single type of Ransomware, so generic solutions do not exist as they are extremely challenging to develop. Some are even designed to just detect only one version of a particular Ransomware. So, it is evident that

current state of the detection techniques is reactive in nature and developed in response to new ransomware releases.

Table 4. Comparative analysis of various Ransomware detection techniques given by the researchers across the globe.

Detection Technique/ Tool	Mode of Analysis	Analysis Methodology	Limitations of the Methodology	Ransomware Samples Analyzed
CRSTATIC [31]	Static analysis	Pre-parsing of PE to find out the system calls, relocation and byte read operations.	Only able to detect Crypto Ransomware family.	Jigsaw, Shatana, Cryptomix
GreatEatlon [32]	Static analysis	Identification of code flows followed by inspecting API usage.	The methodology cannot detect the families that use signature evasion techniques.	Contagio-Mobile
ML-Based hybrid Android analysis using Naïve Bayes [54]	Static & Dynamic analysis	Opcode frequency detection and evaluation of system calls and CPU usage to determine the malicious nature of Android Binaries.	The datasets used do not contain the latest Android Ransomware families	Svpeng, scare package, simple locker
Third-Gen hybrid detection approach [55]	Static & Dynamic analysis	Examination of binary against fixed parameters before running it and then sandboxing it to detect the W-32 dropper file.	The Cerber W-32 dropper has many variants and thus this approach can only detect the W-32 V1.	Cerber
EldeRan [38]	Dynamic analysis	Parameter matching during the initial phase of infection followed by feature selection using Mutual information criteria.	Since it focuses only on detection of early phases of Ransomware, it fails to capture the obfuscated encryptors and export files.	Citroni, Kollah, Kovter
ML-based monitoring technique [40]	Dynamic analysis	Probabilistic supervised Ransomware classification of anomalous network patterns.	The traffic patterns captured can have exploit kits hidden via steganographic techniques	Petya, BadRabbit, Power Ghost
ML-based detection using WEKA and T-Shark [56]	Dynamic analysis	ML analysis of Windows Ransomware network traffic followed by ML classifiers to achieve high detection rate.	WEKA used limited datasets and was not able to distinguish between the two major categories of Ransomware.	Padcrypt, Teslacrypt, Locky
Dynamic API call-based detection approach [57]	Dynamic analysis	Monitoring of dynamic API calls using the CF graphs along with deployment of data mining techniques to detect unknown Ransomware families.	New Ransomware families built via anti-analysis techniques cannot be detected by this approach.	Wannacry, Locky
Markov & Random Forest model-based detection [58]	Dynamic analysis	Detection of Windows API sequence call patterns through Markov model and deploy Random Forest model to control FPR and FNR.	The range resulting from Random Forest model cannot give a perfect estimation and can lead to benign binaries being classified as malicious.	CryptoLocker
UNVEIL [59]	Dynamic analysis	Generation of an artificial sandboxing environment which interacts with binaries to determine their behaviour.	The artificial sandboxing environment cannot always detect DLL hijacking.	SilentCrypt

4.2. Ransomware Avoidance Techniques

Ransomware attacks have been successful mostly because of poor Cyber-hygiene practices. The avoidance techniques available for the masses to protect their devices from the deadly Ransomware are very few in number and are generalized in nature. Researchers have proposed a few advanced techniques for Ransomware avoidance, but they are limited to specific environments and specific strands of Ransomware and hence do not qualify as one-for-all solution.

General techniques that can be followed by users to protect their devices from Ransomware are:

4.2.1. Regular Patches and Updates

When the WannaCry Ransomware hit the world in 2017, it created a chaos everywhere and rendered all the ICE computers useless, bringing the operations at most of the hospitals and clinics in UK to a halt. WannaCry caused infection of devices through the exploitation of a vulnerability in the SMB protocol. SMB is a Windows based protocol that allows the computers to share files when they are on the same domain. An exploit kit named as Eternal Blue was used to exploit the vulnerability and this is how WannaCry after entering one device, infected the whole network. Computing Platforms which are regularly patched and updated have an extremely low chance of being infected with a Ransomware as most of the attackers' prey upon vulnerabilities that have not been patched. Updating and Patching is not just limited to Operating Systems. Browsers and other applications that are live on the network should be updated and patched regularly.

4.2.2. Avoid e-Mails from Unknown Sources and Attachments

Emails from unknown senders should not be opened as they can carry links and attachments which if opened can install Ransomware on the devices. Emails meant for delivering Ransomware are usually very compelling and entice the recipient to click on the links or download the attachments. Organizations should conduct a training for employees to help them identify phishing emails. Attackers can attack a specific department of the organization. For example, the Inventory Department can receive an email with a billing attachment from an attacker posing to be a legitimate dealer [60]. Use of email filters and spam detection extensions should be deployed for all email services.

4.2.3. Disable JavaScript and Java for Browsers

Another important technique to prevent Ransomware spread is to disable JavaScript and Java on Browsers. Malvertising, as discussed in Section 2, tricks the browsers to download executable files which can then infect the whole system. Malvertising uses JavaScript for execution of the malicious code, so disabling it would prove beneficial in preventing Ransomware attacks. The disablement restricts scripting attacks that can lead to open redirects to Ransomware distribution websites.

4.2.4. Controlled Folder Access

This technique works best for organizational environments that deploy Windows based devices for work purposes. It enables the trusted applications to access the designated folders. Designated folders are mapped to different applications when Controlled Folder Access is configured initially. This technique works with a database of trusted applications maintained from time to time. If an application or an executable is not present in the trusted application database, it is barred from modifying the contents of the designated controlled folders. Controlled Folder Access is an excellent avoidance measure as it can protect boot sectors as well which are targeted by the latest Ransomware families. Controlled Folder Access also utilizes an audit mode that can further create a honeypot for the executables that are not present in the trusted application database trying to access protected folders.

As seen above, the Ransomware avoidance techniques are fairly generic in nature and Cyber-hygiene is the best policy to be followed, especially for individual users.

Figure 6 depicts a Ransomware avoidance continuum for different organization types.

