JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

Deterrence Against Zero Day Ransomware Strike A Comparative Analysis

[1]Jaydeep Sarkar, [2]Dipankar Chatterjee

[1]Student of M.Tech in Computer Science & Engineering, [2]Associate Professor of Computer Science & Engineering
Department of Computer Science & Engineering
Supreme Knowledge Foundation Group of Institutions, Mankundu, West-Bengal, India

Abstract

A moderate risk for both individuals and organizations in the realm of network security and cybersecurity is Ransomware. Ransomware is a type of sophisticated malware that targets not only Windows-based operating systems but also Linux and Android. It does this by taking advantage of flaws in the various versions of these operating systems or device driver software to get access to a machine. Once inside, ransomware encrypts user files using strong cryptographic methods, making the data inaccessible and, in many cases, impossible to recover without proper backups. To bypass early security checks, ransomware often disguises itself as a legitimate file before execution. After the malicious payload is activated, reversing the encryption process becomes extremely difficult for known ransomware variants and nearly impossible when a previously unknown variant, commonly referred to as a zero-day attack, is involved. The objective of this paper is to provide a clear understanding of the challenges posed by ransomware and to examine existing mitigation techniques through the analysis of 25 relevant research studies. Several effective prevention strategies are discussed, including secure execution mechanisms, early detection of encryption activity, user-level authorization for file modifications, and Host Intrusion Prevention System (HIPS)–based controls. These approaches can significantly restrict ransomware execution and, in some cases, stop the attack entirely. Since unauthorized file encryption and modification form the core objective of ransomware, preventing these actions directly limits the attacker's success. Therefore, implementing appropriate security measures before an attack occurs is essential for reducing ransomware impact.

Keywords*: Ransomware, Cyber Attack, Virus, Cybersecurity, Malware, Encryption, Threat Detection.*

Introduction

Ransomware is a type of malware designed to block access to a computer system, network, or data until a ransom is paid. Ransomware encrypted files with a specifically designed extension, in most of the cases AES 128-bit and 256-bit encryption process was used. It represents one of the most disruptive forms of cyberattacks today, capable of crippling businesses, public institutions, and individuals alike. Once a system is infected, the malware encrypts files or locks the user out entirely, leaving behind a message demanding payment often in cryptocurrency to restore access. Ransomware is particularly dangerous not only because of the financial losses it can cause, but also due to the severe operational disruptions and long-term reputational harm it inflicts on affected organizations. Critical sectors such as healthcare institutions, government agencies, educational organizations, and large corporations have increasingly become prime targets of these attacks. As a result, organizations are investing more heavily in cybersecurity infrastructure and incident response planning. In many situations, victims are forced to make a difficult decision between paying the ransom—without any assurance that their data will be recovered—or facing data loss along with extended periods of system unavailability. Over time, ransomware attacks have evolved from simple encryption-based schemes into highly sophisticated and targeted operations, employing advanced techniques that often bypass or weaken traditional security defenses. [39]

Types of ransomwares:

Crypto Ransomware (Encryptors), Locker Ransomware, Scareware, Doxware (Leakware), Ransomware-as-a-Service (RaaS), Mobile Ransomware, Master Boot Record (MBR) Ransomware.

Name of few active ransomwares in recent years: BlackCat (ALPHV), LockBit, WannaCry, Jigsaw (Bitcoin Blackmailer).

Stages of ransomware attack or execution

- An Active ransomware executable file (for windows-based operating system), either downloaded into a system either camouflaged or through phishing link.
- These malefic executable files are designed to use system files for proper execution and payload delivery. Such as: kernel32.dll, user32.dll, advapi32.dll, shell32.dll.

- Before payload delivery or while executing this kind of malware update/delete registry keys from HKEY_CURRENT_USER, HKEY_LOCAL_MACHINE and similar registry directories.
- These malware files not just make a Distributed Denial of Service (DDoS) attack but also encrypts the user files using either AES, RSA, RC4 based encryption technique and convert the user files into unknown file type & format.
- Ransomware demonstrates its sophisticated powers by recognizing and setting up Windows firewall rules to block outgoing traffic from installed firewall, antivirus, and anti-spyware program executable binaries.
- Some of the ransomwares changes victim's desktop wallpaper, deletes its own files and after the procedure is complete, it leaves ransom note and some ransom payment information only.
- During ransomware execution process, it may install its dependency file such as device driver, create files & logs inside system volume information, windows root directory, delete shadow drive data, backup plan and files of windows.
- After encryption, the ransomware renames the file with a randomly generated string that follows the pattern [0-9 a-z A-Z_-]{10} and adds a certain extension.

