International Journal of Information Management Data Insights 1 (2021) 100013

Contents lists available at ScienceDirect

International Journal of Information Management Data Insights

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

Review

Information security breaches due to ransomware attacks - a systematic literature review

T.R. Reshmi

Society for Electronic Transactions and Security (SETS), Chennai, India

ARTICLE INFO

Keywords:
Malware
Ransomware
Encrypted attacks
Crypto-modules
Crypto-currency

ABSTRACT

Ransomware is the most predominant cyber threat in the digital infrastructure. The attackers launching ransomware attacks use different techniques to hijack the users' or organizations' files and resources to demand ransom in exchange to free the encrypted/captured data or resources. Although there are many malware attacks, ransomware is considered most dangerous as it imposes a high financial burden on the organization. The crypto-currency is an untraceable payment method that the attacker uses to receive ransom from victims to conceal his/her identity and location. This still creates challenges to trace the attacker or attackers' networks. The article uses the systematic literature review (SLR) approach to provide significant study on the ransomware attacks as it is the area that requires top most attention in critical infrastructure. The paper briefs the various types of ransomware, vulnerabilities, attack methodologies, impacts, mitigation and prevention techniques of the attacks. This research study is mainly focused on Windows OS vulnerabilities. These findings in the survey will be highly beneficial to understand the effects of ransomware attacks in critical infrastructure environments and the use of machine learning to detect and prevent these attacks.

1. Introduction

Critical infrastructure has many sectors that have a debilitating effect on the growth of the economy and security of the nation. Critical Infrastructure security and redundancy advances ensure to maintain secure and uninterrupted functioning of physical or virtual assets, systems and networks (Gheorghe et al., 2018). The communication sector among the critical infrastructure has evolved from voice services into a diverse interconnected industry such as transport, health, defense etc. using terrestrial, satellite, and wireless communications. The communication providers depend on each other to carry the traffic without any interruption and also share resources for interoperability. The communication sector has many private owners who are the prime entities responsible to ensure the security and redundancy of the critical infrastructures. As the communications sector is closely linked to other sectors given below, ensuring safety measures to continuously run the critical infrastructure is the need of every organization.

- The energy sector provides power to all cellular towers, government and non-government offices and other critical communication infrastructures and helps in monitoring and controlling the supply of electricity.
- The information technology sector ensures controlled connectivity of physical devices and internet infrastructures. It also aids in delivering and distributing application, critical control systems, physical architecture, and Internet infrastructure.
- The financial service sector ensures secure communications for financial operations and transactions in markets.
- The emergency service sector focuses on disaster recovery and alerting through various communication media.
- The transportation systems sector concentrates on the fuel and arrangements to ensure the continuous run of backups, generators, communicating infrastructures etc.

Malwares otherwise called malicious software are major threat to critical infrastructures (Rieck et al., 2008). These are designed with an intention to cause damage to the victim's computer or networks that provide services. There are many variants in malwares such as virus, ransomware, spyware, etc (Faruki et al., 2014). Ransomware is malware which is proven to cause sophisticated attack vectors with multiple mutations. Ransomware has affected a broad spectrum of industries like transport, telecommunications, financial companies, public law enforcement and health services. Crypto modules embedded in ransomware are used to render user data unavailable or unreachable. Ransomware either encrypts the files or locks the devices and demands the organization to pay ransom to retrieve the access (Hansman & Hunt, 2005). There are different ransomware which exhibit polymorphic and metamorphic behaviors with code obfuscation and make their scanning and identification challenging with the existing tools.

E-mail address: reshmi@setsindia.net

https://doi.org/10.1016/j.jjimei.2021.100013
Received 27 October 2020; Received in revised form 31 March 2021; Accepted 1 April 2021

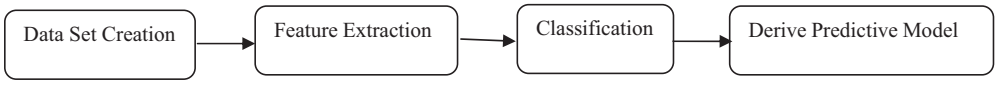


Fig. 1. Training phase of ML assisted malware analysis.

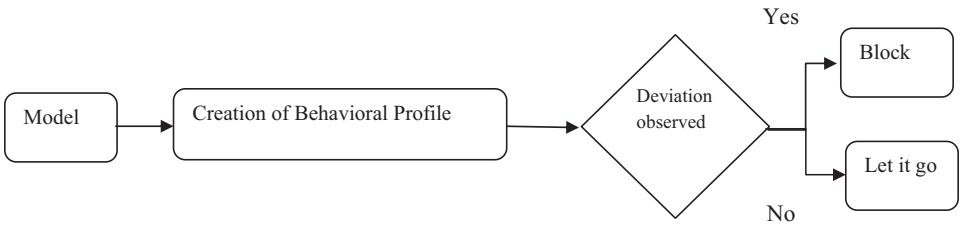


Fig. 2. Testing phase of ML assisted malware analysis.

There are networks hosted by criminals that provide Ransomware-as-a-Service (RaaS) which gives privilege to even amateur attackers to download the ransomware codes and launch attacks. There are also development kits such as Torlocker, TOX etc that are freely available online to develop the ransomware codes and launch attacks. In most of the organizations connected via networks, the business documents and other files are stored in one or more file servers, which are accessible by any geographically placed client ends. So ransomware attacking the mapped network drives causes severe impact on the running business as most of the backups may take time to rebuild. In many cases it may not be file servers, which are always affected by ransomware; it can be compromised ends, which create bypasses to launch remote attacks. Therefore, even if the servers use solutions to prevent attacks, the connected end-points can be vulnerable and cause exploits in the file server.

The ransomware detection solutions are broadly categorized as signatures based or anomaly detection based analysis. The signature based analysis is the de-facto standard way of analysis and detection of ransomware. It works off in an environment of signatures that cover up all known ransomware to detect the threat. The ransomware signatures act like fingerprints that help the solution to identify their presence or threat operations. These solutions hence fail to detect the unknown threat exploits or bugs resulting in zero-day attacks. The anomaly detection based analysis uses different metrics such as network traffic detection, abnormal process calls and other traffic detection for malicious activity identification. But these analyses show high false positives and often legitimate traffic are classified as malicious.

Machine Learning (ML) is gaining popularity in malware detection as it has proven to identify not only existing malwares but also new and obfuscated malwares (Rieck et al., 2011). There are two phases of work in malware analysis using ML (Handa et al., 2019). In the first phase called 'Training Phase', the ML algorithms formalize the set of features extracted from malicious and non-malicious data to build a predictive model. The Fig. 1 shows the phase 1 operation of ML algorithms.

The second phase of ML algorithms is the testing phase, where the predictive model derived from the training phase is used to predict the benign behavior of the malwares. Fig. 2 shows the testing phase in malware analysis. An attacker can manipulate the output of the training phase and the adversarial models using ML are used in many solutions to study this phase effect of classifier manipulation by the attacker in training phase (Chen et al., 2019; Grosse et al., 2017; John & Thomas, 2019).