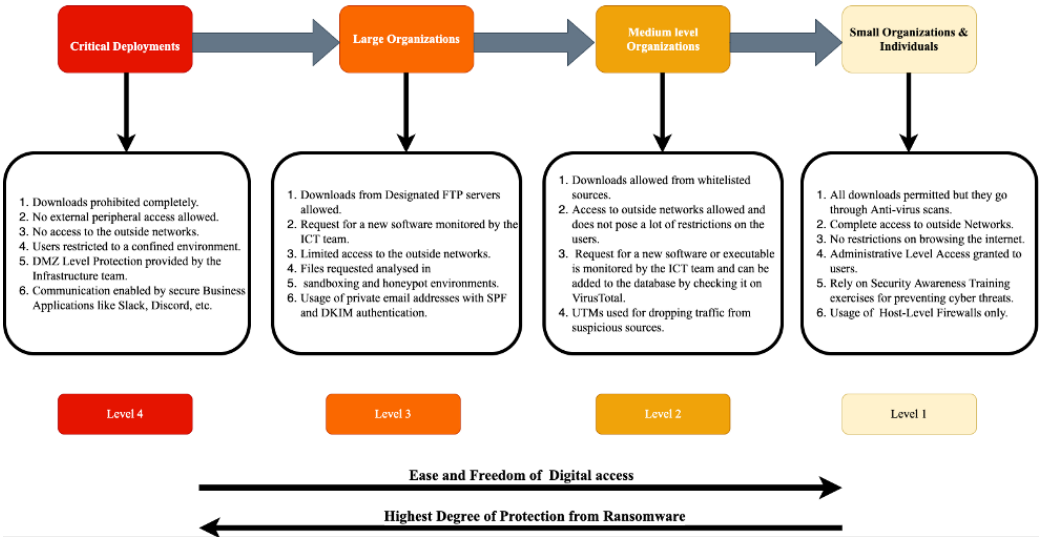

Figure 6. The Ransomware avoidance continuum.

The Level 4 Ransomware Prevention applies to critical infrastructures and restricts their users to a confined or sand-boxed environment. This does not grant the digital freedom to the users but works extremely well in avoiding incidents of Ransomware attacks. Level 3 applies to large organizations. Here users download files (typical open-source software packages) from designated File Transfer Protocol (FTP) servers which are maintained by central Information Technology (IT) teams. All other downloads requested from the open internet first are stored in a sandbox and analyzed both statically and dynamically for detection of malware. Further, software updates can be controlled and distributed by the central IT team and individual users do not have root privileges to make system-level changes. Level 2 applies to mid-sized entities allows users to download files from the open internet but route the traffic through a Unified Threat Management (UTM) device for detecting malware and dropping traffic from suspicious sources. Level 1 applies to small organizations which do not have the necessary IT infrastructure or security policies in place [61]. Here apart from having individual anti-virus software, there is not much by way of security policies. These organizations are the most susceptible to Ransomware attacks and user education and awareness are the most effective strategies for avoiding Ransomware attacks.

Thus, Ransomware avoidance is typically a trade-off between the freedom of digital access and fool-proof security. The more the desired degree of freedom to end users in downloading and installing third-part software applications, the more difficult and complex the task of Ransomware avoidance becomes.

4.3. Ransomware Mitigation Techniques

Ever since the advent of Ransomware, cyber-defenders have been trying to come up with advanced security solutions that would counteract different Ransomware strands. On the other hand, Ransomware designers have exploited new vulnerabilities, preying on lack of cyber-security awareness of a vast majority of the population to wreak havoc. Mitigation of Ransomware attacks involve recovering encrypted data most likely through reverse engineering or not allowing the Ransomware to complete the encryption process. However, in the real-world mitigation techniques have had limited success. A vast majority of individual victims of Ransomware typically end up paying the ransom demand or

losing their data permanently. Still several mitigation techniques that can enable removal of Ransomware and recovery of devices in an efficient manner have been proposed.

Figure 7 sums up the main mitigation methodologies based on the techniques they use.

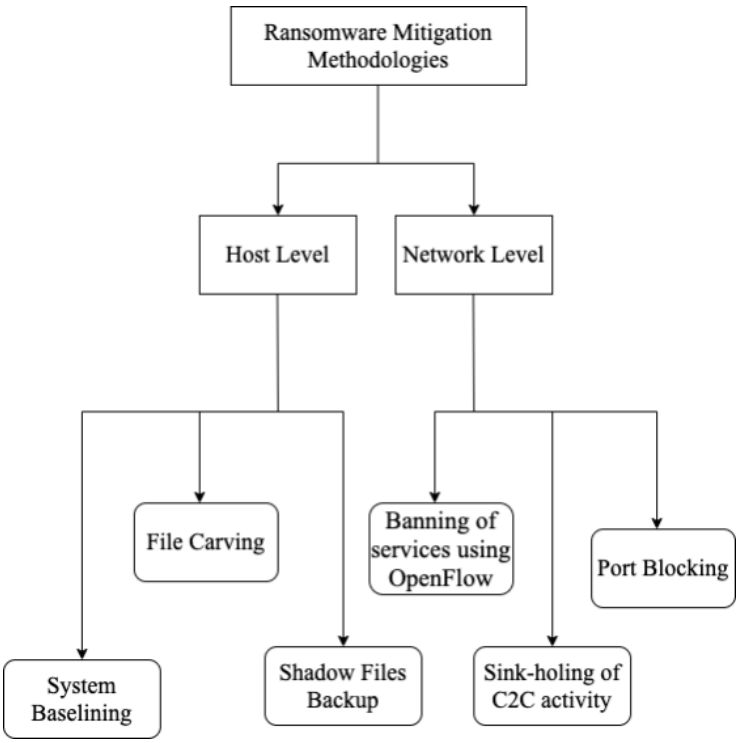

Figure 7. Typical Ransomware mitigation methodologies.

Cabaj et al. [62] devised a mitigation technique that made use of Software defined networking to counteract Ransomware. This method was applied to CryptoWall Ransomware, but was applicable to almost all types of Crypto Ransomware. The technique used dynamic blacklisting of C&C servers when the sample was being run. Without the C&C server, infected machine cannot access the public key that will be used to encrypt it. This technique however could not identify any servers that have not been used previously as C&C servers. The blacklisting technique worked with a list of available proxy servers. The implementation of such a mitigation system was made possible through two SDN based applications, SDN1 and SDN2. SDN1 evaluated DNS responses from the inbound traffic and checked if the domain was already present in the database of illicit proxies. SDN2 enhanced the functionality of SDN1 by reconfiguring the whole network infrastructure to block the Ransomware activity. SDN2 utilized OpenFlow protocol to block the traffic associated with a malicious sample.

