Ransomware Reloaded: Trends, Datasets, and AI-Driven Defenses

A. Merouani, H. Mansouri, ASK Pathan

August 10, 2025

Abstract

Ransomware has emerged as one of the most pervasive and damaging cyber threats in recent decades, targeting a broad spectrum of victims ranging from individuals to critical infrastructure, healthcare institutions, government agencies, and large enterprises. This paper provides a comprehensive and up-to-date overview of ransomware's evolution, taxonomy, business models, and defense strategies. By critically analyzing current research gaps and real-world case studies, this work seeks to guide future efforts toward more effective defense strategies in an increasingly complex cyber threat environment.

1 Introduction

Ransomware has emerged as one of the most pervasive and damaging cyber threats in recent decades, targeting a broad spectrum of victims ranging from individuals to critical infrastructure, healthcare institutions, government agencies, and large enterprises. The earliest known ransomware appeared in the late 1980s, exemplified by the AIDS Trojan, which marked the conceptual inception of malware designed to extort ransom payments by denying access to data or systems [1].

Initially, ransomware attacks in the 2010s took the form of "locker ransomware," which locked user interfaces, or "crypto-ransomware," which stealthily encrypted user files. These early attacks were largely automated, opportunistic, and non-selective [2]. However, as defensive measures such as improved data backups, network and operating system hardening, cloud adoption, and law enforcement efforts intensified, ransomware actors evolved their tactics and business models [3].

A significant milestone in ransomware evolution was the emergence of double extortion schemes, where attackers not only encrypted victim data but also exfiltrated sensitive information to threaten public exposure. The Maze ransomware family, active since 2019, was among the first to popularize this tactic, fundamentally changing the ransomware threat landscape [4]. Building on this, Hive ransomware—operational until mid-2022—pioneered the concept of triple extortion by targeting not only the infected organization but also its customers, employees, and third parties financially harmed by the breach. Basically, Hive ransomware combined encryption, data exfiltration, and third-party pressure into a coordinated extortion campaign, significantly amplifying the coercive power of ransomware [5].

Concurrently, the rise of Ransomware-as-a-Service (RaaS) platforms has lowered the technical barriers for cybercriminals, enabling even non-technical actors to launch sophisticated attacks. This business model has fueled the rapid proliferation and diversification of ransomware campaigns, including targeted "big-game hunting" attacks against high-value organizations [1].

The ransomware threat landscape has been further shaped by geopolitical tensions and the increasing use of ransomware as a weapon in cyber warfare. Since 2022, conflicts such as the Russia-Ukraine war have seen nation-states and affiliated actors deploy ransomware with data theft extortion as a strategic tool to disrupt adversaries, often prioritizing attrition and espionage over direct financial gains [6]. This shift has led to ransomware campaigns becoming more sophisticated, selective, and rapid, with attack timelines shrinking from months to days [3].

Despite the growing severity and complexity of ransomware incidents, academic research and defense mechanisms often lag behind these evolving threats. A critical challenge is the reliance on outdated or limited datasets—such as DARPA 1998 and KDD Cup 1999—that fail to represent modern ransomware variants, diverse platforms including IoT and Cyber-Physical Systems (CPS), or the latest attack methodologies. The scarcity of contemporary, heterogeneous, and publicly available datasets hampers the development of effective, explainable AI-driven detection and mitigation solutions [1].

Moreover, ransomware attacks are increasingly targeting the rapidly expanding landscape of Internet of Things (IoT) devices and systems. The proliferation of interconnected IoT devices in sectors such as healthcare, manufacturing, transportation, and smart cities has created a vast and often vulnerable attack surface. Recent years have witnessed a surge in ransomware campaigns exploiting weak authentication, unpatched firmware, and insecure communication protocols in IoT environments [7]. These attacks can disrupt critical services, compromise sensitive data, and cause cascading failures across interconnected systems, underscoring the urgent need for robust security measures tailored to the unique challenges of IoT ecosystems. As IoT adoption accelerates, the frequency and impact of ransomware incidents in these environments are expected to rise, demanding focused research and coordinated defense strategies to protect both data integrity and operational continuity.

This paper aims to provide a comprehensive and up-to-date overview of ransomware's evolution, taxonomy, business models, and defense strategies. It emphasizes the urgent need for modern datasets and interdisciplinary collaboration to develop robust detection mechanisms. By critically analyzing current research gaps and real-world case studies, this work seeks to guide future efforts toward more effective ransomware prevention and response in an increasingly complex cyber threat environment.

2 Ransomware Types, Evolution, and Trends

2.1 Ransomware Types

Since ransomware emerged in the 1980s, it has primarily been categorized into two main types: crypto-ransomware and locker-ransomware. Recently, however, another category has gained notoriety, referred to as leakware.