There are many commercial and open source Anti-ransomware solutions available in the market segmented by deployment, application, location etc. The key vendors of the ransomware protection solutions are McAfeeLLC, AOKasperskyLab, BitdefenderLLC, FireEyeInc, MalwarebytesInc, SentinelOneInc, SophosLtd, SymantecCorporation, TrendMicroIncorporated, ZscalerInc etc. The sandboxes and software libraries like Cryptosearcher, CryptoHunt, etc. perform the crypto module search and analysis to identify ransomware. Even though there are continuous improvements or updates in the existing Anti-ransomware solutions, it is evidently proved that the new variants of ransomware are not identified by the existing solution and the impacts come to light only after the attack. Analyses also show that no variant of ransomware remains unchanged after each infection and this makes ransomware authors to stay one step ahead since the signatures, domains, or IP addresses associated with the ransomware become obsolete and cannot be identified using signature-based security solutions and threat intelligence solutions. The need of a new paradigm to identify the new and evolved ransomware is very important in the critical infrastructure domains. These ransomware attacks can impose high loss and financial burdens imposing the mandatory requirement for the cyber-insurances to all organizations. The key objectives of this study are as follows:

- To understand the trends within the nomological network on information security exploits surrounding ransomware.
- To understand the different characteristics of ransomware which impact information security in operating systems.
- To understand the different variants of ransomware which impact information security in operating systems.
- To understand detection, prevention and mitigation techniques for ransomware

The article is organized as follows: Section 2 discusses the research methodology adopted in the articles with the driven research questions and also discusses the methods adopted to find available resources such as research papers, search criteria, the source of information and quality assessment. Section 3 describes the techniques surveyed in the review and discusses the findings in detail. Section 4 presents the synthesis of the findings discussed in the previous section. Section 5 presents the discussion of the literature review with a focus on state-of-the-art in machine learning techniques. Section 6 briefs the conclusions derived in the systematic literature review.

2. Research methodology

The guidelines followed in various fields presented in the articles (Brereton et al., 2007; Kumar et al., 2021; Verma et al., 2021) are used to undertake a methodical survey focused on research related to ransomware attacks on critical infrastructures. The review, investigation and exploring methods are formulated as per the guidelines formulated. This section discusses the source of information used for research, selection criteria of articles, the methodology for quality assessment and result evaluation. This article is a synthesis of academic and trade literature and tries to articulate the research questions given below.

- RQ1: What are the most common information security exploits by ransomwares?
- RQ2: How can the behavioral profile of ransomwares be developed during operating system attacks using ML methods?
- RQ3: What are the challenges in detection, mitigation and prevention of ransomwares in operating systems?
- RQ4: How can ML be an effective method for diagnosing ransomware attacks and protection of operating systems?

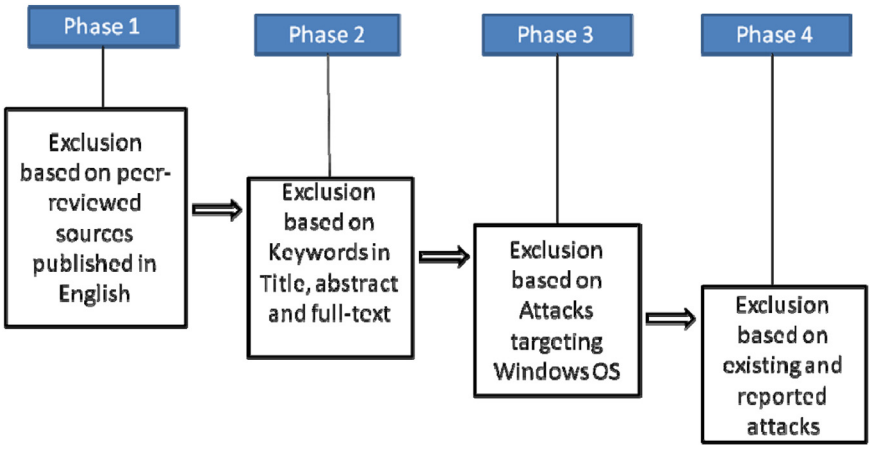


Fig. 3. Inclusion and exclusion criteria for the literature search.

2.1. Source of information

The systematic literature review requires good reference papers keeping the research questions in mind, transparency in steps used for virus review and analysis of the findings obtained. The relevant articles for review is selected by minimizing the selection criteria used in systematic literature reviews. The search for articles was categorized as journals, pre-print and conference articles from various sources. The following databases have been used in the article searches:

- Scopus: (http://www.scopus.com)
- Google Scholar (https://scholar.google.co.in)
- ScienceDirect (http://www.sciencedirect.com)
- Springer (http://www.springer.com)
- IEEE Xplore (http://ieeexplore.ieee.org)
- Arxiv (https://arxiv.org/)
- ACM Digital Library (http://dl.acm.org/)

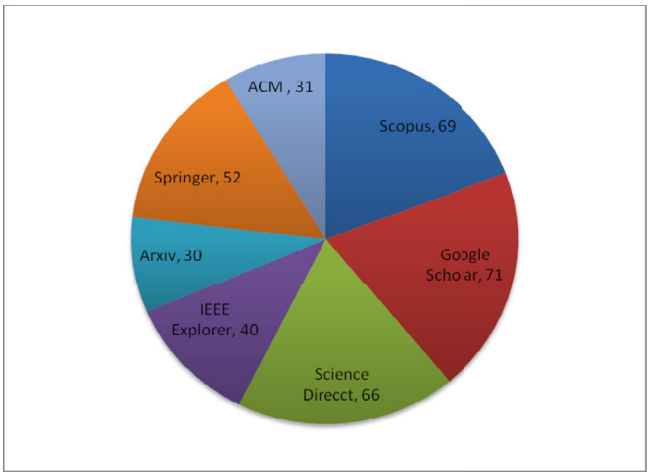
2.2. Search criteria

The keywords are used for the search in the databases mentioned above as per the search strategy suggested by (Grover et al., 2018). The keywords “Ransomware”, “Malware”, “ML+cyber” and “crypto-modules” were used in the abstract of every search. The synonyms of the keywords and other related keywords such as “Remote Access Trojans”, “Bitcoins”, “Command and Control servers (C&C)”, etc. were also used in the searches. The query was refined again to match the results and applied on titles and abstract of the paper. The study was conducted on articles published in the last 12 years. All the procedures were ensured to meet the Quality Assessment Check-list (QAC) published (Kitchenham, 2004) for peer review of journals, books, conferences, white papers and websites.

2.3. Inclusion and exclusion criteria

The inclusion and exclusion criteria for the article selection avoided the biases of any kind and focused on the subject matter. The various principles in the selection are stated below and shown in Fig. 3.

- *Inclusions* - Study focusing on ransomware activities, attacks, defence and detection mechanism in Windows OS, information published in peer reviewed and published in reputable journals or conference papers listed in the above given databases and published in English language.
- *Exclusions* – Study on the new evolving variants of ransomware and vulnerabilities in other operating systems and mobiles, information published in news and magazine publications and articles not written in English language.



Sources	2010-2015	2016	2017	2018	2019	2020
Scopus	8	9	10	12	13	17
Google Scholar	8	9	11	10	15	18
Science Direct	6	11	12	10	15	12
IEEE Xplorer	3	5	7	4	10	11
Arxiv	2	3	4	6	7	8
Springer	4	7	7	9	11	14
ACM	3	5	6	8	6	3

Fig. 4. Sources of ransomware research papers.

3. Findings

The section is an overview of the core concepts of the technical discussions from the sources of information and explores the limitations in the existing solutions. From the trend of the research publication in academic and trade literature, it is observed that the articles published on this specific topic have increased in the last four years. There had been a peak in the articles published in this subject towards the end of 2019 to the mid-2020. The related articles published in various databases and used to extract core concepts are given in Fig. 4.

3.1. Characteristics of ransomware

The behavior analysis of malwares confirms that ransomware performs actions differently from other malwares. The five common steps of actions during a ransomware attack are diagrammatically represented in Fig. 5.

Fig. 5. Operational steps of ransomware attacks.