Zimba et al. [63] made use of reverse engineering to uncover the actual operation followed by different strands of Ransomware. The authors stated that option for data recovery exists inside the attack structure and the underlying code of the Ransomware, despite how complex the Ransomware looks. The approach followed by them comprised of two modules. The first module used reverse engineering to find out the functions for data deletion and recovery in the source code of the malware. Through the first module, the authors were able to identify various properties of a Ransomware by deploying various scans like Virus scans, obfuscation checks, meta-data extraction etc. The second module used sandboxing for analyzing the behavior of the Ransomware. This module comprised a server-side environment and client-side environment. In the server-side environment, Cuckoo server [64] and Volatility were being run. Cuckoo was responsible for delivering the Ransomware. In the client-side environment, there were various Virtual Machines running Windows 7 Desktop Edition. Through Volatility, Ransomware was being analyzed dynamically. Various behavioral features of the sample were collected through the second

module. The authors then proceeded to discuss the file hiding techniques used by the attackers. They found out that the attackers don't use secure file deletion techniques which make file recovery impossible [65]. Through their experiment, they were able to recover data because of the weak deletion methodologies used by the Ransomware. In the samples analyzed by the authors, almost all of the samples deleted the volume shadow copies; but due to timely offline backup of those copies led them to restore the victim's device. Even in the cases where Ransomware was able to evade sandboxes, the authors were able to restore captive data using the methodology of generation of public key pairs on the victim's device.

Baykara et al. [66] developed an application called Safe Zone in which a single file, kept all the files of a user by compressing them. The file created by the authors was known as safezone.safe and was kept in a non-stop write mode so that no other sources could modify it. The application made use of a logging system called File Watcher that would log all events in the Safe Zone as well as track the modifications made in the parent folders of the files added to the Safe Zone. The application had another feature that would check for integrity in safezone.safe. The application had an interface that even a non-technical user would be able to understand easily. In case of a Ransomware attack, victims can safely go back to the last backup logged in Safe Zone and recover the system to its previous state.

Akbanov et al. [67] made use of Software Defined Networking to mitigate WannaCry Ransomware in a network. The authors deployed two Windows 7 virtual machines along with REMnux to simulate the propagation of WannaCry via EternalBlue exploit in a test bed network. In their experiment, the authors restricted the spread of Ransomware to only one device. Thus, in order to combat the further expansion, they devised a SDN based technique which dynamically inspected DNS traffic for anomalies. Since EternalBlue exploit results from flaws in the SMB server, SMB traffic is also looked into very carefully so as to detect the presence of any botnet activity. Initially, all the malicious traffic is sent to the controller which then parses all the packets and matches the malicious ones against blacklisting database. It then checks for WannaCry indicators like dropper and C2C server file. TCP port 445 is monitored by the controller and as soon as any traffic from this port or TCP port 139 arrives, it is restricted by the controller so that Ransomware cannot propagate further from the infected host. It is however not able to detect the newer versions of WannaCry that use advanced exploits like EternalRomance and EternalIce because of the evasion mechanisms deployed by them.

Sophos developed an endpoint mitigation tool called Intercept X that claims to eliminate Zero-day APT families. Intercept X uses behavioral analysis to prevent Ransomware families from modifying registries. According to Endpoint Security's Testing Guide [68], Intercept X has a success rate of 99.7% in detection and mitigation with just one false alarm in the real world test. Intercept X also deploys exploit prevention techniques that help in finding out extremely advanced adversary shell-coding patterns and blocking them before they are able to gain access into the registry. Along with these features, Intercept X brings a new feature called Crypto Guard that can recover encrypted files. Despite the extremely high efficiency, further research needs to be conducted into how and whether it can detect and mitigate the latest families that deploy anti analysis techniques.

Microsoft released two products called Defender for Endpoint and Defender for Identity for extensive protection against Ransomware attacks. They have been thoroughly tested against the largest malware database in the world, AV-TEST. Both of them scored 100% protection level in the October 2020 test. This test included new 12316 malware samples along with 339 Zero Day strands. However, the rate of introduction of new strains of Ransomware makes it virtually impossible to build fool-proof solutions. McAfee LLC [69] patented a framework that was able to identify if any unauthorized executable was trying to modify the local files on the system and create a security event for the same. The framework used entropy values to distinguish between files and their modified form. Any value above the threshold would denote a security breach and thus, the framework would create a security event accordingly. The security event would then be monitored

and if the entropy value was way too high, then the system would be taken back to the last snapshot in order to mitigate the Ransomware attack. System baselining, checkpointing and rollbacks require significant storage requirements.

Dell EMC [70] invented a framework that replicated all the appends and writes from a server to two different copies, a local and a remote. The local copy resided in a local production site whereas the remote copy was kept in a remote disaster recovery site. A sliding time window was used to measure the deduplication ratio in an arbitrary chosen length of data. If this ratio was on the increasing end of the threshold, the framework claimed to have detected a Ransomware. In order to mitigate the attack, the framework would stop any pending appends and writes designated for the remote site. While such schemes work well for data files, retrieving licensed applications and ensuring complete system recovery has not been attempted by existing mitigation techniques and mechanisms.

While some mitigation strategies have proved effective against existing strains of Ransomware, their effectiveness has been demonstrated in a controlled lab environment. In real-world scenarios Ransomware spreads because of unpredictable human responses and actions and a divergence of security policies, devices and deployments across vendors. This is due to the lack of standardization efforts in devising security mechanisms and large-scale collaborative efforts involving governments, security organizations and researchers.

5. The Notorious Djvu Ransomware: A Case Study

Recently, a lot of individual users have been subjected to one of the most widespread ransomware strands, Djvu. Djvu, alternatively known as STOP, is a huge ransomware family with almost 250 variants, updated on a weekly basis. It was released in the last quarter of 2018 and its initial success led to development of different sub-strands. The widespread nature of Djvu is due to multiple distribution sources. The most common sources include e-mail attachments, cracks and keygens for bootlegged software. Ransomware authors of Djvu place the encryption source code in the crack packages and distribute them via torrent websites.