- **Crypto:** This is the oldest and most prevalent type of ransomware. Crypto-ransomware aims to encrypt the victim's important files and demand a ransom

in exchange for a key to decrypt the data. One of the most popular crypto-ransomware examples is WannaCry, which used the EternalBlue exploit for rapid network spread. In addition, Ryuk targeted large organizations with human-operated manual attacks. Most of these ransomware variants use current encryption algorithms such as RSA or AES, because if they are applied correctly, it is almost impossible to recover encrypted data without having the decryption key [8].

- **Locker:** Another popular category emerged in the 2010s. The ransomware in this category aims to lock the user out of their system in exchange for a ransom payment to regain access to the system. One of the popular examples is WinLocker, an early ransomware that locked the Windows UI (User Interface), popular in the early 2010s. Locker ransomware is less common now because it is relatively easy to resolve and can be dealt with using some techniques [9].
- **Leakware:** This is the new powerful form of ransomware that threatens victims by leaking their data to the public, causing irreversible damage on the reputational and financial levels. This type of ransomware usually goes after big companies or entities, as the ransom will be larger and the harm will be bigger for these entities. This new form of ransomware proposes the double extortion technique, as it combines encrypting the data and exfiltrating [10].

Figure 1: Ransomware Types and families

2.2 Timeline of Major Attacks and Innovations

Ransomware has evolved rapidly over the past decade, with several landmark attacks and innovations marking its progression from opportunistic malware to sophisticated, targeted campaigns.

- **2017: WannaCry** — Leveraging the EternalBlue exploit, WannaCry caused a global outbreak affecting hundreds of thousands of systems across industries and critical infrastructure. It demonstrated the devastating impact of automated ransomware spreading via network vulnerabilities [1].
- **2019: Maze** — Maze was among the first ransomware families to introduce the tactic of *double extortion*, combining traditional file encryption with data exfiltration to threaten victims with public release of sensitive information if ransoms were not paid. This fundamentally changed the ransomware threat landscape by increasing pressure on victims [3].
- **2021–2022: High-profile attacks** — Notable incidents include the Colonial Pipeline attack by DarkSide ransomware, which disrupted fuel supply on the U.S. East Coast, and the Costa Rica government attack by the Conti group, which led to a national emergency declaration. These attacks highlighted ransomware's growing impact on critical infrastructure and government operations [1].
- **Recent years: Emergence of triple extortion** — Building on double extortion, ransomware groups such as Hive (operational until mid-2022) pioneered *triple extortion* tactics. These campaigns not only encrypt victim data and threaten data leaks but also target third parties—such as customers, employees, and suppliers—financially harmed by the breach, thereby amplifying coercion and ransom demands [11].

This timeline reflects ransomware's shift from automated, opportunistic attacks to highly targeted, multi-faceted extortion campaigns, often facilitated by Ransomware-as-a-Service (RaaS) business models. The increasing sophistication and rapid evolution of ransomware tactics continue to challenge detection and mitigation efforts across diverse platforms and sectors.

2.3 Ransomware Generations: 1.0 → 2.0 → 3.0+

To provide a concise mental model for readers, we map the ransomware families and landmark attacks onto three evolutionary *generations*. Each generation is defined by its *dominant business model* and *extortion technique*, terminology that aligns with recent taxonomy work by Connolly et al. [2] and McIntosh et al. [3].

1.0 — Locker & Crypto (1984–2016) Ransomware 1.0 either locks the user interface or encrypts user files, then demands a single ransom in exchange for a key to decrypt user files or unlock the user interface. One of the most notable ransomware families in this generation was WinLocker(Locker Ransomware) and WannaCry (Crypto Ransomware). Offline, unchangeable, and periodically-tested backups (typically on tape or air-gapped media) was the de facto mitigation strategy of the Ransomware 1.0 era. Since the 1.0 variants did not do any data exfiltration and only encrypted locally, cleanup of clean