The various infection vectors used for ransomware attack are malicious advertisements, compromised sites, spamming, social engineering, drive-by-downloads, etc. (Dargahi et al., 2019; Javaheri et al., 2018). The infection happens either in locally or remotely stored files or in memory. The newly identified ransomware go file-less (Anon 2021; Kumar, 2020) and do memory infections which are unidentifiable by static or dynamic malware analysis. The key used by the ransomware may be stored locally or retrieved from the C&C server. The C&C server will be conFig.d using IP address or static/dynamic Domain Name System (DNS). If the symmetric encryption is used by the attacker, the key may be locally stored and may not contact an external server. In case of asymmetric keys used, the local machine may have a public key and have to contact the server for the private key. It is commonly seen that the ransomware encrypts only a few bytes of files during infection as it doesn't want to get quickly noticed. In many cases the file extensions are changed in the final stages of infection. Finally to reveal itself the ransomware keeps notes to convey the action to be taken by the victim to retrieve the data or resources back. The commonly seen techniques to keep notes are creation of image, text or HTML files. Sometimes system calls are triggered to change desktop background or deny access to login to computer.

The analyses on the trends of ransomware attacks show that most of the compromised personal computers were using Windows Operating System (OS). Even though the impact of ransomware attacks are very similar in IoT devices, mobile devices and personal computers, the paper focuses only on the ransomware families that target critical infrastructure devices running Windows OS. Antivirus engines currently in the market identify and categorize the malware as ransomware if it does one or more of the following operations: encrypt the files, change the Master Boot Record (MBR), delete files, steal information and escalate privilege (Nadir & Bakhshi, 2018). The ransomware inspects the pattern of file access and system operations on the files. Based on the analyzed access pattern the attack action happens. The number of files accessed by ransomware will be relatively very high when you compare with the normal system operations. The ransomware accesses the Metadata of the file from MBR and new values are inserted to deny access or delete the files. The canary files are used by Anti-ransomware software to monitor the file activities in directories or folders. So many ransomware tries to delete these canary files to avoid getting noticed. The network activities of infected devices are even monitored by some variants of ransomware and steal the access information. These malicious software are even capable of accessing network servers by cracking the access limitations and encrypt or delete files or backups.

3.2. Variants of ransomware

The Ransomware variants are classified as Crypto and Locker ransomware. The Crypto ransomware uses a crypto algorithm to encrypt all the user data files and demand ransom to share the key for decryption. The Locker ransomware uses privilege escalation technique through various management applications and restricts the access of resources to the users. The persistence techniques are adopted by the Locker ransomware to ensure the resources are locked even after reboot.

The PC Cyborg, is believed to be the first ransomware that appeared in December 1989. It used initialization vector (IV) and a symmetric key to encrypt the files. In 2004, the Locker ransomware (e.g., SMS, Fake FBI) and fake antivirus ransomware Spysherrif, Performance Optimizer etc. emerged. Later the cyber-world has seen many variant forms of ransomware which caused serious business loss or interruptions (Herrera Silva et al., 2019). The Cryptolocker, Cryptowall, Filecoder, GPCode etc. are some ransomware variants which encrypt the file or data stored in the compromised computer. The Cryptolocker and Cryptowall use the Cryptography Next Generation (CNG) cryptography library of Windows OS to encrypt the files. The RSA keys are used to encrypt the files and are retrieved from the C&C server. These malware initially targeted the logical drives introduced in the system and then the evolved variants encrypted the connected drives too. The later versions encrypted all non-system files including network shares to avoid the file retrievals without paying the ransom. The malware used functions such as GetLogicalDrives, GetDriveType, etc. to find network drives and retrieve the information to launch attacks (Keshavarzi & Hamid, 2020). After encrypting the files during ransomware attack, in many cases a private key will be used for decryption. This data of private key for decryption called key blob is stored as a separate file or appended or prepended in existing files depending on the ransomware family.

The Filecoder gets the raw access of files such as volume, cluster information using the Defragmentation API, and overwrites the files. This malware checks the multiple extends of the file and retrieves the file map using the DeviceIoControl from kernel32.dll (Kharraz et al., 2015). It triggers New Technology File System (NTFS) to check the Master File Table (MFT) file records and finds the VCN-to-LCN mapping information of the file records. Initially GPCode used a simple symmetric key and hence the encryption key was easily retrieved by checking the memory. There are records that the later variants of GPCode used AES-256, RSA-1024 and bigger asymmetric keys for encryptions. The Gpcode and Filecoder families use the IRP MJ DIRECTORY CONTROL function to retrieve the list of files and use Win32 CreateFile to open the files. The IRP MJ CREATE (Herrera Silva et al., 2019) function triggered on each create will return a handle to the file objects. Hence, when the file is closed, IRP MJ SET INFORMATION can delete it.

The Seftad ransomware (Anon 2020a) attacks the MBR and replaces it with illegitimate MBR. This displays the ransom payment message thereby preventing the compromised system from loading the boot code in the active partition. These attacks can be revoked by retrieving the unlock code which is hard-coded into the library by reverse engineering. The ransomware variants such as Urausy, Reveton, Winlock, etc. establish a persistent desktop lock procedure during attacks. The malware activates the new desktop by using the access mode that enables SwitchDesktop function and receives inputs from the user end. Few variants also use another approach to lock the desktop and displays a lock banner which is a downloaded HTML page containing the warning message and geo-location with hidden controls. During the locking procedure, the malware also disables all the special keys and keyboard shortcuts by installing the hook procedure that monitors the input events.

The NEMTY provided Ransomware-as-a-service and introduced NEPHILIM/NEPHYLIM ransomware distributed through exposed Remote Desktop Protocol (RDP) (O'Meara & Parisi, 2020). This ransomware managed to communicate payment information through email communication. The other variants of RDP infected ransomware such as Crysis, and SAMSAM are also very infamous variants (Anon 2020b). The ransomwares such as Alphacrypt, Jigsaw, Locky, BadRabbit, Cerber, Chimera, Petya, CryptorBit, Nemucod, CryptoDefense, NotPetya, CryptoLocker, CryptoWall, SamSam, TeslaCrypt, Torrentlocker, Gerber, VaultCrypt, WannaCry, and NEFILIM use AES-128 encryption for encrypting files in compromised computer. This AES encryption key is then encrypted using an RSA-2048 embedded in the ransomware. The ransomware during the encryption also adds the string "NEFILIM" as a file marker to all encrypted files. The filenames of the encrypted files will

have the extension .NEFILIM appended to their names. It is therefore very challenging to retrieve the locked key in these attacks as it needs the RSA private key to start with the decryption.

The exploit developed by U.S. National Security Agency (NSA) called "EternalBlue" was used in WannaCry ransomware attack in 2017 (Kao & Hsiao, 2018). The attacker also used a privilege escalation, DoublePulsar code injection technique and installed the malware with the highest privileges on an endpoint. Some ransomwares like Dharma and BitPaymer use user access control bypass exploits that set the path in a specific registry giving highest privilege to the ransomware.

The Sodinokibi ransomware uses CVE-2018-8453, a Win32k Elevation of Privilege (EoP) use-after-free vulnerability to launch attacks (Loman, 2019). Using this exploit the malware runs arbitrary code in kernel mode and gains access to view, change and delete data; moreover, it can create new accounts with high privileges too. Once a system is compromised, the attacker might use penetration-testing tools to access other security flaws. For example, TASKKILL.EXE is used to terminate processes of security solutions. The ProcessHacker tool hacks the machine and gains complete access. Similarly, tools like CobaltStrike, Meterpreter, or PowerShell Empire, which are used for remote access, can be used to launch attacks by privilege escalations.

There are ransomware variants that run the malicious tasks quickly and cause maximum impacts before being discovered. The multithreaded modern CPUs are effectively utilized by the ransomwares in these variants. The Sodinokibi is one such ransomware. Similarly, LockerGoga and MegaCortex ransomware using sub-processes accelerate documents processing in sets and prevent their detection.