5.1. The Djvu Modus Operandi

Djvu variants use different encryption techniques. The earlier variants used AES, a symmetric encryption algorithm. Since AES uses a single key for both encryption and decryption, researchers were able to extract the key from victims and were able to contain the virus. Later variants used RSA for encryption. A novel aspect of Djvu's RSA variant is that it encrypts only the initial portion of the files, say 2 to 5 MB of the file, so that file carving would become challenging. Another reason for this approach is that RSA is computationally intensive, thus making it difficult for reverse engineers to create a decryption tool. Djvu details are summarized in Table 5 below:

Table 5. Djvu Ransomware details.

Name	Djvu
Ransomware Type	Crypto Family
File Extensions	.djvu, .kasp, .nopsk, .tfude, etc.
Author Email	helpshadow@india.com, restoredjvu@india.com, helpshadow@firemail.cc
Delivery Method	Email Attachments, Cracks, Keygens, Packaged Software
Decryption	Offline IDs: yes, Online IDs: no
IOC	Changed Checksums, .txt files appearing on the Desktop
Ransom Amount	$800

In the infection phase, once the strand is delivered to the victim's device, the next sub phase is where the encryption file is dropped from the skeleton program. As soon as the

deliverable is executed by the potential victim, Djvu gets activated and starts manipulating various files. Figure 8 depicts the sequence of operations followed by Djvu.

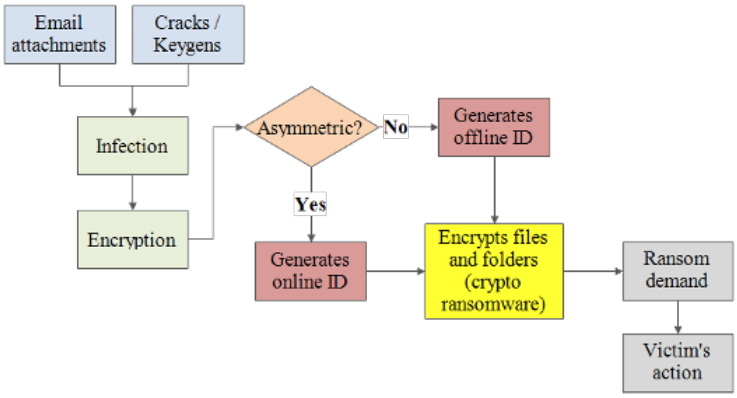

Figure 8. Djvu Ransomware's sequence of operations.

In order to prevent carving attempts, Djvu deletes the OS's shadow volume and renders the important Windows registry entries unusable. Considering the typical encryption scenario, Djvu encrypts the common files and folders, thereby appending extensions like .djvu, .udjvu, .djvur, etc. to them. As soon as the encryption process is complete, which takes around forty-five seconds to one minute after the execution of the deliverable, a ransom note in the form of a .txt file is stored on the desktop and contains a message regarding the encryption of victim's files. The message also contains the email addresses of the Ransomware authors which need to be contacted in order to get the files decrypted. If the victim pays the ransom amount within 72 h of encryption of the files, then the authors promise a 50% discount on the ransom amount. Upon contacting the email addresses provided in the ransom note, a cryptocurrency wallet is provided by the authors where the payment is to be made. As stated in the previous section, the authors can passively watch the blockchain for tracking the payment, this technique promises anonymity to them.

With the previous versions, since AES was being used, a single decryption tool could be created and be replicated to help other victims. It is interesting to note that Djvu strands using AES create victim IDs with t1 appended to the end. These IDs are used for making payments. Thus, for victim IDs ending in t1, it is possible to use decryption tools available on the internet. This is due to lack of any C2C activity in the Ransomware. However, the authors learnt from the drawbacks and started using asymmetric cryptographic techniques along with C2C server activity.

5.2. Tackling Djvu

Currently there are only a few detection strategies that can detect the presence of Djvu. We suggest that reverse engineers can use both static and dynamic analysis techniques. Using static analysis, we can identify the Indicators of Compromise (IOC) parameters like varied checksums and email addresses etc. Along with this, malicious strings if any can be examined. Djvu can also be analyzed using dynamic techniques where, using Wireshark, its network activity or any interactions with a C2C server can be measured. Tools like Process Hacker can give us very important information like the local API calls Djvu will make for DLL hijacking and API hooking. The Ghidra tool [71] can help us reverse engineer a strand as well as enable us to find the language it is written in.

One main reason for Djvu's success is poor Cyber-hygiene practiced by end users. A lot of users still use cracked software to avoid paying for the licenses. Plus, recovery is never guaranteed if you are hit by a Ransomware attack. Since Djvu resides in malicious email attachments as well as cracked software present on Peer-to-Peer (P2P) websites, basic security awareness among users goes a long way in preventing such attacks. An AI-based prevention tool/browser extension that advises/warns users and helps them practice better Cyber-hygiene would be a good start in this direction. A further extension

to the tool can be envisaged to download any file to a sandbox, transfer the downloaded file to industry-standard Ransomware analysis tools like ANY.RUN, get the analysis results and allow or prevent the users from installing the downloaded software.

As discussed in the previous section, most Ransomware attacks are extremely hard to mitigate because of the absence of strand specific solutions. Also, it is hard to decide between network-level or host-level mitigation strategies for effective removal of Ransomware. In case of the earlier versions of Djvu that use Advanced Encryption Standard (AES), host level solutions need to be looked into whereas for RSA based Djvu, network-level strategies come into play. Further, backup and restore options, similar to ones on smartphones, need to be explored for individual systems to truly mitigate the impact of Ransomware. Table 6 presents a summary of potential detect, avoid and mitigate strategies for Djvu.

Table 6. DAM strategies for Djvu Ransomware.

Detect	Avoid	Mitigate
Static Analysis – checksums, emails, APIs, malicious strings	AI-based Cyber-hygiene assistants	System backup and restore
Dynamic Analysis – Ghidra, Wireshark & Process Hacker for reverse engineering, network analysis and API call analysis	Sandboxed downloads - analyze all downloads via ANY.RUN analyzer and then install	Scheduled disk mirroring
Custom Dynamic Analysis – DJVU performance profile tracking and matching	Firewalls and anti-Ransomware software	Decrypting files by reverse engineering the strand (improbable)

6. Future Directions in Ransomware Protection

The DAM framework evaluates different combat strategies for preventing ransomware attacks and widespread financial losses. Out of all the combat strategies, avoidance techniques are the most desirable in protecting users and organizations from ransomware. However, effective avoidance techniques at an organizational level entail significant cost, large IT teams, multiple levels of security and some restricted user access privileges. At the individual level practicing Cyber-hygiene is the only effective avoidance strategy. Since avoidance is the holy grail for ransomware security, detection and mitigation are more viable real-world strategies. Early and fool-proof detection of ransomware attacks is desirable if effective mitigation strategies are to be implemented. Even though, most of the techniques discussed above detect ransomware within a timeframe of 50 to 60 s of their initial spread, advanced strands can perform DLL hijacking and UAC bypassing within five to ten seconds and are able to encrypt the files within fifteen seconds. Once the files are encrypted, it is extremely difficult to reverse engineer the operations performed. Thus, mitigation techniques can be deployed only if detection is extremely fast and that is always a challenge as early inferencing can lead to false positives.