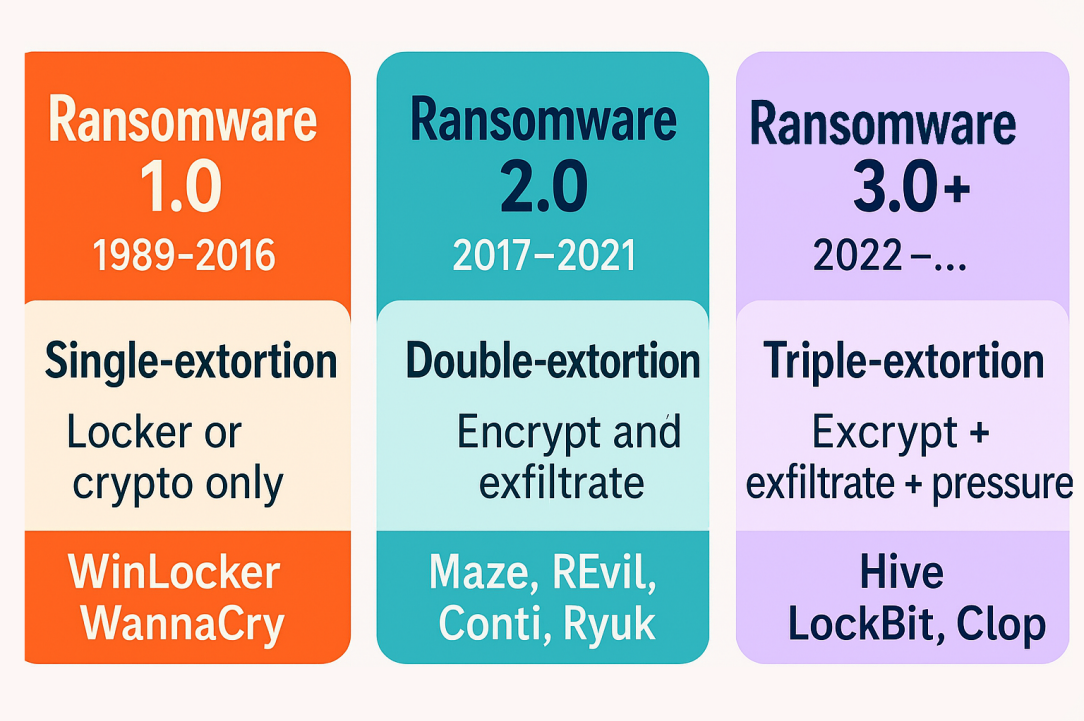

Figure 2: Ransomware generations with representative families.

backups entirely rendered the ransom ask moot—a tactic specifically noted in most initial estimates [12, 3] and is to this day listed as the most successful standalone mitigant for then.

2.0 — Double-Extortion & RaaS (2017–2021) Introduced by `Maze` [4], this stage combines encryption with *data exfiltration* and utilizes *Ransomware-as-a-Service* platforms to enable affiliates to go after *big-game* corporations [3]. For Ransomware 2.0, the key mitigation correction is that off-line backups no longer suffice, since victims need to interrupt data publication upon exfiltration as well. The literature thus converges on a three-pronged remedy: 1. Strong, immutable, off-line backups – still needed to restore encrypted files without paying the decryptor. 2. Data-loss, exfiltration detection & DLP controls, to find and block mass-scale theft before encryption activation, and thus take away the attackers' best negotiating cards [1,2]. 3. Segmentation + incident response at velocity – network micro-segmentation, EDR, and playbooks to limit lateral motion and remove the actor promptly, reducing dwell time from weeks to hours [3].

To put it briefly, 2.0 mitigation = backups + exfil defense, defined as the "new baseline" in recent surveys.

3.0+ — Triple-Extortion & Geopolitical Weapon (2022–...) A human-driven, multi-stage attack that combines encryption and large-scale data exfiltration with at least one additional coercion vector, e.g., DDoS, customer harassment, or regulatory-fine threats—often executed via RaaS marketplaces and increasingly leveraged as a geopolitical disruption tool [6, 5]. To mitigate these recent ransomware families, researchers implement these techniques:

1. **Zero-Trust Segmentation:** software-defined micro-segmentation to halt lateral movement in minutes.

2. **Immutable Backups:** off-line, versioned, and routinely tested recovery playbooks.
3. **Real-Time Exfil Defense:** DLP + NDR + CASB to detect and block data theft *before* encryption triggers.
4. **External-Pressure Defense:** DDoS-scrubbing and upstream black-holing.
5. **AI-Driven EDR + Deception:** honey-tokens and canary files for sub-minute containment and evidence capture.
6. **Cross-Functional IR Drills:** legal, PR, and supply-chain liaisons—because 3.0 impact is measured in brand and compliance fines, not just downtime.

3 Anatomy of a Ransomware Attack

To gain a deep understanding of recent ransomware variants, we must analyze the anatomy of ransomware attacks in detail, specifically the different stages of the kill chain.

3.1 Ransomware Phases

Based on [1, 13], the ransomware attack can be divided into 3, 4, or even 6 stages. With that being said, we divide the new generation of ransomware attacks into 4 major phases.

1. **Initial Access:** Also called the Delivery and Reconnaissance phase, the attacker in this stage aims to collect information about the targeted victim by network scanning, social engineering, and credential harvesting. In order to deliver the attack, the attacker uses multiple methods, such as:

   - **Phishing Emails:** The attacker sends an email to the victim containing malicious links or attachments. For example, a fake invoice with a ransomware macro.
   - **Exploit Vulnerabilities:** Attackers scan for and exploit unpatched vulnerabilities in operating systems, applications, or network devices to gain access and deploy ransomware. One of the best examples is the EternalBlue exploit (WannaCry).
   - **RDP Exploitation:** Attackers use weak or stolen RDP (Remote Desktop Protocol) credentials to obtain remote access to the target server and then implant ransomware using a remote desktop login session.