Some ransomware like WannaCry, GandCrab and BitPaymer call the functions FlushFileBuffers and WriteThrough to make the encrypted documents persist in the storage drive and hold for ransom (Kharraz & Kirda, 2017). It is noted that Wannacry Ransomware mainly targets Windows 7 machines to launch attacks. It uses a single thread process and escalates the privilege on each document. It creates encrypted copies of all documents and moves it to %temp% folder with new filename and extension. Then using TASKDL.EXE and VSSADMIN.EXE scrambles the original files and volume shadow copies. Finally change the desktop wallpaper to alert the victim regarding the attack. The GandCrab and Sodinokibi ransomwares exploit Windows POWERSHELL.EXE and triggers to automatically run the ransomware after several days without letting the victim be notified till the attack is hosted. Similarly, ransomware like Ryuk exploit the trusted running process like SVCHOST.EXE by injecting malicious code and the MegaCortex ransomware encrypt documents from a trusted process using the Windows RUNDLL32.EXE application. The BitPaymer ransomware runs from a NTFS Alternate Data Stream (ADS) and thereby hides without getting notified. Few famous ransomware that exploit vulnerabilities in Windows OS, encryption type, infecting methodology and identified year are listed in Table 1.

3.3. Detection, prevention and mitigation techniques for ransomware attacks

There were many solutions put forward to analyse and dynamically react to the detected anomalies that shield the users and organizations from being the victim to ransomware attacks. The cryptographic algorithm used in each ransomware is different and it would be highly beneficial to look into the executables and locate these crypto modules. There are several techniques used to analyze and identify the cryptographic modules. To broadly classify the two methods for the analysis and detection are: Static and Dynamic analysis.

1 Static analysis is used to detect the crypto-binary functions prior to their execution. It also performs heuristic analysis such as presence of loops, entropy, high ratio of bitwise operations etc. These techniques exploit crypto constants for analysis and data flow graphs to aid in detection of signatures.

2 Dynamic analysis tries to learn the crypto algorithms during runtime. The avalanche effect of input on output is one way of study to understand the perturbation built. Assessing the aggregation of contiguous memory accesses form input and output parameters is another methodology used in this analysis.

There are many commercial and open sources available in the market for ransomware analysis, detection and attack recovery. These solutions use the approach that exploits features of ransomware interaction from the logs of network communication, system states and I/O exchanges. Many of these tools are proven to perform well in detecting and preventing many of the existing ransomware.

The decoy files that misdirect the target files of the attacker is a primitive method used to prevent ransomware attacks (Genç et al., 2019). But the new variants of ransomware have techniques to differentiate original and decoy files with an entropy calculation. Shannon's entropy calculation using the formula given below says the entropy value of range 1 to 8 shows the distribution of bytes across the file. The entropy value predicts the next character in the file based on the previous character. So the normal files have low entropy values compared to compressed or generated files. To calculate the entropy of a file, the frequency of all ASCII (0-127) and extended ASCII characters (128-255) in a file is counted and use the probability in the Shananon's entropy formula. So creating decoy files that closely resemble the original files is required to implement this approach.

The ransomware also checks the commonly used filename extensions to launch attacks. Some ransomware looks for a specific local file and if not found will exit without encrypting the files. For example with use of extension-less files called perf or perf.dat (Fayi, 2018) in c:\windows prevent Petya/NotPetya ransomware attacks. The Windows 10 Controlled Folder Access (CFA) white-listing is one method with which ransomware attacks can be prevented. CFA allows only trusted applications to access documents and files in a specific location. But proper and active maintenance is most needed to ensure the working of CFA as per the required policies.

There are approaches to hook the System Service Descriptor Table (SSDT) *i.e.* the internal dispatch table within Microsoft Windows to monitor function calls and get hints of the malicious activities of ransomware attacks (Sihwail et al., 2018). The SSDT table holds the pointer to the kernel functions that are revoked by system calls either with a "int $0 \times 2e$" or with sysenter instruction (used in latest Windows Versions). The register eax stores a value that is a system call number, which will be invoked by the kernel. The ntdll.dll library calls sysenter and it calls another system call number that is eax register value. The eax register of 32 bits has only 12-bits used as an index in the table. The 18-upper bits are unused and middle 2 bits are used to select appropriate service descriptor tables. So a maximum of 4 System Descriptor tables (SDT) with the 2 bit combination can be used. Of these only 2 are used in Windows OS called KeServiceDescriptorTable and KeServiceDescriptorTableShadow, of which the first one is exported by the ntoskrnl.exe and the second one is not exported. Both these tables have System Service Table (SST) structure with fields such as ServiceTable, CounterTable, ServiceLimit and Argument Table. The KeServiceDescriptorTable points to one SST that further points to the SSDT table. KeServiceDescriptorTableShadow points to two SST where the one points to the same SSDT and the second points to the secondary SSDT table. There are commands like dps, which can completely list or even change the entries in the SSDT table. There are also options to dump the complete entries in the SSDT table. If the pointers in the SSDT table can be changed to hook into the kernel routine stored there. Hence, during ransomware attacks the SSDT entries move to the protected mode and hooks to any kernel routines can be reverted back.

The significant number of status changes occurring in a very short period in MFT entries of the deleted files and insertion of a large number of MFT entries with encrypted content in the $DATA attribute of files created with unshared different paths occurs during ransomware

Table 1
Ransomware variants exploiting Window OS.

Campaign	Ransomware	Encryption	Infecting method	Identified Year
Social Engineering	CryptoLocker	Symmetric, AES encryption	Spam/Corrupted webpages	2013
	CryptoDefense	Asymmetric	Spam/Phishing	2014
	CryptoWall	Asymmetric, RSA-2048 bits	Spam/Malicious ads/Malicious sites	2014
	TeslaCrypt	Symmetric, AES 256-CBC	Spam/Phishing	2015
	CTBLocker	Symmetric, AES encryption	Spam	2015
	CryptVault	Asymmetric, GnuPG	Spam	2015
	ToX	Symmetric, AES encryption	Spam	2015
	TorrentLocker	Symmetric, AES encryption	Spam	2015
	Xorist	Symmetric, TEA cipher	Spam	2016
	Jigsaw	Symmetric, AES encryption	Spam	2016
	Chimera	Symmetric, AES encryption	Phishing	2015
	Locky	Symmetric, AES encryption	Spam	2016
	CryptXXX	Symmetric, AES encryption	Spam	2016
	Raa	Symmetric, AES encryption	Spam	2016
	Fsociety	Symmetric, AES encryption	Spam/Malicious sites	2016
	KillDisk	Symmetric, AES encryption	Spam	2016
	Anubis	Symmetric, AES encryption	Spam	2016
	Matrix	Symmetric, AES encryption	Spam	2016
	Locky	Symmetric, AES encryption	Spam	2017
	Satan	Symmetric, AES encryption	Worm	2017
	CryptoShadow	Symmetric, AES encryption	Spam	2017
	Sage	Symmetric, AES encryption	Spam	2017
	Scarab	Symmetric, AES-CBC	Spam	2018
	Retwyware	Symmetric, AES encryption	Spam	2018
	Egregor	Asymmetric, RSA encryption	Spam	2020
Vulnerable Software/Servers	Revenge	Symmetric, AES encryption	Compromised sites	2017
	SamSam	Asymmetric, RSA-2048 bits	Vulnerable Servers	2016
	Petya	Symmetric, AES encryption	Fake Software/Worm	2016
	Cerber	Symmetric, AES encryption	Fake Software	2016
	Enigma	Symmetric, AES encryption	HTML attachments	2016
	Bart	Symmetric, AES encryption	HTML attachments	2016
	Patcher	Symmetric, AES encryption	Fake Applications	2017
	BTCWare	Symmetric, RC4 encryption	RDP	2017
	WannaLocker	Symmetric, AES encryption	Fake game plugins	2017
	DMALocker	Symmetric, AES encryption	Compromised Sites	2015
	NotPetya	Symmetric, AES encryption	Worm	2017
	CryptoSheild	Symmetric, AES encryption	Compromised sites	2017
	GlobeImposter	Asymmetric, RSA-2048 bits	Compromised sites/software	2017
	BadRabbit	Symmetric, AES encryption	Compromised sites	2017
	WannaCry	Symmetric, AES encryption	Worm	2017
	Virlock	Asymmetric, RSA-2048 bits	Encrypted files	2014
	Hermes2.1	Symmetric, AES encryption	GreenFlash Sundown Flash Player	2018
	Ryuk	Symmetric, AES encryption	Directed attacks	2018
	GandCrab	Symmetric, AES encryption	Fake software crack sites	2018
	Katyusha	Asymmetric, RSA-2048 bits	Worm	2018
	LockerGoga	Symmetric, AES encryption	Worm	2019