It is safe to say that current technology does not offer an end-to-end security blanket protecting individuals and large organizations from the threat of ransomware. Therefore, organizations need to consistently invest in legal penetration testing services in addition to purchase of cyber insurance policies. The former leads to rigorously testing the defense perimeter and constantly upgrading and tuning the security policies to cater to new security threats. Future directions in the evolution of ransomware protection are outlined below:

6.1. Browsers as the First Line on Defense

Files downloaded from the internet through the Internet Browser are primarily responsible for ransomware infection. Little to no research has been conducted till now to detect ransomware inside the browser or even have the capability to warn the users. Ren et al. [72] designed a three-layer-security solution that in its first stage used a browser extension that could identify malicious websites and also kept track of unauthorized down-

loads that occurred through these websites. A major downside of this extension is that it can only block websites that are already residing in a predefined list. Malvertising is known to occur through trusted websites as well. It utilizes the JavaScript execution capabilities of the browser to trick it to download the malicious file. That is why the browser should be equipped with security features so that as soon as an executable is downloaded, it should be moved into a sandbox so that its behavior can be analyzed. Hence, extensive research needs to be carried out for building ransomware detection and isolation features inside the browser.

6.2. Trusted and Non Trusted Sources

Although this counts as a preventive measure, maintaining a database of trusted and non-trusted sources through a global collaboration/crowdsourcing between credible entities will help in improving alert systems for potentially malicious sites and internet sources. The database can be created by incroporating Qualys' SSL Labs APIs [73] which will ensure the trustworthiness of a website. This database can be similar to the one created by Alexa [74] that ranks websites based on different parameters. Then, this database can be used by web-browsers and anti-malware extensions that will monitor the activities of a user and issue an alert when a potentially dangerous website is browsed.

6.3. Avoiding Privilege Escalation in Windows Based Platforms

Traditionally Windows based devices are the most susceptible to ransomware attacks due to weak authorization and authentication policies which can be abused by malicious users. One of the techniques used by malicious executables to gain unauthorized access into the systems is privilege escalation. DLL Hijacking and bypassing UAC mechanism are the two main ways by which Windows Privilege Escalation is carried out to gain folder and registry access in order to encrypt them.

Despite the existence of avoidance strategies like Controlled Folder Access and cloud powered Windows Defender AV [75], malicious portable executables can use extremely advanced techniques like Anti-Analysis mechanisms, API hooking and Process Injections to infect the system. Also, the concept of secure registry needs to be looked into so as to develop better prevention strategies. The notion of hierarchy-based file-system standard needs to be incorporated into such platforms so that role-based access control and privilege-based access control can be defined and enforced.

6.4. Adoption of AI Based Chat-Bot Assistants for Ensuring Cyber-Hygiene among Users

When it comes to dangerous attacks like Ransomware in cyberspace, prevention is the best cure. Prevention of Ransomware attacks is highly dependent on the behavior of the users on the Internet. This, in turn is governed by Cyber-hygiene practices. In this context, AI-based chat-bot assistants that can warn users against the repercussions of downloading files from untrusted sources can be useful. Such tools will be able to monitor the web activity of the user and help improve their Cyber-hygiene. Educating users and preventing them from performing actions leading to cyber-attacks will probably be one of the most effective avoidance solutions.

6.5. Use of a Sanitized Software Download Service

A repository of sanitized open-source software packages available for download as a service can be designed which users can use to download popular software packages without the fear of malware infection. The repository may employ a list of File Lock PEA trusted keys. For verification purposes, each package can be matched against the stored keys and checksums.

6.6. Backup and Restore

It is very common for mobile devices to be backed up completely and to restore new devices with the data and applications from the backed-up image of the device. We believe

that such a service is viable for individual laptops/desktops as well. Users shall be able to quickly recover their data in case their system is compromised by reformatting the hard disk and performing a restore from the last backup. Microsoft with its large installed base can contemplate offering such a service to users. This backup is different from a data backup on Google Drive for instance as it involves the backup and management of installed and maybe licensed third-party applications as well. In all the operating systems, the backup functionality is present as a recurring process, such as a cronjob in Linux or scheduled task in Windows. All a user has to do is to set up the backup functionality so that it gets automated and occurs in a timely manner. Although the physical operating systems do not have capability of working with snapshots, but the concept of Last Known Good Configurations work here, which help in mitigating the effect of Ransomware.

6.7. CVE Monitoring

Most of the Ransomware attacks are successful because of two major factors, poor Cyber-hygiene and unpatched system vulnerabilities. Ethically, penetration testers try to find out Zero Day vulnerabilities before the malicious actors, and these vulnerabilities are fed into a database of Common Vulnerabilities and Exploits (CVE). But most of these vulnerabilities are not patched by developers thus leading to highly advanced and chained attacks. Thus, a server for latest CVEs can be created which may be used to retrieve real time information regarding patching possible exploits and vulnerabilities.

7. Conclusions

In this article, we presented the DAM framework for analyzing Ransomware combat strategies. Different strategies, their modus-operandi and limitations are also discussed. Ransomware is rapidly increasing in complexity, adversity and multiplicity. Ready-to-go RaaS has even equipped the unskilled attacker in launching effective attacks. Detection and mitigation techniques have not kept pace with the increasing sophistication of the Ransomware and remain both cost and resource intensive making it feasible only for large organizations to adopt them. For small organizations and individuals' simpler interventions like trusted sources for software downloads, sanitized downloads, assistants to improve Cyber-hygiene, automated backup and restore and use of screening services such as ANY.RUN, Cloudflare etc. are the only feasible protection options for now. Future work will focus on creation of an Artificial Intelligence based browser extension that will be used for monitoring Cyber-hygiene of individuals and organizations alike.