Ransomware attack history and current trends

The development of cybercrime from isolated events to a pervasive, coordinated danger is reflected in the history of ransomware attacks worldwide. The first known ransomware attack was in the early 2000s, where AIDS Trojan (a.k.a. PC Cyborg) claimed its first victim with a demand to send $189 to a PO Box in Panama. In mid 2000s early ransomware like Gpcode used weak encryption, and most attacks targeted individuals via spam emails. CryptoLocker classification as a Trojan horse in 2013 made a chaos with the use of strong encryption and demand Bitcoin. Spread through malicious email attachments. Targeting both individuals and corporations, variants such as CryptoWall, TeslaCrypt, and Locky surfaced between 2014 and 2016. Bitcoin helped payment systems advance, making it more difficult to track down transactions. In 2017 WannaCry (a.k.a wannacryptor) infected over 200,000 systems across 150 countries, including the UK's NHS, Spain's Telefónica and FedEx with a damage estimated to be worth $4 billion. The targeted operating system was mainly windows based. The old and outdated SMB Server v.1 protocol was targeted to gain access in almost all latest versions of windows. Microsoft was forced to release security update MS17-010(KB4012212) [41] for that particular vulnerability for all os versions including the out-of-support version, Windows 7. Microsoft also asked the user to turn of the SMB1.0/CIF File Sharing option if it is not in use. Mid 2017 a tool named WanaKiwi and WanaKey was able to decrypt the data in the hands of the ransom software, but only if the user had not restarted or turned off the computer. NotPetya was disguised as ransomware but was a destructive wiper made a damage estimated cost $10 billion globally.

During the pandemic years of COVID-19 Ransomware-as-a-Service (RaaS) attack became dominant targeting healthcare and remote work infrastructure were very common. Currently ransomware groups are using AI-assisted phishing, data destruction, and targeted backup's deletion technique for latest generation ransomwares.

Unknown ransomware attacks have steadily increased over the past few years, giving people and businesses alike a lot of headaches. Active ransomware groups like Revil, BlackBasta, Conti, Maze, Lockbit are contributing in top 5 ransomware groups. New entries such as Vice Society, BlueSky etc, were also observed.

Global ransomware damage costs prediction

Ransomware, the fastest-growing category of cybercrime, is 35 years old and is predicted to cost victims roughly $275 billion annually by 2031, with a new attack occurring every two seconds as criminals continue to improve their malware payloads and related extortion tactics, according to Cybersecurity Ventures. [36]

Different ransomware activity

Ransomware	Active since	Encryption	Attack method	Estimated damage
Cerber	2016	AES-256 + RSA for key encryption	CVE-2023-22518 vulnerability, Malicious Websites & Ads	$10 million USD
Locky	2016	AES-128 in ECB + RSA-2048	Script based executable file using macros (.docx, .xlsx)	$100 million USD
KeRanger	2016	AES (with RSA key exchange)	Spread through Transmission, a popular torrent client for macOS	$2.4 million USD
WanaCrypt0r	2017	AES-128 for file encryption, RSA-2048 to encrypt AES keys	EternalBlue (SMBv1 flaw)	$4 to 8 billion USD
NotPetya (also referred to as Petya)	2017	AES-128 encryption (with RSA-2048)	CVE-2017-0144 vulnerability, SMBv1 protocol	$8 to $10 billion USD
Phobos	2018	AES + RSA hybrid encryption	RDP brute force, phishing, and vulnerable VPN services	$100 to $300 million USD
REvil (aka Sodinokibi)	2019	AES + RSA	Exploits, phishing, remote desktop (RDP) brute-force, and software supply chain attacks	$1 to $2 billion USD