   Regardless of the attack methods we mentioned, ransomware can still infect systems through other methods such as exploit kits (EK), self-spreading mechanisms, bundled freeware applications, or by taking advantage of weak or misconfigured management protocols. During this stage, the antivirus might detect the ransomware based on signature-based detection. However, many ransomware families use obfuscation and other methods to hide. These techniques not only bypass defense systems but also increase the damage they cause.

Table 1: Key Delivery Techniques in Ransomware Attacks.

Technique	**Description**	**Example**
Phishing Emails	Malicious links/attachments in emails	Fake invoice with ransomware macro
Exploit Vulnerabilities	Use of unpatched software flaws	EternalBlue exploit (WannaCry)
RDP Exploitation	Use of weak/stolen credentials to access systems remotely	Manual deployment across the network
Drive-by Downloads / Malvertising	Automatic download from compromised or malicious websites/ads	Infected ad on a news site

2. **Lateral Movement and Privilege Escalation:** Lateral movement is a critical phase in the ransomware attack lifecycle, occurring after attackers gain initial access to a network. Instead of stopping at the entry point, attackers use lateral movement techniques to expand their reach, seeking out valuable systems, data, and credentials across the environment. This phase includes multiple essential features. Attackers expand their network reach through East-West lateral movement by using weak segmentation and compromised credentials and legitimate administrative tools, including PowerShell, PsExec, and WMI (Windows Management Instrumentation). Attackers use built-in system tools and normal user behavior imitation through "living off the land" techniques to evade detection in their attempts to bypass traditional security alerts. Attackers maintain control through the installation of multiple backdoors, which enable them to access the network after compromising any single point. Network scanning and Active Directory reconnaissance enable attackers to discover high-value systems, including domain controllers and critical servers, and sensitive data repositories. After establishing their position, attackers deploy their payload to spread ransomware or other malicious software across multiple systems at once, which results in amplified operational and financial damage.

3. **Data Exfiltration and Encryption.** Based on [1], the Data Exfiltration and Encryption stages of ransomware attacks can be defined as follows:

   Ransomware attacks have developed from basic file encryption to more advanced data exfiltration strategies with far larger impacts and coercion. The attack process normally consists of two tightly coupled stages: data exfiltration followed by encryption.

   The attacker steals the victim's sensitive or confidential data silently before encrypting victim files. This stolen data might be personal information, intellectual property, financial data, or other assets of value. This action is geared towards developing a second leverage point: when victims do not pay the ransom, the attacker tells them that they would leak or auction the stolen data, leading to reputational loss, regulatory fines, or financial damage. This is the main pivotal tactic in the current double extortion strategy. In certain instances, it is further extended to

triple extortion by extorting third-party individuals connected with the victim.

Exfiltration is characterized through stealthy reconnaissance and lateral movement, wherein the attacker discovers useful reservoirs of information and backup infrastructures. Attackers employ a range of methods for eluding discovery, including encrypting data during transit or employing legitimate network protocols. After data exfiltration is achieved, ransomware starts the encryption process in which victims' files are encrypted by high-strength cryptographic algorithms such as AES or RSA. Advanced ransomware utilizes advanced encryption techniques, including intermittent encryption of data blocks in a bid to make it faster and avoid detection mechanisms operating at the host level. Encryption makes data and systems inoperable, and the victims are requested to pay for decryption keys.

The encryption process itself is typically made to be quick and subtle, employing code packing and obfuscation techniques in order to evade detection by anti-malware. The attackers can further shut down or bypass protection software and destroy backups so they will no longer be restored for free.

With the irreparable damage via encryption and the added risk of data exfiltration, timely discovery of ransomware attacks during or even prior to such activity is paramount. Pre-encryption detection of malicious activity can enable organizations to contain compromised devices, maintain data integrity, and even block data leaks. However, the dynamic nature of ransomware, including zero-day encryption methods and sophisticated evasion capabilities, hinders early detection.