Author Contributions: Conceptualization: A.K., A.G. and S.T.; writing—original draft preparation: A.K. and R.G. methodology: R.G. and G.S.; writing—review and editing: A.G., S.T. and I.E.D. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: No data is associated with this manuscript.

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

References

1. Johnson, B. The Growing Menace of Ransomware. Available online: https://alliantnational.com/the-growing-menace-of-ransomware/ (accessed on 26 August 2021).
2. Sophos. The State of Ransomware 2020. Available online: https://www.sophos.com/en-us/medialibrary/Gated-Assets/white-papers/sophos-the-state-of-ransomware-2020-wp.pdf (accessed on 14 December 2020).
3. AH, A.K.; CC, Y.Y.; Ping, M.; Zahra, F. Cybersecurity Issues and Challenges during COVID-19 Pandemic. Available online: https://cyber-trust.eu/2021/01/07/cyber-security-challenges-during-the-covid-19-pandemic/ (accessed on 7 January 2021).
4. Kalaimannan, E.; John, S.; DuBose, T.; Pinto, A. Influences on ransomware's evolution and predictions for the future challenges. *J. Cyber Secur. Technol.* **2016**, *1*, 1–9. [CrossRef]

5. Emm, D. Cracking the code: The history of Gpcode. *Comput. Fraud. Secur.* **2008**, *2008*, 15–17. [CrossRef]
6. Bodkhe, U.; Tanwar, S. Secure data dissemination techniques for IoT applications: Research challenges and opportunities. *Softw. Pract. Exp.* **2021**, *51*, 2469–2491. [CrossRef]
7. Purplesec. The Growing Threat of Ransomware. Available online: https://purplesec.us/resources/cyber-security-statistics/ransomware/ (accessed on 19 December 2020).
8. Braue, D. Global Ransomware Damage Costs Predicted to Exceed 265 Billion by 2031. Available online: https://cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-reach-250-billion-usd-by-2031/ (accessed on 3 June 2021).
9. Maennel, K.; Mäses, S.; Maennel, O. Cyber Hygiene: The Big Picture. In Proceedings of the 23rd Nordic Conference, NordSec 2018, Oslo, Norway, 28–30 November 2018; pp. 291–305. [CrossRef]
10. Tischer, M.; Durumeric, Z.; Foster, S.; Duan, S.; Mori, A.; Bursztein, E.; Bailey, M. Users Really Do Plug in USB Drives They Find. In Proceedings of the 2016 IEEE Symposium on Security and Privacy (SP), San Jose, CA, USA, 23–26 May 2016; pp. 306–319. [CrossRef]
11. Lee, J.K.; Moon, S.Y.; Park, J.H. CloudRPS: A cloud analysis based enhanced ransomware prevention system. *J. Supercomput.* **2017**, *73*, 3065–3084. [CrossRef]
12. Sood, A.K.; Enbody, R.J. Malvertising–exploiting web advertising. *Comput. Fraud. Secur.* **2011**, *2011*, 11–16. [CrossRef]
13. Hernandez-Castro, J.; Cartwright, E.; Stepanova, A. Economic Analysis of Ransomware. *SSRN Electron. J.* **2017**, 1–14. [CrossRef]
14. Mansfield-Devine, S. Ransomware: taking businesses hostage. *Netw. Secur.* **2016**, *2016*, 8–17. [CrossRef]
15. Hathaliya, J.J.; Tanwar, S.; Tyagi, S.; Kumar, N. Securing electronics healthcare records in Healthcare 4.0: A biometric-based approach. *Comput. Electr. Eng.* **2019**, *76*, 398–410. [CrossRef]
16. Salvi, M.H.U.; Kerkar, M.R.V. Ransomware: A cyber extortion. *Asian J. Converg. Technol. (AJCT)* **2016**, *2*, 1–6.
17. Yaqoob, I.; Ahmed, E.; Habib ur Rehman, M.; Ahmed, A.I.A.; Al-Garadi, M.; Imran, M.; Guizani, M. The rise of ransomware and emerging security challenges in the Internet of Things. *Comput. Netw.* **2017**, *129*, 444–458. [CrossRef]
18. Simmons, G.J. Symmetric and asymmetric encryption. *ACM Comput. Surv. (CSUR)* **1979**, *11*, 305–330. [CrossRef]
19. Yassein, M.B.; Aljawarneh, S.; Qawasmeh, E.; Mardini, W.; Khamayseh, Y. Comprehensive study of symmetric key and asymmetric key encryption algorithms. In Proceedings of the 2017 International Conference on Engineering and Technology (ICET), Antalya, Turkey, 21–24 August 2017; pp. 1–7.
20. Bajpai, P.; Sood, A.K.; Enbody, R. A key-management-based taxonomy for ransomware. In Proceedings of the 2018 APWG Symposium on Electronic Crime Research (eCrime), San Diego, CA, USA, 15–17 May 2018; pp. 1–12.
21. Savage, K.; Coogan, P.; Lau, H. *The Evolution of Ransomware*; Symantec: Mountain View, CA, USA, 2015.
22. Labuschagne, W.; Burke, I.; Veerasamy, N.; Eloff, M. Design of cyber security awareness game utilizing a social media framework. In Proceedings of the 2011 Information Security for South Africa, Johannesburg, South Africa, 15–17 August 2011; pp. 1–9.
23. Hampton, N.; Baig, Z.A. Ransomware: Emergence of the Cyber-Extortion Menace. In Proceedings of the 13th Australian Information Security Management Conference, Perth, Australia, 30 November–2 December 2015; pp. 47–56. [CrossRef]
24. Tanwar, S.; Vora, J.; Tyagi, S.; Kumar, N.; Obaidat, M. A systematic review on security issues in vehicular ad hoc network. *Secur. Priv.* **2018**, *1*, 1–26. [CrossRef]
25. Aurangzeb, S.; Aleem, M.; Iqbal, M.A.; Islam, M.A. Ransomware: A survey and trends. *J. Inf. Assur. Secur.* **2017**, *6*, 48–58.
26. Tailor, J.P.; Patel, A.D. A comprehensive survey: Ransomware attacks prevention, monitoring and damage control. *Int. J. Res. Sci. Innov* **2017**, *4*, 116–121.
27. Tandon, A.; Nayyar, A. A comprehensive survey on ransomware attack: A growing havoc cyberthreat. In *Data Management, Analytics and Innovation*; Springer: Singapore , 2019; pp. 403–420.
28. Genç, Z.A.; Lenzini, G.; Ryan, P. The Cipher, the Random and the Ransom: A Survey on Current and Future Ransomware. In *Advances in Cybersecurity*; University of Maribor Press: Maribor, Slovenia, 2017.
29. Oz, H.; Aris, A.; Levi, A.; Uluagac, A.S. A Survey on Ransomware: Evolution, Taxonomy, and Defense Solutions. *arXiv* **2021**, arXiv:2102.06249.
30. Kok, S.; Abdullah, A.; Jhanjhi, N.; Supramaniam, M. Ransomware, threat and detection techniques: A review. *Int. J. Comput. Sci. Netw. Secur.* **2019**, *19*, 136.
31. Subedi, K.P.; Budhathoki, D.R.; Dasgupta, D. Forensic analysis of ransomware families using static and dynamic analysis. In Proceedings of the 2018 IEEE Security and Privacy Workshops (SPW), San Francisco, CA, USA, 24 May 2018; pp. 180–185.
32. Zheng, C.; Dellarocca, N.; Andronio, N.; Zanero, S.; Maggi, F. Greateatlon: Fast, static detection of mobile ransomware. In Proceedings of the International Conference on Security and Privacy in Communication Systems, Guangzhou, China, 10–12 October 2016; Springer: Berlin/Heidelberg, Germany, 2016; pp. 617–636.
33. Andronio, N.; Zanero, S.; Maggi, F. HelDroid: Dissecting and Detecting Mobile Ransomware. In *Research in Attacks, Intrusions, and Defenses*; Bos, H., Monrose, F., Blanc, G., Eds.; Springer International Publishing: Cham, Switzerland, 2015; pp. 382–404.
34. Arzt, S.; Rasthofer, S.; Fritz, C.; Bodden, E.; Bartel, A.; Klein, J.; Le Traon, Y.; Octeau, D.; McDaniel, P. Flowdroid: Precise context, flow, field, object-sensitive and lifecycle-aware taint analysis for android apps. *ACM Sigplan Not.* **2014**, *49*, 259–269. [CrossRef]
35. Hsiao, S.C.; Kao, D.Y. The static analysis of WannaCry ransomware. In Proceedings of the 2018 20th International Conference on Advanced Communication Technology (ICACT), Chuncheon, Korea, 11–14 February 2018; pp. 153–158.
36. Ferguson, J.; Kaminsky, D. *Reverse Engineering Code with IDA Pro*; Syngress: Seattle , WA, USA, 2008.