Maze (ChaCha ransomware)	2019	ChaCha20 stream cipher for file content + RSA-2048 for key encryption	RDP brute force attacks, VPN vulnerability: CVE-2019-11510, WMI, SMB shares	$800 million USD
LockBit	2019	Hybrid — AES-256 + RSA-2048	RDP Brute Force	$85,000 to $10 million USD
Conti	2020	AES-256 + RSA	Remote Desktop Protocol (RDP) Brute Force, Exploits of Unpatched windows Vulnerabilities using process injection, API hooking	$2.7 to $5.5 billion USD
DarkSide	2020	AES-256	Ransomware-as-a-Service (RaaS)	$4.4 million in Bitcoin
BlackCat aka ALPHV	2021	AES or ChaCha20	Phishing emails, and compromised RDP or VPN services	$1.6 billion USD

Targeted file types

File types that are significant to consumers and organizations are usually the targets of ransomware, particularly those that are likely to hold valuable data or intellectual property. Such as: Word Documents(“.doc”, “.docx”, “.txt”, “.rtf”), Microsoft Excel(“.xls”, “.xlsx”), Microsoft PowerPoint(“.ppt”, “.pptx”), Microsoft Access(“.accdb”, “.mdb”), Outlook email data, Image files(“.jpg/jpeg”, “.png”, “.gif”), Generic database formats(“.sql”, “.db”), Audio files(“.mp3”, “.aac”, “.wav”), Video files(“.mp4”, “.mkv”, “.avi”), Compressed archives(“.zip”, “.rar”), Backup and temporary files(“.bak”, “.tmp”), Disk images(“.iso”, “.img”), System or application logs(“.log”).

Comparative study of current methods

Sl No	Paper Name	Author(s) & Year	Dataset/ Sample	Technique/ Method	Detection Accuracy/Ratio
1	Early detection of crypto-ransomware using pre-encryption detection algorithm	S.H. Kok, Azween Abdullah, NZ Jhanjhi, Year- 2020	Sgandurra et al. (2016)	Analyse the system API call using Cuckoo Sandbox an signature/SHA-256 hash-based detection. Trained a model based on the extracted data.	80:20
2	PayBreak: Defence Against Cryptographic Ransomware	Eugene Kolodenker, William Koch, Gianluca Stringhini and Manuel Egele Year- 2017	107 ransomwares samples	PayBreak, key vault mechanism that pro-actively protects against the threats posed by crypto-based ransomware	PayBreak can successfully recover from 12 different ransomware family out of 107 samples.
3	Ransomware Detection Using the Dynamic Analysis and Machine Learning: A Survey and Research Directions	Umara Urooj, Bander Ali Saleh Al-rimy, Anazida Zainal, Fuad A. Ghaleb and Murad A. Rassam Year- 2021	2019 to 2021 from different platforms including Virus Share, Virus Total	Machine & deep learning with static analysis and dynamic analysis	-
4	AI-Based Ransomware Detection	Jannatul Ferdous, Rafiqul Islam, Arash Mahboubi, and Md Zahidul Islam Year- 2024	Virus Total Virus Share, Malshare, Ransom watch (malware samples)	Systematic evaluation framework of AI-based ransomware detection model	Overall accuracy 97.15
5	Ransomware Attack: An Evolving Targeted Threat	Manuj Aggarwal Year- 2023	Reference journals	Protective measures and maintaining proper and tested backups	-
6	A Ransomware Early Detection Model based on an Enhanced Joint Mutual Information Feature Selection Method	Tasnem Magdi Hassin Mohamed, Bander Ali Saleh Al-rimy, Sultan Ahmed Almalki Year- 2024	Total 1524 samples from different ransomware detection studies	Ransomware Early Detection and Defence System using Machine Learning, Enhanced Joint Mutual Information (EJMI) a proposed model.	Enhanced Joint Mutual Information (EJMI) method- Using RF: 99.62% Using SVM: 98.77% Using KNN: 98.77% Using FCNN: 95.18%