attacks. So the changes in the MFT table during file creation, encryption or deletion of files can be closely monitored to identify the ransomware. Similarly, if the solution can monitor all I/O requests that user-mode processes generate to access file systems and discard the suspicious requests before they reach the file system driver could beneficially prevent ransomware attacks. Recovering of the deleted files from the ransomware attacks is possible in some cases using recovery tools like *Recuva* (Kamble et al., 2015). Based on the $DATA attribute, the resident or non-resident file needs to be copied. If it is resident, simple copying of content to another location is done otherwise the RunList in the MFT is parsed and raw data is copied to another location. Since the files deleted during ransomware attacks are considered as unallocated clusters, it can be allocated with new files and recovery of old files is not possible. To complicate the recovery process, the Dharma ransomware sets the file size to 0 bytes before deletion leaving zero chances for recovery. Therefore, an early detection of the ransomware attack is very much important for recovery.

Even though the existing solutions use different techniques as listed in the table 2 given below, one of the shortcomings described in most of the techniques is the inability to detect and prevent new attacks. The table 2 highlights the techniques used by the solutions and the problem addressed with limitations.

3.3.1. *Machine learning based ransomware detection solutions*

The ransomware authors are hosting new attacks by evolving or obfuscating the existing ransomware strains, so it is the need of the hour to come up with solutions that can detect both existing and new attacks. There are many machine designs to dynamically detect the ransomware using ML algorithms and the discussion of the same is covered in detail in the coming subsection.

Many of the ransomware detection solutions using ML techniques use supervised learning techniques and hence need a training phase. These proposals are based on the different sets of statistics extracted from the ransomware actions. However there are few proposals that use unsupervised algorithms too. In most of the cases, ML techniques are used to detect zero day attacks with generalized models and compact feature sets. The dynamic trace of the variable length data flow is used by machine learning techniques to classify crypto modules. The algorithms like Support Vector Machines (SVM), Naive Bayes, Decision-Tree, K-Means Clustering etc. are used for this purpose.

A Windows kernel developed by Continella et al. (Continella et al., 2016) monitors the file system operations such as listing, read, rename, write and entropy. The common patterns of access data for genuine applications are studied and sample applications with ransomware activities in a controlled environment are used to train the model. Data of

Table 2
Ransomware detection and prevention solutions.

Sl No.	Solution	Technique	Problem Addressed	Limitation
1	Cryptodrop (Alzahrani et al., 2017)	Indicator Score Board, Union Indicator, Shannon Entropy	Malicious files are observed	Recognises benign activities and not specifically ransomware
2	2entFOX (Ahmadian & Shahriari, 2016)	Bayesian Network-based Analysis	Detection of highly survivable ransomware and prevention of backup intrusions or access	Low survivable ransomwares are not accounted
3	File FingerPrinting Technique (FFT) (Boukhtouta et al., 2016)	Process monitoring, File system and registry activity monitoring, Access Request monitoring	Analysis of Ransomware activities during attacks	No prevention method discussed
4	LAMP and WAMP Server (Yslas, 2021)	Behavior analysis in Virtual environments	Signature based recommendations	New attacks are not accounted
5	SdGuard (Hong et al., 2017)	Stack Activity Analyzer, I/O log Analyzer	Regulate access rules and avoid ransomware attacks on external devices	Attacks on Internal storage is not addressed
6	UNVEIL (Kirda, 2017)	Behavior analysis in Virtual environments, Semantic Characterizations, Honeyword analysis	Tamper attacks of any Locker ransomware	Detection of Crypto-ransomware is impossible
7	Redemption (Kharraz & Kirda, 2017)	Redemption defense system on OS I/O storage ports, Structural Similarity (SSIM) index method	End-point security solution that differentiates ransomware and benign activities	Detection of Locker-ransomware is impossible
8	SDN (Cabaj et al., 2018)	HTTP message analysis, Message sequence and content size analysis	Early warning detection system using Openflow Switches and NOX controller	Detection of few variants using static taint analysis
9	EFCM (Al-rimy et al., 2017)	C&C Communication monitoring, String analysis, Data centric detection	Prevention of ransomware attacks using static data centric feature	New variant ransomware cannot be detected
10	ZELTZERS (ZeJtzer, 2015)	Renaming the system tool, Backup recovery	Cloud based preventive maintenance against four common ransomware variants	Protection against only few variants
11	Honeypot (Moore, 2016)	Honeypots and IDS to screen network logs	Automated tool to detect both active and passive malware in android environment	The dynamism exhibited by new ransomware can bypass the tool
12	SheildFS (Continella et al., 2016)	Add-on self-healing hard-on driver for Windows OS	An immune system add-on to the Windows that can roll back suspicious events	The threshold level set out for encryption notification creates bypass to most of the ransomware variants
13	PRPB (Patyal et al., 2017)	Process monitoring, Backup and recovery layers	Multi-layered approach to backup and recovery attacks	Not dynamic to overcome new attacks
14	PAYBREAK (Kolodenker et al., 2017)	Session Hybrid Encryption Key (HEK), escrow mechanism for recovery	Proactive defense mechanism to secure system files	Signature based solution that cannot detect new variants
15	EXPMONITOR (Kiraz et al., 2017)	Public Key cryptosystem analysis and detection	Defense mechanism that uses AES encryption schemes	The ransomware running symmetric key cryptography cannot be detected

different scales are used to study the short term and long term behavioral patterns. The model used a random forest supervised learning algorithm which was able to detect many of the existing ransomware. The proposal based on supervised regularized logistic regression algorithm was put forward by EldeRan (Sgandurra et al., 2016) which used large feature sets obtained from static and dynamic analysis. The training phase is done offline by monitoring the executable in the sandbox environment. The features used are extracted from API calls, registry key usage, new or intermediate files created, file system operations, specific strings in the binary. A SVM classifier was proposed by Hasan and Rahman (Hasan & Rahman, 2017) which used features extracted from the mutual information criterion extracted from static and dynamic analysis.

Chen et al. (Chen et al., 2017) obtained 70,000 features from the API calls used by malicious software or processes. The applied correlation technique is used to reduce the dimensionality using the results obtained using Random Forest, SVM, Simple Logistic algorithm and the Naïve Bayes. Similarly the solution from Ahmadian and Shahriari (Ahmadian & Shahriari, 2016) used features from cryptographic API calls that modified Windows Registry and created the Bayesian network. There were many proposals inspired by the biological immune system behaviors. One among these solutions was the proposal from Wu et al. (Wu et al., 2014) on a negative selection algorithm where V-detector was used for the classification. The features extracted from API functions, network operations or memory patterns of the ransomware process were analyzed using bio-inspired supervised learning algorithms (Ab Razak et al., 2018). The solution used a low variance filter to eliminate features with values below a threshold.

The proposal put forward by Venkatraman et al. (Venkatraman et al., 2019) considered only the API call from processes and their frequencies as the only feature by the classifier which created images for comparisons. The SVM classifier and multi-layer perceptron were both trained for this purpose. Similarly the set of domain names is used as the only input feature used in the solution proposed by Chadha and Kumar (Chadha & Kumar, 2017). These domain names are generated using the Domain Generation Algorithm which is extracted from the ransom note displayed by various families of ransomware. The authors also did a comparative study based on the classification results obtained from several supervised and unsupervised algorithms.