4. **Ransom Demand:** After the victim has been successfully attacked, the ransomware attackers usually demand a ransom to be paid within a specified time frame, usually 24 or 48 hours. Failure to pay the ransom often leads to the permanent loss of data or equipment failure. If the victim complies with the attacker's demands and pays the ransom, the attacker will provide the decryption key to recover the victim's data. However, this is not the only pressure point that the new generation of ransomware leverages. Let us see a few more:

   - *Double extortion:* The threat of stolen data becoming publicly available remains a concern even after paying the ransom. The risk of data leakage persists even after the ransom payment. In some cases, attackers might request separate payments for encryption keys and non-disclosure of the stolen information. Groups like Maze, REvil, and Conti have been reported to use such multi-layered ransom demands.
   - *Triple extortion:* The strategy of further coercion in ransomware attacks, like DDoS attacks, blackmailing business associates, or leaking sensitive customer information, is an extension of the classic ransom demands. As the detailed study by [1] reveals, ransomware gangs have increasingly employed such multi-layered extortion techniques to exert further pressure on victims and ensure higher chances of ransom payment.

     DDoS Attack: Attackers can, in parallel or as a follow-up, assault the victims' online services or critical infrastructure with DDoS attacks. This interferes with ordinary business operations, resulting in downtime and lost revenue, and is yet another coercive mechanism to bully victims into making timely payment of ransoms.

Threats to Business Partners: Ransomware attackers widen their leverage by threatening the victim's surroundings, such as suppliers, customers, or partners. By threatening these third parties—either with explicit attacks or threats of publishing sensitive information about them—attackers generate more extensive operational and reputation risks that heighten the victim's urgency to pay.

These strategies are a development of what has now been referred to as triple extortion, a combination of the previous double extortion strategy (encryption and data leakage threats) with other leverage points. The study points out that such multi-extortion strategies have increasingly become ubiquitous among advanced ransomware gangs as a badge that they are transitioning to more secure defenses and a requirement to further maximize leverage on victims.

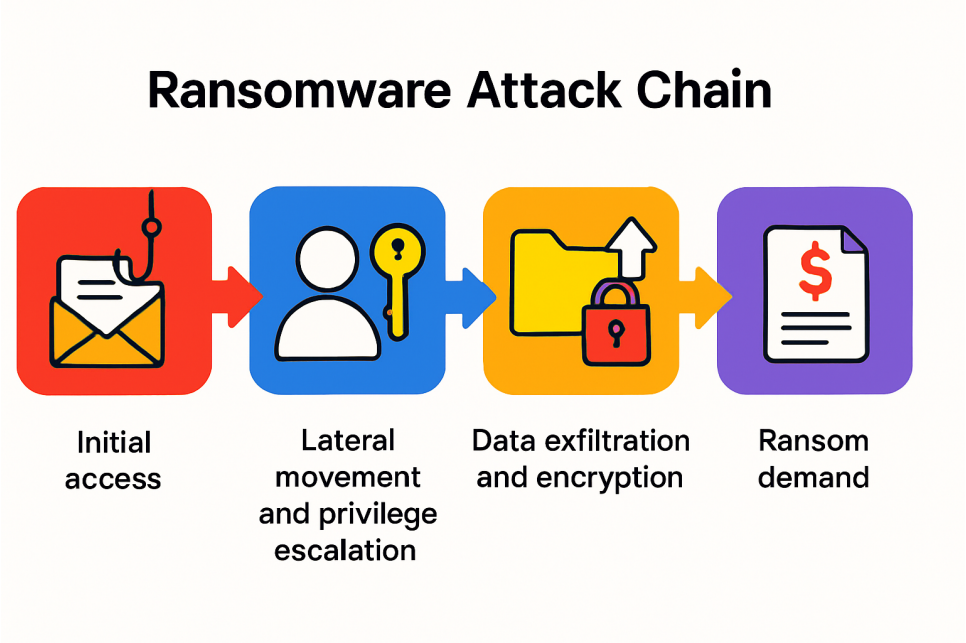

Figure 3: Ransomware Attack Chain

4 Detection, Prevention, and Mitigation

In this section, we aim to examine the latest studies in combating ransomware based on three major categories, namely detection, prevention, and mitigation. We have examined a variety of recent studies in order to achieve that.

4.1 Detection

The detection phase is the process of identifying ransomware activity on the system during or before the encryption. In this context, the researchers have applied a variety of methods, including ML (Machine Learning), entropy, and honeypots.

Table 2: Definitions of Detection, Prevention, and Mitigation in Ransomware Context

Term	**Definition**	**Focus Area**
Detection	Identifying ransomware activity early to enable containment and limit damage	Early warning, monitoring, alerting
Prevention	Implementing measures to stop ransomware from entering or executing in the environment	Proactive defense, user education, controls
Mitigation	Reducing the impact and spread of ransomware during/after an attack, and restoring operations	Incident response, recovery, containment

4.1.1 Machine Learning

In some recent studies on ransomware detection, researchers have sought to improve detection rates, avoid false positives, and tackle the difficulty of keeping up with the rapid 'evolution' of ransomware by developing machine learning (ML) and deep learning (DL) detection techniques. Let us discuss some of the significant contributions from studies that looked into ransomware detection.