7	Temporal Data Correlation Providing Enhanced Dynamic Crypto-Ransomware Pre-Encryption Boundary Delineation	Abdullah Alqahtani and Frederick T. Sheldon Year: 2023	Virus share, informer.com (malware samples)	(i) Temporal Data Correlation (ii) Pre-encryption Feature Extraction (iii) Training and Testing of our early detection model	Using LR: 0.892 Using SVM: 0.93 Using DBN: 0.946 Using CNN: 0.931 Using MLP: 0.916
8	Malware Attack Detection in Large Scale Networks using the Ensemble Deep Restricted Boltzmann Machine	Janani Kumar and Gunasundari Ranganathan Year: 2023	Malrec and CTU-13 including Hash and samples	Ensemble Deep Restricted Boltzmann Machine (EDRBM) using AI	EDRBM detects malware with high reliability
9	ShieldFS: A Self-healing, Ransomware-aware Filesystem	Andrea Continella, Alessandro Guagnelli, Giovanni Zingaro, Giulio De Pasquale, Alessandro Barenghi, Stefano Zanero, Federico Maggi Year: 2016	1,763 million IRP data, 383 active ransomware samples from Virus total	1) Automatically shadowing a file whenever, the original one is modified 2) Shield filesystem.	ShieldFS encryption detection 97.70% without any false positive
10	An Enhanced Minimax Loss Function Technique in Generative Adversarial Network for Ransomware Behaviour Prediction	Mazen Gazzan, Frederick T. Sheldon Year: 2023	8152 samples collected from Virus share & informer.com	Bi-Gradual Minimax (BGM) loss function for the Generative Adversarial Network (GAN) Algorithm	GAN: 0.994 at 50 features GAN: 0.995 at 50 features
11	Using Machine Learning for Early Detection of Ransomware Threat Attacks in Enterprise Networks	Badhon Mondal, Sri Sai Nithin Chowdary Dukkipati, Md Tanvir Rahman, Md Toukir Yeasir Taimun Year: 2025	CICIDS 2017 Ransomware Dataset, CSE-CIC-IDS 2018 Dataset, Open Malware Dataset (Kaggle)	Classification Models for Ransomware Detection 1) Support Vector Machines (SVM) 2) Random Forest 3) Neural Network (Deep Learning)	Support Vector Machine (SVM) 96.5% Random Forest (RF) 94.8% Deep Neural Network (DNN) 95.6%
12	Enhancing Cybersecurity: Comparative Insights in Machine Learning Models for Ransomware Detection	Md. Tauhidur Rahman Rafi, Iffath Tanjim Moon, Md. Musfiqur Rahman Mridha, Md. Shahid Ahammed Shakil, Md. Jamil Chaudhary, and Md. Taufiq Khan Year: 2025	138,047 samples and 57 unique attributes	1)Ransomware Detection using GANs 2)Ransomware Detection through Machine Learning 3)Ransomware Detection using Random Forests	This research confirms the efficacy and efficiency of machine learning algorithms, namely ensemble ones like Logistic Regression + Gradient Boosting and Random Forest + ANN, with high accuracy and low values of false positive in ransomware detection.
13	Ransomware detection using deep learning based unsupervised feature extraction and a cost sensitive Pareto Ensemble classifier	Umme Zahoora, Asifullah Khan, Muttukrishnan Rajarajan, Saddam Hussain Khan, Muhammad Asam & Tauseef Jamal Year: 2022	https://rissgroup.org/ransomwaredataset/. Detailed	"CSPE-R" The workflow is decomposed into 5 phases: (1) core features hunting, (2) cost matrix formulation, (3) learning heterogeneous base estimators, (4) estimator selection, and (5) decision aggregation.	1) Proposed method with ensemble selection, ACC: 93.0 2) Proposed method without ensemble selection, ACC: 85.3 3) Front 1, ACC: 93.0 4) Front 2, ACC: 84.6