37. Grossman, N. EternalBlue Everything There Is to Know. In *Check Point Research*; Available online: https://research.checkpoint.com/2017/eternalblue-everything-know/ (accessed on 29 September 2017).
38. Sgandurra, D.; Muñoz-González, L.; Mohsen, R.; Lupu, E.C. Automated dynamic analysis of ransomware: Benefits, limitations and use for detection. *arXiv* **2016**, arXiv:1609.03020.
39. Cover, T.M. *Elements of Information Theory*; John Wiley & Sons: Hoboken, NJ, USA, 1999.
40. Fernandez Maimo, L.; Huertas Celdran, A.; Perales Gomez, A.L.; Garcia Clemente, F.J.; Weimer, J.; Lee, I. Intelligent and dynamic ransomware spread detection and mitigation in integrated clinical environments. *Sensors* **2019**, *19*, 1114. [CrossRef]
41. Kao, D.Y.; Hsiao, S.C. The dynamic analysis of WannaCry ransomware. In Proceedings of the 2018 20th International Conference on Advanced Communication Technology (ICACT), Chuncheon, Korea, 11–14 February 2018; pp. 159–166.
42. Morato, D.; Berrueta, E.; Magaña, E.; Izal, M. Ransomware early detection by the analysis of file sharing traffic. *J. Netw. Comput. Appl.* **2018**, *124*, 14–32. [CrossRef]
43. Johnson, A.; Haddad, R.J. Evading Signature-Based Antivirus Software Using Custom Reverse Shell Exploit. In Proceedings of the SoutheastCon 2021, Atlanta, GA, USA, 10–13 March 2021; pp. 1–6.
44. Chen, Q.; Islam, S.R.; Haswell, H.; Bridges, R.A. Automated ransomware behavior analysis: Pattern extraction and early detection. In Proceedings of the International Conference on Science of Cyber Security,Nanjing, China, 9–11 August 2019; Springer: Berlin/Heidelberg, Germany, 2019; pp. 199–214.
45. Analytica, O. *US Pipeline Hack to Make Ransomware Risks a Priority*; Emerald Expert Briefings: Oxford, UK, 2021 .
46. Imtiaz, S.I.; ur Rehman, S.; Javed, A.R.; Jalil, Z.; Liu, X.; Alnumay, W.S. DeepAMD: Detection and identification of Android malware using high-efficient Deep Artificial Neural Network. *Future Gener. Comput. Syst.* **2021**, *115*, 844–856. [CrossRef]
47. Taheri, L.; Kadir, A.F.A.; Lashkari, A.H. Extensible android malware detection and family classification using network-flows and API-calls. In Proceedings of the 2019 International Carnahan Conference on Security Technology (ICCST), Chennai, India, 1–3 October 2019; pp. 1–8.
48. Giles, J. Scareware: The inside story. *New Sci.* **2010**, *205*, 38–41. [CrossRef]
49. Chien, E. Techniques of adware and spyware. In Proceedings of the Fifteenth Virus Bulletin Conference, Dublin, Ireland, 5–7 October 2005; Volume 47.
50. Kok, S.; Abdullah, A.; Jhanjhi, N. Early detection of crypto-ransomware using pre-encryption detection algorithm. *J. King Saud-Univ.-Comput. Inf. Sci.* **2020**, 1–16, Early Access. [CrossRef]
51. Kumar, P.R.; Ramlie, R.E.B.H. Anatomy of Ransomware: Attack Stages, Patterns and Handling Techniques. In Proceedings of the International Conference on Computational Intelligence in Information System, Bandar Seri Begawan, Brunei Darussalam, 25–27 January 2021; Springer: Berlin/Heidelberg, Germany, 2021; pp. 205–214.
52. Moussaileb, R.; Cuppens, N.; Lanet, J.L.; Le Bouder, H. Ransomware Network Traffic Analysis for Pre-encryption Alert. In Proceedings of the International Symposium on Foundations and Practice of Security, Toulouse, France, 5–7 November 2019; Springer: Berlin/Heidelberg, Germany, 2019; pp. 20–38.
53. Al-rimy, B.A.S.; Maarof, M.A.; Prasetyo, Y.A.; Shaid, S.Z.M.; Ariffin, A.F.M. Zero-day aware decision fusion-based model for crypto-ransomware early detection. *Int. J. Integr. Eng.* **2018**, *10*, 82–88. [CrossRef]
54. Ferrante, A.; Malek, M.; Martinelli, F.; Mercaldo, F.; Milosevic, J. Extinguishing ransomware-a hybrid approach to android ransomware detection. In Proceedings of the International Symposium on Foundations and Practice of Security, Nancy, France, 23–25 October 2017; Springer: Berlin/Heidelberg, Germany, 2017; pp. 242–258.
55. Kara, I.; Aydos, M. Static and dynamic analysis of third generation cerber ransomware. In Proceedings of the 2018 International Congress on Big Data, Deep Learning and Fighting Cyber Terrorism (IBIGDELFT), Ankara, Turkey, 3–4 December 2018; pp. 12–17.
56. Alhawi, O.M.; Baldwin, J.; Dehghantanha, A. Leveraging machine learning techniques for windows ransomware network traffic detection. In *Cyber Threat Intelligence*; Springer: Cham, Switzerland, 2018; pp. 93–106.
57. Chen, Z.G.; Kang, H.S.; Yin, S.N.; Kim, S.R. Automatic ransomware detection and analysis based on dynamic API calls flow graph. In Proceedings of the International Conference on Research in Adaptive and Convergent Systems, Krakow, Poland, 20–23 September 2017; pp. 196–201.
58. Hwang, J.; Kim, J.; Lee, S.; Kim, K. Two-Stage Ransomware Detection Using Dynamic Analysis and Machine Learning Techniques. *Wirel. Pers. Commun.* **2020**, *112*, 2597–2609. [CrossRef]
59. Kharaz, A.; Arshad, S.; Mulliner, C.; Robertson, W.; Kirda, E. {UNVEIL}: A large-scale, automated approach to detecting ransomware. In Proceedings of the 25th {USENIX} Security Symposium ({USENIX} Security 16), Austin, TX, USA, 10–12 August 2016; pp. 757–772.
60. Richardson, R.; North, M.M. Ransomware: Evolution, mitigation and prevention. *Int. Manag. Rev.* **2017**, *13*, 10.
61. Vora, J.; Italiya, P.; Tanwar, S.; Tyagi, S.; Kumar, N.; Obaidat, M.S.; Hsiao, K. Ensuring Privacy and Security in E-Health Records. In Proceedings of the 2018 International Conference on Computer, Information and Telecommunication Systems (CITS), Colmar, France, 11–13 July 2018; pp. 1–5. [CrossRef]
62. Cabaj, K.; Mazurczyk, W. Using software-defined networking for ransomware mitigation: the case of cryptowall. *IEEE Netw.* **2016**, *30*, 14–20. [CrossRef]
63. Zimba, A.; Wang, Z.; Simukonda, L. Towards data resilience: The analytical case of crypto ransomware data recovery techniques. *Int. J. Inf. Technol. Comput. Sci.* **2018**, *10*, 40–51. [CrossRef]