Recent advancements in ransomware detection have focused heavily on ML and DL techniques to address the increasing sophistication and evasiveness of ransomware attacks. Researchers have proposed hybrid models that combine static and dynamic analysis features, such as memory dump analysis, to detect both known and unknown ransomware families, including REvil, LockBit, and BlackCat, thereby improving detection accuracy and reducing false positives [14]. Comparative studies indicate that decision tree algorithms outperform other classifiers like support vector machines and multilayer perceptrons, achieving detection accuracies up to 98.83% on real-world datasets [15]. Additionally, random forest, logistic regression, and neural network models have demonstrated high effectiveness, with random forest reaching up to 99.9% accuracy in Windows environments [16], [17]. Deep learning innovations, such as group normalization-based bidirectional long short-term memory (GN-BiLSTM) networks, have further enhanced detection and family-wise classification capabilities, achieving near-perfect accuracy (99.99%) even against obfuscated and novel ransomware variants [18].

Feature engineering techniques like recursive feature elimination with cross-validation (RFECV) have optimized model performance by selecting the most relevant features, including entropy and byte frequency, leading to detection accuracies exceeding 99% [16]. Molina et al. [19] introduced a new method for ransomware classification that uses paranoia activities, a sequence of API calls used by ransomware to locate a good execution environment. The authors fingerprinted the paranoia activities associated with over 3K samples of common and up-to-date ransomware families. They showed that their method can achieve 94.92% classification accuracy.

Collectively, these contributions represent significant progress toward proactive, accurate, and timely ransomware detection in increasingly complex threat landscapes.

4.1.2 Other Methods

While machine learning is at the forefront of ransomware detection, several other technologies and approaches play essential roles in identifying, stopping, and analyzing ran-

somware threats. Here are some widely adopted methods, often used in combination for a multi-layered defense.

Structural features obtained from ransomware consist of file hashes, header information, function/API/system calls, strings, opcodes, and file types. Researchers obtain these features from ransomware samples without running the samples.

Strings The majority of ransomware families include embedded text; in most cases, it shows after the ransomware finishes the exfiltration and encryption process, and it may contain keywords like "encrypt", "bitcoin", or even hardcoded IP addresses. These strings might be useful indicators when analyzing binaries [20].

File hashes The hash value of a sample can be compared to well-known entries in a database. The authors in [21] explore the integration of machine learning hash analysis within a backup system to proactively detect ransomware threats by combining multiple data sources and employing intelligent algorithms. However, depending only on hash values can be risky, as the attackers can slightly change the file to generate a new hash.

Function/API/System Calls: To identify which functions or APIs an upcoming program is likely to call, static analysis can be employed. The calls made by a ransomware program are often of great importance because they typically involve critical activities such as, but not limited to, encryption, deallocating memory, file calls, and network communication. The unique nature of these calls can potentially differentiate a ransomware program from an unmalicious or benign program [22].

Opcode: The opcodes and the patterns in which they occur are also helpful indicators when determining if something has ransomware behavior or at least describing the behavior of the ransomware. In [23], researchers have created a new machine learning system that can spot ransomware attacks early by analyzing how programs operate at the most basic level in computer memory. The technique focuses on opcode analysis - essentially looking at the fundamental commands that software uses to interact with the computer's processor and memory systems.

Researchers look at behavioral features as well by executing ransomware samples in monitored environments. Some of these behavioral features are the following: registry changes, log file entries, process activity, file system changes, system calls, input/output patterns, network traffic, system resource usage, and even sensor data.

Registry Activity: An activity of ransomware on a Windows system is that it typically makes changes to the registry during installation to ensure the program stays on the system following a reboot. This is not a behavior exclusive to ransomware and is also seen with other forms of malware, so tracking registry activity will be best used along with one or more of the stated indicators. Anand et al. proposed RTR-Shield, a rule-based tool to detect and block crypto ransomware activity in its early stage of execution. The tool primarily relies on two monitoring blocks: Registry Activity Monitoring Block (RAMB) and File Trap Monitoring Block (FTMB) [24].

Host Logs: Using host logs is another behavior that can track ransomware. Host logs may contain events that could be viewed as suspicious and link those events to ransomware behavior. A researcher can track digital footprints of malicious activity with Windows host logs and investigate how a specific ransomware sample interacts with the host environment [25].

File System Activity: A strong indication that ransomware is occurring is that ransomware creates a well-defined process that scans for files, encrypts them, and deletes or overwrites the original files. By monitoring the file system's activity, the file system changes can be a strong indicator that an attack is in motion. In [26] authors have

proposed a hybrid machine learning model, combines Support Vector Machines (SVM) and Random Forests (RF), specifically designed to detect ransomware through analysis of file system activities.