14	Understanding Ransomware Attacks: Trends and Prevention Strategies	FNU Jimmy Year: 2023	IEEE, Springer, MDPI, Elsevier, IET, Archive.org, Microsoft, CrowdStrike, Symantec, and Techspot were considered	Fooling attacker by Patel & Tailor, 2020, blocking server message block (SMB) ports or disabling SMBv1 and Software Restriction Policies	Defensive strategies, including a hybrid machine learning solution integrating KNN and density-based algorithms, achieving a high ransomware attack prediction accuracy of 98%, (Sreejith Gopinath & Aspen Olmstead, 2022).
15	Mitigating the Effects of Ransomware Attacks on Healthcare Systems	Sreejith Gopinath, Aspen Olmstead Year: 2022	-	Store simulated sensitive data outside the system boundary to employ advanced protocols to ensure safety and authorized access to the data stored in the repository.	Storage approach proposed by this work. Resilience to attack is Very High
16	A Socio-technical Approach to Preventing, Mitigating, and Recovering from Ransomware Attacks	Dean F. Sittig, Hardeep Singh Year: 2016	-	1) Ensure Adequate System Protection 2) Ensure More Reliable System Defence 3) Ensure Comprehensive System Monitoring 4) Respond, Recover, Investigate	-
17	Ransomware: Recent advances, analysis, challenges and future research directions	Craig Beaman, Ashley Barkworth, Toluwalope David Akande, Saqib Hakak, Muhammad Khurram Khan Year: 2021	Github (https://github.com /ytisf/theZoo) & (https: //github.com /leonv024/RAASNet)	1) Machine learning detection approaches 2) APIs/system calls 3) File I/O 4) APIs/system calls, Registry keys, File I/O, Strings 5) Volatile memory dump features	All the papers surveyed in this paper found from 87.56% to 99.80% of accuracy
18	Fight Virus Like a Virus: A New Defense Method Against File-Encrypting Ransomware	Joshua Morris, Dan Lin, and Marcellus Smith Year: 2021	thezoo - a live malware repository, Virus share	THE FREEDOM SYSTEM (Encryption Recovery System)	100% detection accuracy in terms of identifying ransomware and 90% of existing ransomware strains that do not seek administrator rights
19	An Effective Self-Configurable Ransomware Prevention Technique for IoMT	Usman Tariq, Imdad Ullah, Mohammed Yousuf Uddin and Se Jin Kwon Year: 2022	194 GB of data including backups, xml and supported multimedia files	Tizen 6.0 M2 (Linux LTS), Logistic Regression	Detection Accuracy: Equal to or over 90 percent.
20	Ransom Access Memories: Achieving Practical Ransomware Protection in Cloud with DeftPunk	Zhongyu Wang, Yaheng Song, Erci Xu, Haonan Wu, Guangxun Tong, Shizhuo Sun, Haoran Li, Jincheng Liu, Lijun Ding, Rong Liu, Jiaji Zhu, and Jiesheng Wu Year: 2024	https://tianchi.aliyun.com/ dataset/177511? lang=en-us	DeftPunk, a practical ransomware detection and data recovery framework for cloud EBS	Precision: 95.8% Recall: 98.6% F1-score: 97.1%
21	An Effective and Efficient Features Vectors For	Nawaf A. Khalil, Ban M. Khammas Year: 2022	VirusTotal & ShieldFS	Five Machine learning techniques (feature extraction, N-gram	Accuracy of classification equal to 98.33%

	Ransomware Detection Via Machine Learning Technique			vector, and CF-NCF)	
22	A Framework for Analyzing Ransomware using Machine Learning	Subash Poudyal, Kul Prasad Subedi, Dipankar Dasgupta Year: 2019	Virus Total, Virus Share and theZoo	A reverse engineering framework incorporating feature generation engines and machine learning.	Assembly Level: 94.46% Dll Level: 86.38% Combined Level: 95.5% Individual Family Detection: 98.62% Logistic regression: 89.18% Random Forest: 97.95%
23	Timed Automata for Mobile Ransomware Detection	Fabio Martinelli, Francesco Mercaldo and Antonella Santone Year: 2020	VirusTotal	Formal Model Creation & Formal Model Verification using system call trace	Precision: 0.96 Recall: 0.97 F-Measure: 0.96
24	Leveraging Machine Learning for Ransomware Detection	Nanda Rani, Sunita Vikrant Dhavale. Year: 2022	Ransomware samples collected from various sources	Machine Learning and Deep Learning	Accuracy: 98.21%
25	GuardFS: a File System for Integrated Detection and Mitigation of Linux-based Ransomware	Jan von der Assena, Chao Feng, Alberto Huertas Celdrán, Róbert Oleš, Gérôme Bovet and Burkhard Stiller Year: 2024	MalwareBazaar, github	Integrated Detection and Mitigation of Ransomware Through the File System 1) File System Plane 2) Detection Plane	Accuracy for unseen Ransomware: 94% & Accuracy for known Ransomware: close to 100%