The modern processors have special registers that account various machine-level operations. The high-encryption operation is one among such machine-level operations in the CPU and this observation is used as the criteria for the ransomware detection proposed by Ucci and Baldoni (Ucci & Baldoni, 2019). The sampled value of these special register values when no ransomware attacks prevailed were used in an autoencoder which is the artificial neural network used in an unsupervised learning algorithm. The system was designed with no ransomware data and only anomaly detection from the learned behavior is used for ransomware detection.

There are many solutions which have not used all extracted features as input to the ML algorithm. These solutions are designed as a hybrid approach combining ML and other ad-hoc techniques. The file system traversal performed by ransomware was thoroughly studied by Moussaileb et al. (Moussaileb et al., 2020) and the study concluded that the decoy files are targeted by the ransomware. The classifier based on Random Forest, Decision tree and k-Nearest Neighbors algorithms were used for the study and analyses. The file access primitives such as frequent open read and write are another feature set used as input in the classifier proposed by Mehnaz et al. (Mehnaz et al., 2018). The authors also used decoy files and file encryption monitoring to complement the solution. The solution proved Random Forest performed better compared to Decision Trees, Naïve Bayes or Logistic Regression.

The Ramsomwall (Shaukat & Ribeiro, 2018) proposed to employ ML classifiers when anomaly features are generated from the suspected processes. This solution also inspected binary executables before execution, API calls and text strings. The solution also uses canary files and its accesses and modifications are tracked. The supervised algorithms like Logistic Regression, SVM, Artificial Neural Networks, Random Forest and Gradient Tree Boosting are used for the final process classification based on certain extracted features. The features exclusively extracted from network traffic are used as the feature set in the two classifiers proposed by Almashhadani et al. (Almashhadani et al., 2020). The detection system extracted nearly twenty features from the TCP, HTTP and DNS traffic. In the decision making using two classifiers, one does per packet feature extraction and other does flow-based feature extraction. The algorithms such as Random Forest, Bayes Networks, SVM and Random Trees were used in the classifier.

The proposal put forward by Lee et al. (Lee et al., 2019) concentrates on the backup file system using ML techniques. The solution technique analyses the encryption in the file before it is copied into the backup file system. The training phase is implemented in the backup system and the threshold values of entropy are calculated for all the files on different criteria. The client hosts compares the entropy threshold value sent and decides whether the new file version is encrypted or not. The solution uses three techniques to calculate the entropy of the files and is used as the input data for the ML algorithms. The comparative study of Decision trees, k-Nearest Neighbours, kernel SVM and Multi-layer Perceptron is done in the solution. Many commercial versions such as RansomFlare (Chong, 2017) and Acronis True Image (Alsagoff, 2010) also use ML algorithms for their processes.

4. Synthesis of findings

The section provides the review aided for understanding the attack methodologies and various countermesures adopted. Most of the research papers focused on Windows was reviewed because it is the targeted OS by the most of the attackers. In defending the attacks by ransomware in Windows OS, many proposals were put forward. The metrics commonly used for accessing and suggesting improvements proposed in literature are as follows:

4.1. Central processing unit (CPU)

The rise in CPU utilization due to the file encryption is accounted as an early alarm for the ransomware triggered encryptions. The datasets used calculate the True-Positive Rates (TPR) and False-Positive Rates (FPR) for arriving at the accuracy level of the results that differentiates the benign and genuine activities of the applications or software. But there were many suggestions for threshold level set for the CPU utilization to flag the sample as benign or genuine and which is yet another explored problem by researchers. So in many cases ransomware strains take great care to ensure that the CPU utilization never goes beyond the threshold set and remains undetected. The solutions accounting CPU utilization alone will not be beneficial to identify and detect all ransomware.

4.2. File system operations

The file system operations changing the records in MBR and MFT are closely watched in many solutions to understand the ransomware activities. The abnormal call for functions such as CreateFile, ReadFile, WriteFile, RenameFile and EncrptFile signifies the ransomware attack as per the literature. The early detection of ransomware attacks assisted by monitoring these function calls helps in taking quick preventive measures. Any change in access control or privilege escalation is also monitored in the file system to avoid the management tool set access by attackers.

4.3. Behavior based pattern recognition

The identified ransomware behavior patterns are studied and added as signatures in many of the solutions. The patterns can be like accessing management tools, privilege escalation, file system accesses etc. The persistence techniques used by the ransomware is also used as a behavior pattern for identifying the ransomware variant.

4.4. Content based pattern recognition

The certain pattern of strings and crypto-modules are used in identifying the content and categorizing the sample as malicious or genuine in many cases. The content based pattern recognition is suitable for detecting existing ransomware using signatures. The limitation in finding new variants of ransomware is a challenge seen in these solutions too.

4.5. Reboot-to-restore

The kernel level or OS level configuration uses techniques to keep the configuration intact if suspected change or modification is noticed in the computer configurations. The system immediately goes on for a reboot to restore the default system configurations and backup files. In many cases the malware uses intelligence to identify the configuration and do privilege escalations to cancel or reschedule the recovery.

Even though the metrics evaluated techniques are employed in the existing solutions, it is very rarely reported that a new or mutant strain is identified and reported before attacks. So there are still more features or metrics to be identified for better analysis and categorizing the files. There is also a need for in-depth analysis of humongous logs from network, events, processes, and memory dumps etc. which require machine learning assisted solutions.

5. Discussion

There are plenty of solutions or research prototypes focusing on detection and prevention of ransomware attacks. Recovering data after an attack has always been found extremely difficult and impossible in most of the cases. Hence there are only very few solutions that assure file recovery after a ransomware attack. These attacks pose grave threat to user data and intercept productivity of the running business. Even though all the solutions discussed identify many of the ransomware attacks, the evolved variants adopt techniques to bypass these solutions and attack the computer without being noticed. There are ransomware prevention techniques, which analyze the common behavioral traits of ransomware such as accessing file information, successive encryption of files etc. to find the ransomware. Of late, the mutant forms of ransomware variants have concealed the behavioral threat to bypass from these preventive methods. So, finding and preventing newly coming up ransomware would be challenging with the existing preventive solutions.

5.1. Theoretical contribution

The need of the hour is to ensure information security at both individual and organizations level by avoiding threats from ransomware.

The extinct variants with their inherent evolution are the major trends in RaaS used by the criminals evolved to something for the sources of income. The survey states that the codes used in attacks are often basic and sometimes a high level scripting language is even used. Various cryptosystems using both symmetric and asymmetric cryptography are employed in most of the cases. Most of the ransomware attacks hosted and reported do not do mass extortion and are used for targeted attacks in limited perimeter. The strength the ransomware authors built from the fear they generate into the user mind using the 'Name-for-shame' technique is a point to rethink and come up with a new strategy for ransomware defense. The ransomware attacks or infections are to be monitored with a mature and complex enough activity that deserves compliments for early detection.

There are many theoretical surveys which discuss the preventive measures to be taken at the individual and organization level against ransomware attacks. The first step is a good policy with procedures in protecting corporations from these security threats. These policies should give guidelines for all users even if they are not computer professionals and there should be management level support for policy and procedure enforcement. The second step is a multi-layer prevention solution is the next step that can be achieved by IT infrastructure efficiently managed by IT professionals who do maintenance, troubleshooting, and compliance management. The third requirement is a report system which uses internal email or enterprise instant messaging to make users aware of the system patches/updates.

There are many studies focusing on efficiency improvements of the ransomware detection and prevention techniques. Thorough research in this field have identified many features which would give hints for earlier identification of both existing and new ransomware variants. The ML algorithms require humongous data for their analysis and hence the collection of training and testing data is another outcome from these researches. The limitations of the traditional signature based solutions in finding the new variants is also a major issue that was highlighted as the findings in the research.