I/O Access Patterns: Ransomware operations such as file encryption, deletion, or overwriting typically generate repetitive input/output activities—namely, frequent read, write, and delete actions. By analyzing these I/O access patterns, it is possible to detect ransomware behavior [27].

Network Activity: Ransomware often communicates with external servers to send or receive data. Features like destination and source IP addresses, port numbers, domain names, and the protocols used can reveal suspicious communication behavior and help flag potential ransomware [28].

Resource Usage: Encryption is a resource-intensive task. As a result, unusually high CPU or memory consumption may indicate the presence of ransomware running in the background [29].

Table 3: Core Ransomware Detection Technologies.

Detection Technology	**Primary Focus**	**Key Advantage**	**Limitation**
Signature-Based	Known malware patterns	Fast detection	Misses new/unknown threats
Heuristic-Based	Suspicious actions	Spots novel variants	Prone to false positives
Behavioral Analysis	Anomalous behavior	Catches polymorphic threats	Resource intensive
Network/Traffic Analysis	Abnormal network flows	Early warning of exfiltration	May trigger false alarms
Sandboxing	Dynamic behavior inspection	In-depth file analysis	Can be bypassed
Deception/Honeypots	Decoy engagement	Early detection, threat study	Only if attacker interacts
Encryption/File Change Monitoring	File system activities	Real-time ransomware alerts	Often after attack is underway
EDR/Continuous Monitoring	Endpoint surveillance	Immediate detection/response	Requires expertise, resources

4.2 Prevention Strategies

In an attempt to prevent ransomware attacks, the researchers have used a variety of techniques, including network segmentation, immutable backups, and endpoint detection and response (EDR). In this section, we examine the notable existing works on prevention strategies for combating ransomware. Kharraz and Kirda [12] proposed a dynamic analysis model for ransomware detection. The idea is to observe and interact with the user's files or desktop. The system detects the first interaction of the ransomware with user data and tracks the changes to the files to identify patterns for ransomware activity. Kim et al. [30] proposed an outline of a ransomware detection model relying on the random number generated by the user's OS. The model is designed to work for ransomware that uses the CryptGenRandom() to generate the random number, and the encryption key is

recovered after an infection occurs. Ami et al. [31] proposed a file-access control policy system that provides ransomware prevention by imposing a file-access control policy. This system uses biometric authentication and schemes such as CAPTCHA to determine if a user is human or not, and based on the results, the system prevents malicious software from modifying and deleting user files.

Lee et al [32] concentrated on securely backing up encryption keys in a protected repository. This approach allows systems or files compromised by ransomware to be recovered easily, thereby providing effective protection against such malicious attacks. Lee et al [33] proposed a Moving Target Defense (MTD) system via changing file extensions. The files' extensions are randomly and continuously changed to confuse ransomware encryption attempts, to protect files against ransomware even when encryption tactics evolve dynamically. AlSabeh et al [30] used API call interception to detect environment probing. Their solution focuses on detecting ransomware processes probing their execution environment by intercepting Windows API calls. Then it aborts suspicious processes attempting environment detection, preventing ransomware from activating. Wani and Revathi [34] focused on IoT-based ransomware families by proposing an IoT-focused prevention system using SDN gateways. The software defined network gateways monitor and control IoT traffic, enforcing security policies to detect and mitigate ransomware. Specifically, it protects IoT devices from ransomware infiltration via network-level controls.

The above mentioned methods basically focus on preventing ransomware infections or mitigating attack effects by removing suspicious apps, blocking unauthorized file access, using dynamic file defense, securing keys, early detection through cloud systems, or IoT network monitoring.

4.3 Mitigation

The literature on ransomware mitigation contributions focuses on comprehensive strategies and technologies to reduce damage and improve resilience against ransomware attacks. Key mitigation approaches include. Cabaj and Mazurczyk [35] introduced a pair of mitigation frameworks. Initially, their system observes network traffic to detect unusual activities and then mitigates threats in real-time by isolating compromised hosts through control rules. Kolodenker et al. [36] proposed Paybreak, which counters ransomware by securely managing encryption keys, enabling victims to recover encrypted files without needing to pay the ransom.

Maimó et al. [37] underscored the significance of ransomware security within Integrated Clinical Environments (ICE). They devised a solution that utilizes an SDN (Software-Defined Network) framework in conjunction with Network Function Virtualization (NFV) to limit the spread by substituting and isolating compromised systems. Akbanov et al. [38] also suggested a ransomware mitigation approach via software-defined networking. Their model can intercept infected hosts in real-time by scrutinizing network traffic for suspicious file activities, and they evaluated the model using the WannaCry variant. Rouka et al. [39] carried out an extensive static and dynamic analysis of the ExPetr ransomware. Their approach, which relies on an SDN-based system, aimed to mitigate threats through three strategies: blocking ports, inspecting HTTP packets, and analyzing SMB messages. The authors opted to use the WannaCry sample in their model's evaluation.