Proposed technique and methodology

- Prevention of auto file execution: Auto file execution refers to the process where a file (such as a program, script) is automatically run or opened by the system without requiring the user's permission to manually launch it. There are several events where an executable file can run without consent of the user, such as system startup, user login, removable device, scheduled time via Task Scheduler. Using a proper measure like removing any unwanted program form startup directory or disabling any startup entry from task manager. For windows users to disable any auto execution using windows registry, create a REG_DWORD file naming NoDriveTypeAutoRun in the HKEY_CURRENT_USER\ Software\ Microsoft\ Windows\ CurrentVersion\ Policies\ Explorer directory and set value data to 0xFF (255). In build functions like User Account Control helps to prevent potentially harmful programs from making changes to a system. Using group policy editor user can disable Autorun function. In windows local group policy editor enable set the default behavior for Autorun and set it to "Do not execute any autorun commands" and enable turn off Autoplay and set it to "All Devices". Also manually check task scheduler for unknown file entry in for schedule execution.

- Encryption detection of files: Using a modest, background-running file system monitoring tool to keep a watch on and spot any strange encryption on both user and system data. This method shall stop all encryption processes, including the main root process that controls the malicious encryption process.

- Prevent uninstallation of crucial application: Some ransomware uses innovative strategies to remove or uninstall protection products before running the original malware file, so that malicious process can't be stopped during execution. A self-defense security program ought to be installed on every system.

- Blocking of unused ports: Blocking of unused ports is a fundamental security practice to reduce the attack surface and prevent unauthorized access to a system or network. Many network services and applications use specific ports to communicate over the internet or local networks, and some of these ports, if left open, can be exploited by attackers to gain access to the system.

- Blocking unknown network connections: Blocking unknown network connections is a critical security measure to safeguard your network and systems from unauthorized access, potential cyber-attacks, and data exfiltration. Unauthorized or unknown network connections can include attempts by malicious actors to infiltrate systems, exploit vulnerabilities, or infiltrate sensitive data.

Future work and limitations

Future will completely depend on nature of work direction, threat analysis and funding. Major security companies investing a large amount of funds for R&D purpose. Ransomware is not just a malware, its being used by many hackers and attackers as a tool of terror. Zero-day attacks can't be prevented by just signature checking like MD5, SHA256. Behavior analysis using artificial intelligence are being widely used now days for prevention and protection. It is also the part of the future ransomware defence technique along with different file systems and protective data vaults. Implementing layered defence with combination of

pre-encryption detection and proactive detection can be the future. Further decryption tools must be the part of all anti-malware solutions.

Current detection techniques focus on limiting the number of encrypted files by blocking processes that exhibit ransomware-like behavior, such as API calls, registry key modifications, or embedded binary strings. Due to the dynamic nature of ransomware these days, developing a suitable defence layer against current and potential threats from ransomware is a difficult task for any individual, organization, or security firm. Future ransomware attacks should be more resilient and diverse. Similar to how various security firms are attempting to stop these assaults, ransomware is always changing. similar to how AI and ML are used in threat defence. Every day, ransomware attack methods change, including new approaches, security layer breaches, the discovery of update and patch vulnerabilities, and out-of-date equipment. Covering every facet of a system and keeping an eye on every node's or device's incoming and outgoing connections is impossible. Additionally, it is impossible to forecast which system would become the next target of a ransomware assault. When working on danger detection or prevention techniques, where maximum defense is the best option, this type of limitation occurs. [42]

Conclusion

Zero-day ransomware attacks pose a serious and constantly evolving threat to both individuals and organizations because they exploit previously unknown vulnerabilities in software, systems, or applications. Since these attacks occur before patches or signatures are available, traditional security mechanisms alone are often insufficient. As a result, the most effective way to reduce their impact is through a proactive and multi-layered security approach that combines prevention, early detection, and rapid response capabilities. The adoption of artificial intelligence and machine learning techniques has shown promising results in identifying abnormal behavior and potential ransomware activity at an early stage. Compared to post-infection detection, data protection and preventive mechanisms provide significantly better outcomes by stopping or limiting the attack before widespread damage occurs. Although several proactive detection systems have proven effective against zero-day ransomware, the threat remains persistent due to the continuous evolution of attack techniques. In conclusion, defending against zero-day ransomware requires a holistic and adaptive security strategy that emphasizes prevention, detection, and timely response. While it is not possible to completely eliminate the risk, the integration of advanced security technologies, adherence to best practices, and the development of a resilient backup and recovery strategy can greatly improve an organization’s ability to prevent, mitigate, and recover from zero-day ransomware attacks.