5.2. Practical implications

The challenges identified of late in the analysis of ransomware and research focuses required are as discussed. The ransomware attacks use custom-made ciphers and hence their detection and categorization was proved to be ineffective in classical solutions. The attacker uses code obfuscation and hence generic detection is also really tough using classical analysis approaches. The signatures based on strings, domain names, IP addresses, DNS names etc. become obsolete quickly due to the obfuscation methods used by ransomware mutants. The ransomware executes and behaves like genuine privacy preserving applications and pointing the presence of malign codes in suspicious situations often throws false positives and causes serious problems with anomaly based detection techniques.

The ML based existing solutions require in-depth analysis for features selection and optimization techniques for effective detection of new variants of ransomware. Hence creating training data set for deriving precise ransomware attacks detection model within stipulated timeline (Identification of features, online training of the attack detection engine for dynamic modeling to reduce attack surface) is identified as the practical requirement for improvements. ML models have shown promising signs in identifying ransomware attacks hosted by identified ransomware and its mutants.

6. Conclusion

Advancements of tools and techniques are required as the ransomware are quickly evolving in this era. There are many industrial and academic proposals that run in local hosts, servers, cloud etc. to detect and prevent these attacks. Many proposals have suggested that the log analysis of file system behaviors, network packets, memory dumps, etc. can give hints for early detection of ransomware. So based on the available research, the article depicts the issues and challenges of existing solutions for applying these techniques in the real environment due to various limitations. The existing solutions are heuristic and stress the use of AI/ML techniques for better ransomware detection and prevention. ML is being identified as the best way to analyze humongous logs from various sources and improve the effectiveness of classification. The feature selection is the main criteria for the application of the ML techniques in these logs. The findings in the systematic literature review conclude that quick and easy classification of logs from various sources using ML technique with precisely identified features would enhance effectiveness of the Anti-ransomware solutions.

Declaration of Competing Interest

None.

Acknowledgement

The author like to thank Society of Electronic Transactions & Security (SETS) members, Dr. P.V Ananda Mohan (Mentor), Dr. P.K Saxena (Advisory Board - Chairman), Dr. Sarat Chandra Babu (Executive Director), Dr. Prem Laxman Das (Senior Scientist) and Mr. Kunal Abhishek (Scientist) for their timely support and guidance to carry out the research study. Sincere thanks to the editor and the anonymous reviewers for their valuable time and efforts in suggesting improvements for the paper.

References

Gheorghe, A. V., Vamanu, D. V., Katina, P. F., & Pulfer, R. (2018). Critical infrastructures, key resources, and key assets. In *Critical infrastructures, key resources, key assets* (pp. 3–37). Cham: Springer.

Rieck, K., Holz, T., Willems, C., Düssel, P., & Laskov, P. (2008). Learning and classification of malware behavior. In: D. Zamboni (eds). *Detection of intrusions and malware, and vulnerability assessment. DIMVA, lecture notes in computer science* vol *5137*.

Faruki, P., Bharmal, A., Laxmi, V., Ganmoor, V., Gaur, M. S., Conti, M., & Rajarajan, M. (2014). Android security: A survey of issues, malware penetration, and defenses. *IEEE Communications Surveys & Tutorials, 17*(2), 998–1022.

Hansman, S., & Hunt, R. (2005). A taxonomy of network and computer attacks. *Computers & Security, 24*(1), 31–43.

Rieck, K., Trinius, P., Willems, C., & Holz, T. (2011). Automatic analysis of malware behavior using machine learning. *Journal of Computer Security, 19*(4), 639–668 Jan 1.

Handa, A., Sharma, A., & Shukla, S. K. (2019). Machine learning in cybersecurity: A review. *Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery, 9*(4), e1306.

John, Teenu S., & Thomas, Tony (2019). Adversarial attacks and defenses in malware detection classifiers. In *Handbook of research on cloud computing and big data applications in IoT* (pp. 127–150). IGI global.

Chen, Bingcai, Ren, Zhongru, Yu, Chao, Hussain, Iftikhar, & Liu, Jintao (2019). Adversarial examples for CNN-based malware detectors. *IEEE Access, 7*, 54360–54371.

Grosse, Kathrin, Papernot, Nicolas, Manoharan, Praveen, Backes, Michael, & McDaniel, Patrick (2017). Adversarial examples for malware detection. In *European symposium on research in computer security* (pp. 62–79). Cham: Springer.

Brereton, P., Kitchenham, B. A., Budgen, D., Turner, M., & Khalil, M. (2007). 'Lessons from applying the systematic literature review process within the software engineering domain. *Journal of Systemand Software, 80*(4), 571–583.

Kumar, Sunil, Kumar Kar, Arpan, & Vigneswara Ilavarasan, P. (2021). Applications of text mining in services management: A systematic literature review. *International Journal of Information Management Data Insights, 1*(1), Article 100008.

Verma, Sanjeev, Sharma, Rohit, Deb, Subhamay, & Maitra, Debojit (2021). Artificial intelligence in marketing: Systematic review and future research direction. *International Journal of Information Management Data Insights*, Article 100002.

Grover, Purva, Kumar Kar, Arpan, & Vigneswara Ilavarasan, P. (2018). Blockchain for businesses: A systematic literature review. In *Conference on e-Business, e-Services and e-Society* (pp. 325–336). Cham: Springer.

Kitchenham, Barbara (2004). In *Procedures for performing systematic reviews: 33* (pp. 1–26). Keele, UK: Keele University.

Dargahi, T., Dehghantanha, A., Bahrami, P. N., Conti, M., Bianchi, G., & Benedetto, L. (2019). A cyber-kill-chain based taxonomy of crypto-Ransomware features. *Journal of Computer Virology and Hacking Techniques, 15*(4), 277–305.

Javaheri, D., Hosseinzadeh, M., & Rahmani, A. M. (2018). Detection and elimination of spyware and Ransomware by intercepting kernel-level system routines. *IEEE Access, 6*, 78321–78332.

https://www.scmagazine.com/home/security-news/Ransomware/netwalker-Ransomware-actors-go-fileless-to-make-attacks-untraceable/.

Kumar, Sushil. (2020). An emerging threat Fileless malware: A survey and research challenges. *Cybersecurity 3.1*, 1–12.