64. Xu, T.; Chen, Y.; Zhao, J.; Fu, X. Cuckoo: towards decentralized, socio-aware online microblogging services and data measurements. In Proceedings of the 2nd ACM International Workshop on Hot Topics in Planet-Scale Measurement, San Francisco, CA, USA, 15 June 2010; pp. 1–6.
65. Hathaliya, J.J.; Tanwar, S. An exhaustive survey on security and privacy issues in Healthcare 4.0. *Comput. Commun.* **2020**, *153*, 311–335. [CrossRef]
66. Baykara, M.; Sekin, B. A novel approach to ransomware: Designing a safe zone system. In Proceedings of the 2018 6th International Symposium on Digital Forensic and Security (ISDFS), Antalya, Turkey, 22–25 March 2018; pp. 1–5.
67. Akbanov, M.; Vassilakis, V.G.; Logothetis, M.D. Ransomware detection and mitigation using software-defined networking: The case of WannaCry. *Comput. Electr. Eng.* **2019**, *76*, 111–121. [CrossRef]
68. Sophos. Endpoint Security Buyers Guide. Available online: https://www.enterpriseav.com/datasheets/endpointbuyersguide.pdf (accessed on 18 June 2021).
69. LLC, McAfee Mitigation of Ransomware. U.S. Patent 20180018458A1, 10 November 2020.
70. EMC, Dell Detecting and Protecting against Ransomware. U.S. Patent 10819738B2, 27 October 2018 .
71. Bhat, O.; Yeprem, Z.; Lingesh, V. CS 6501 Project Report–Hoos' Upto No Good. Available online: https://www.researchgate.net/profile/Omkar-Bhat/publication/333907927_Comparison_of_3_Reverse_Engineering_Tools/links/5d0bf123299bf1547c7154e4/Comparison-of-3-Reverse-Engineering-Tools.pdf (accessed on 18 June 2021).
72. Ren, A.L.Y.; Liang, C.T.; Hyug, I.J.; Broh, S.N.; Jhanjhi, N. A Three-Level Ransomware Detection and Prevention Mechanism. *EAI Endorsed Trans. Energy Web* **2020**, *7*, 1–7. [CrossRef]
73. Simoiu, C.; Nguyen, W.; Durumeric, Z. An Empirical Analysis of HTTPS Configuration Security. *arXiv* **2021**, arXiv:2111.00703.
74. Amazon. Available online: www.alexa.com (accessed on 18 June 2021).
75. Microsoft. Next-Gen Ransomware Protection with Windows 10 Creators Update Ransomware in 2017: Growing in Sophistication and Reach. Available online: https://download.microsoft.com/download/8/A/3/8A3ADCCE-C141-4E31-AB0D-26AA990D70A0/Next_gen_ransomware_protection_with_Windows_10_Creators_Update_EN_US.pdf (accessed on 17 August 2021).