References

1. Early detection of crypto-ransomware using pre-encryption detection algorithm (S.H. Kok, Azween Abdullah, NZ Jhanjhi), 2020.

2. PayBreak: Defence Against Cryptographic Ransomware (Eugene Kolodenkerz, William Koch, Gianluca Stringhiniy, and Manuel Egele) Boston University, MITRE, University College London, 2017.

3. Ransomware Detection Using the Dynamic Analysis and Machine Learning: A Survey and Research Directions (Umara Urooj, Bander Ali Saleh Al-rimy, Anazida Zainal, Fuad A. Ghaleb and Murad A. Rassam), 2021.

4. AI-Based Ransomware Detection: A Comprehensive Review (Jannatul Ferdous, Rafiqul Islam, Arash Mahboubi, And Md Zahidul Islam), 2024.

5. Ransomware Attack: An Evolving Targeted Threat (Manuj Aggarwal), 2023.

6. A Ransomware Early Detection Model based on an Enhanced Joint Mutual Information Feature Selection Method (Tasnem Magdi Hassin Mohamed, Bander Ali Saleh Al-rimy, Sultan Ahmed Almalki), 2024.

7. Temporal Data Correlation Providing Enhanced Dynamic Crypto-Ransomware Pre-Encryption Boundary Delineation (Abdullah Alqahtani and Frederick T. Sheldon), 2023.

8. Malware Attack Detection in Large Scale Networks using the Ensemble Deep Restricted Boltzmann Machine (Janani Kumar and Gunasundari Ranganathan), 2023.

9. ShieldFS: A Self-healing, Ransomware-aware Filesystem (Andrea Continella, Alessandro Guagnelli, Giovanni Zingaro, Giulio De Pasquale, Alessandro Barenghi, Stefano Zanero, Federico Maggi), 2016.

10. An Enhanced Minimax Loss Function Technique in Generative Adversarial Network for Ransomware Behavior Prediction (Mazen Gazzan and Frederick T. Sheldon), 2023.

11. Using Machine Learning for Early Detection of Ransomware Threat Attacks in Enterprise Networks (Badhon Mondal, Sri Sai Nithin Chowdary Dukkipati, Md Tanvir Rahman, Md Toukir Yeasir Taimun), 2025.

12. Enhancing Cybersecurity: Comparative Insights in Machine Learning Models for Ransomware Detection (Md. Tauhidur Rahman Rafi, Iffath Tanjim Moon, Md. Musfiqur Rahman Mridha, Md. Shahid Ahammed Shakil, Md. Jamil Chaudhary, and Md. Taufiq Khan), 2025.

13. Ransomware detection using deep learning based unsupervised feature extraction and a cost sensitive Pareto Ensemble classifier (Umme Zahoora, Asifullah Khan, Muttukrishnan Rajarajan, Saddam Hussain Khan, Muhammad Asam & Tauseef Jamal), 2022.

14. Understanding Ransomware Attacks: Trends and Prevention Strategies (FNU Jimmy, Senior Cloud consultant, Deloitte, USA), 2023.

15. Mitigating the Effects of Ransomware Attacks on Healthcare Systems (Sreejith Gopinath, Aspen Olmstead), 2022.

16. A Socio-technical Approach to Preventing, Mitigating, and Recovering from Ransomware Attacks (Dean F. Sittig, Hardeep Singh), 2016.

17. Ransomware: Recent advances, analysis, challenges and future research directions (Craig Beaman, Ashley Barkworth, Toluwalope David Akande, Saqib Hakak, Muhammad Khurram Khan), 2021.

18. Fight Virus Like a Virus: A New Defense Method Against File-Encrypting Ransomware (Joshua Morris, Dan Lin, and Marcellus Smith), 2021.

19. AvePoint. Ransomware Readiness Checklist | AvePoint. 2022. Available online: (https://www.avepoint.com/ebook/ransomware-readiness-checklist), 2022.