Nadir, I., & Bakhshi (2018). Contemporary cybercrime: A taxonomy of ransomware threats & mitigation techniques. In *International conference on computing, mathematics and engineering technologies (iCoMET)* (pp. 1–7). IEEE.
Herrera Silva, J. A., Barona López, L. I., Valdivieso Caraguay, Á. L., & Hernández-Álvarez, M. (2019). A survey on situational awareness of ransomware attacks - detection and prevention parameters. *Remote Sensing, 11*(10), 1168.
Keshavarzi, Masoudeh, & Hamid, Reza Ghaffary (2020). I2CE3: A dedicated and separated attack chain for Ransomware offenses as the most infamous cyber extortion. *Computer Science Review, 36*, Article 100233.
Kharraz, Amin, Robertson, William, Balzarotti, Davide, Bilge, Leyla, & Kirda, Engin (2015). Cutting the gordian knot: A look under the hood of ransomware attacks. In *International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment* (pp. 3–24). Cham: Springer.
https://threatpost.com/new-seftad-ransomware-attacks-master-boot-record-113010/74714/ (Accessed on 25 March 2020)
O'Meara, M. M. K., & Parisi, A. (2020).Current ransomware threats,
http://www.techiesjournal.com/type-of-ransomware/1238/ (Accessed on 25 March 2020)
Kao, D. Y., & Hsiao, S. C. (2018). The dynamic analysis of WannaCry ransomware. In *2018 20th International Conference on Advanced Communication Technology (ICACT* (pp. 159–166). IEEE.
Loman, M. (2019).How ransomware attacks,
Kharraz, A., & Kirda, E. (2017). Redemption: Real-time protection against ransomware at end-hosts. In *International symposium on research in attacks, intrusions, and defenses* (pp. 98–119). Cham: Springer.
Genç, Z. A., Lenzini, G., & Sgandurra, D. (2019). On deception-based protection against cryptographic ransomware. In *International conference on detection of intrusions and malware, and vulnerability assessment* (pp. 219–239). Cham: Springer.
Fayi, S. Y. (2018). What Petya/NotPetya ransomware is and what its remidiations are. In *Information technology-new generations* (pp. 93–100). Cham: Springer.
Sihwail, R., Omar, K., & Ariffin, K. A. (2018). A survey on malware analysis techniques: Static, dynamic, hybrid and memory analysis. *International Journal on Advanced Science, Engineering and Information Technology, 8*(4-2), 1662.
Kamble, D. R., Jain, N., & Deshpande, S. (2015). Cybercrimes solutions using digital forensic tools. *IJ Wireless and Microwave Technologies, 6*, 11–18.
Alzahrani, A., Alshehri, A., Alharthi, R., Alshahrani, H., & Fu, H. (2017). 'An overview of ransomware in the windows platform. In *2017 International Conference on Computational Science and Computational Intelligence (CSCI)* (pp. 612–617). IEEE.
Ahmadian, M. M., & Shahriari, H. R. (2016). '2entFOX: A framework for high survivable ransomwares detection. In *2016 13th international iranian society of cryptology conference on information security and cryptology (ISCISC)* (pp. 79–84). IEEE.
Boukhtouta, A., Mokhov, S. A., Lakhdari, N. E., Debbabi, M., & Paquet, J. (2016). Network malware classification comparison using DPI and flow packet headers. *Journal of Computer Virology and Hacking Techniques, 12*(2), 69–100.
Yslas, V. (2021). 'The Cost of Ransomware'.
Hong, S., Liu, C., Ren, B., & Chen, J. (2017). Sdguard: An android application implementing privacy protection and ransomware detection. In *Proceedings of the international conference on mobile systems, applications, and services, ser. MobiSys: 17* pp. 149-149.
Kirda, E. (2017, February 1). UNVEIL: A large-scale, automated approach to detecting ransomware (keynote). *2017 IEEE 24th international conference on software analysis, evolution and reengineering (SANER)*. IEEE Computer Society pp. 1-1.
Kharraz, A., & Kirda, E. (2017). Redemption: Real-time protection against ransomware at end-hosts. In *International symposium on research in attacks, intrusions, and defenses* (pp. 98–119). Cham: Springer.
Cabaj, K., Gregorczyk, M., & Mazurczyk, W. (2018). Software-defined networking-based crypto ransomware detection using HTTP traffic characteristics. *Computers & Electrical Engineering, 66*, 353–368.
Al-rimy, B. A., Maarof, M. A., & Shaid, S. Z. (2017, 23). A 0-day aware crypto-ransomware early behavioral detection framework. In *International Conference of Reliable Information and Communication Technology* (pp. 758–766). Cham: Springer.
ZeJtzer, L. (2015). 5 steps to building a malware analysis toolkit using free tool. *Zektzer Security Corp*.
Moore, C. (2016). Detecting ransomware with honeypot techniques. In *2016 cybersecurity and cyberforensics conference (CCC)* (pp. 77–81). IEEE.
Continella, A., Guagnelli, A., Zingaro, G., De Pasquale, G., Barenghi, A., Zanero, S., & Maggi, F. (2016). ShieldFS: A self-healing, Ransomware-aware filesystem. In *Proc. 32nd annual conf. comput. secur. appl. ACSAC* (pp. 336–347). 10.1145/2991079.2.
Patyal, M., Sampalli, S., Ye, Q., & Rahman, M. (2017). Multi-layered defense architecture against ransomware. *International Journal of Business and Cyber Security, 1*(2).
Kolodenker, E., Koch, W., Stringhini, G., & Egele, M. (2017, 2). Paybreak: Defense against cryptographic ransomware. In *Proceedings of the 2017 ACM on Asia conference on computer and communications security* (pp. 599–611).
Kiraz, M. S., Genç, Z. A., & Öztürk, E. (2017). Detecting large integer arithmetic for defense against crypto ransomware. *Cryptology ePrint Archive, Report, 558*, 2017.
Sgandurra, D., Muñoz-González, L., Mohsen, R., & Lupu, E. C. (2016).''Automated dynamic analysis of ransomware: Benefits, limitations and use for detection,'', arXiv:1609.03020. [Online]. Available: https://arxiv.org/abs/1609.03020
Hasan, M. M., & Rahman, M. M. (2017). RansHunt: A support vector machine based Ransomware analysis framework with integrated feature set. In *Proc. 20th int. conf. comput. inf. technol. (ICCIT)* (pp. 1–7).
Chen, Z.-G., Kang, H.-S., Yin, S.-N., & Kim, S.-R. (2017). Automatic Ransomware detection and analysis based on dynamic API calls flow graph. In *Proc. int. conf. res. adapt. convergent syst* (pp. 196–201).
Wu, B., Lu, T., Zheng, K., Zhang, D., & Lin, X. (2014). Smartphone malware detection model based on artificial immune system. *China Communications, 11*(13), 86–92.
Ab Razak, M. F., Anuar, N. B., Othman, F., Firdaus, A., Afifi, F., & Salleh, R. (2018). Bio-inspired for features optimization and malware detection. *Arabian Journal for Science and Engineering, 43*(12), 6963–6979.
Venkatraman, S., Alazab, M., & Vinayakumar, R. (2019). A hybrid deep learning image-based analysis for effective malware detection. *Journal of Information Security and Applications, 47*, 377–389.
Chadha, S., & Kumar, U. (2017). Ransomware: Let's fight back!. In *2017 International Conference on Computing, Communication and Automation (ICCCA)* (pp. 925–930). IEEE.
Ucci, D., & Baldoni, R. (2019). Survey of machine learning techniques for malware analysis. *Computers & Security, 81*, 123–147 Aniello L.
Moussaileb, R., Navas, R. E., & Cuppens, N. (2020). Watch out! Doxware on the way…. *Journal of Information Security and Applications, 55*, Article 102668.
Mehnaz, S., Mudgerikar, A., & Bertino, E. (2018). Rwguard: A real-time detection system against cryptographic ransomware. In *International symposium on research in attacks, intrusions, and defenses* (pp. 114–136). Cham: Springer.
Shaukat, S. K., & Ribeiro, V. J. (2018). RansomWall: A layered defense system against cryptographic ransomware attacks using machine learning. In *2018 10th international conference on communication systems & networks (COMSNETS* (pp. 356–363). IEEE.
Almashhadani, A. O., Kaiiali, M., Carlin, D., & Sezer, S. (2020). Maldom Detector: A system for detecting algorithmically generated domain names with machine learning. *Computers & Security, 93*, Article 101787.
Lee, K., SY, Lee, & Yim, K. (2019). Machine learning based file entropy analysis for ransomware detection in backup systems. *IEEE Access, 7*, 110205–110215.
Chong, H. (2017). SeCBD: The application idea from study evaluation of ransomware attack method in big data architecture. *Procedia Computer Science, 116*, 358–364.
Alsagoff, S. N. (2010). Malware self protection mechanism issues in conducting malware behaviour analysis in a virtual environment as compared to a real environment. In *2010 International Symposium on Information Technology: 3* (pp. 1326–1331). IEEE.

Reshmi TR is a scientist in Society for Electronic Transactions and Security (SETS), Under Office of Principal Acientific Adviser to Government of India. She received her Ph.D in Information & Communication Engineering from Anna University in 2015. Her expertise and area of interests include IPv6, Cyber security, 5G security, etc. She has authored more than 20 SCI and Scopus indexed journals. She has also presented papers in many reputed national and international conferences. She is an IPv6 forum certified Engineer (Silver), HCL certified Infrastructure Engineer & Cisco certified Network Academy Instructor. She is an active member of ISOC, IPv6 forum, IAENG and many professional forums.