20. A Survey on Situational Awareness of Ransomware Attacks—Detection and Prevention Parameters (Juan A. Herrera Silva, Lorena Isabel Barona López, Ángel Leonardo Valdivieso Caraguay and Myriam Hernández-Álvarez), 2019.

21. Prevention of Crypto-Ransomware Using a Pre-Encryption Detection Algorithm (S. H. Kok, Azween Abdullah, NZ Jhanjhi and Mahadevan Supramaniam), 2019.

22. Mitigating adversarial evasion attacks of ransomware using ensemble learning (Usman Ahmed, Jerry Chun-Wei Lin, Gautam Srivastava), 2022.

23. Leveraging Machine Learning Techniques for Windows Ransomware Network Traffic Detection (Omar M. K. Alhawi, James Baldwin & Ali Dehghantanha), 2018.

24. Pre-Encryption Ransomware Detection (PERD) Taxonomy, and Research Directions: Systematic Literature Review (Mujeeb ur Rehman Shaikh, Mohd Fadzil Hassan, Rehan Akbar, Rafi Ullah, K.S. Savita, Ubaid Rehman, Jameel Shehu Yalli), 2024.

25. An Improved Protection Approach for Protecting from Ransomware Attacks (Ferhat GUVÇİ1, Ahmet ŞENOL), 2023.

26. Ransomware Threats (Nagaraja Seshadri, Rubia Fathima), 2020.

27. Ransom Access Memories: Achieving Practical Ransomware Protection in Cloud with DeftPunk (Zhongyu Wang, Yaheng Song, Erci Xu, Haonan Wu, Guangxun Tong, Shizhuo Sun, Haoran Li, Jincheng Liu, Lijun Ding, Rong Liu, Jiaji Zhu, and Jiesheng Wu), 2024.

28. Advances in Malware Analysis and Detection in Cloud Computing Environments: A Review (S. Madhusudhana Rao, Arpit Jain), 2023.

29. Ransomware Analysis using Feature Engineering and Deep Neural Networks (Arslan Ashraf, Abdul Aziz, Umme Zahoora, Muttukrishnan Rajarajan, Asifullah Khan), 2020.

30. Timed Automata for Mobile Ransomware Detection (F. Mercaldo, F. Martinelli, and A. Santone), 2021.

31. An Effective and Efficient Features Vectors For Ransomware Detection Via Machine Learning Technique (Nawaf A. Khalil, Ban M. Khammas), 2022.

32. A Framework for Analyzing Ransomware using Machine Learning (Subash Poudyal, Kul Prasad Subedi, Dipankar Dasgupta), 2019.

33. Timed Automata for Mobile Ransomware Detection (Fabio Martinelli, Francesco Mercaldo and Antonella Santone), 2020.

34. Leveraging Machine Learning for Ransomware Detection (Nanda Rani, Sunita Vikrant Dhavale), 2022.

35. GuardFS: a File System for Integrated Detection and Mitigation of Linux-based Ransomware (Jan von der Assena, Chao Feng, Alberto Huertas Celdrán, Róbert Oleš, Gérôme Bovet and Burkhard Stiller), 2024.

36. https://cybersecurityventures.com/wp-content/uploads/2023/11/RansomwareCost.pdf

37. 2022 Ransomware attack report published by Blackfog, (https://www.blackfog.com/2022-ransomware-attack-report/), 2022.

38. LockBit 3.0 Ransomware Targets Fullerton India: Company Reverts to Offline Operations as a Precaution (https://www.timesnownews.com/technology-science/lockbit-3-0-ransomware-targets-fullerton-india-demand-a-staggering-2400-crores-ransom-in-just-5-days-article-99721253), 2023.

39. What Is Ransomware? Understanding and Preventing Ransomware Attacks (https://www.trellix.com/security-awareness/ransomware/what-is-ransomware/), 2025.

40. Ransomware Resilience: Proactive Measures to Prevent and Recover from Attacks (Rajender PellReddy), 2024.

41. MS17-010(KB4012212) https://www.catalog.update.microsoft.com/Search.aspx?q=KB4012212

42. Ransomware Statistics 2025: Trends, Costs, and Key Threats (https://deepstrike.io/blog/ransomware-statistics-2025), 2025.