Davies et al. [40] employed live forensic tools to study the memory obtained from a system compromised by ransomware. This investigation aimed to recover the keys neces-

sary to decrypt files locked by NotPetya, Bad Rabbit, and Phobos ransomware through evidence found in the analyzed memory. Faghihi and Zulkernine [41] introduced a data-centric method for both mitigating and detecting crypto-ransomware attacks specifically targeting smartphones. XXXXXXXXXX

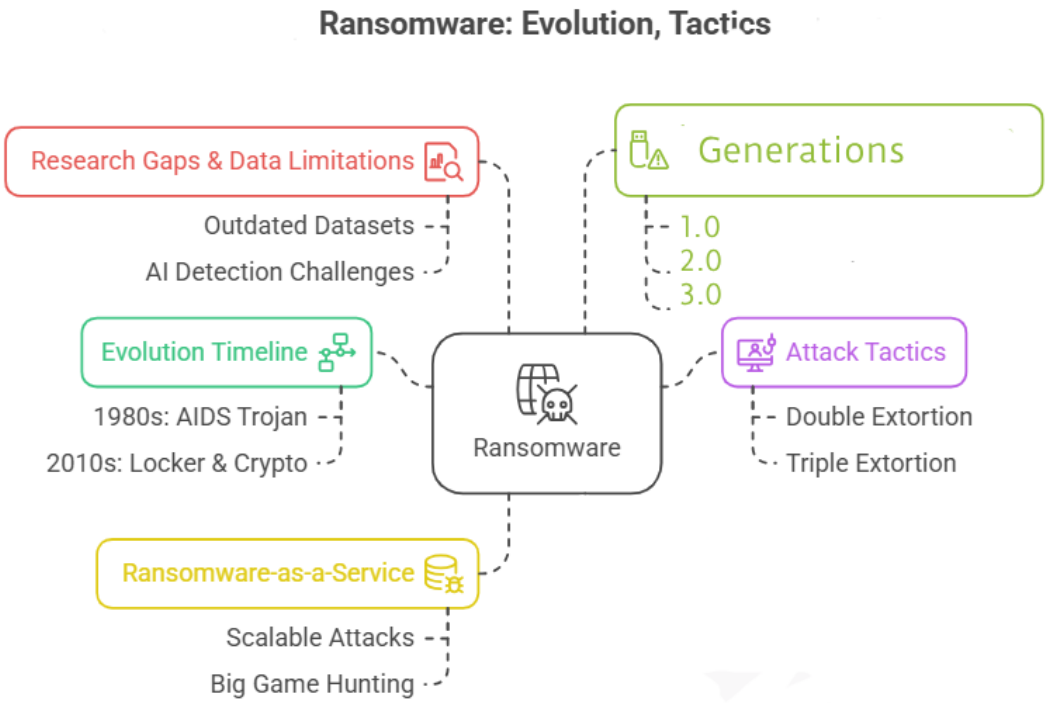

Figure 4: Ransomware Evolution and Tactics

5 Evaluation of Ransomware Detection, Prevention, and Mitigation Strategies

Ransomware defense requires a multi-faceted approach encompassing **detection**, **prevention**, and **mitigation** techniques. Below is an evaluation of each strategy, considering their effectiveness, technological trends, limitations, and research directions.

5.1 Detection Strategies

Main Approaches

- **Machine Learning-Based Detection:** Over 70% of studies leverage machine learning (ML) or deep learning for detecting ransomware, using features such as API calls, opcode sequences, registry changes, network behavior, and file activities. ML models (e.g., SVM, Random Forest, LSTM) are applied for detection on PCs, mobile, and IoT platforms.
- **Behavioral/Dynamic Analysis:** Observing program behavior at runtime to detect suspicious actions such as rapid file encryption, high-entropy file writes, or abnormal network connections.

- **Static Analysis:** Inspecting code, API usage, PE headers, or other static features of executable files for known malicious patterns without execution.
- **Hybrid Methods:** Combining static and dynamic analysis to maximize detection coverage and reduce false positives.
- **Decoy (Honeypot) Techniques:** Deploying fake files or honeytokens to trap ransomware and trigger early alerts when accessed.

Strengths

- **Accuracy:** ML models achieve high accuracy (some report >98% TPR) when trained on comprehensive, up-to-date datasets.
- **Adaptability:** Dynamic and hybrid analysis improve the chance of catching previously unseen ransomware.
- **Low Overhead:** Static analysis does not require code execution, offering speed and safety.

Weaknesses

- **Evasion and Concept Drift:** Advanced ransomware employs obfuscation, packing, and code manipulation to evade detection. ML models are vulnerable to adversarial attacks that alter code or input features. Concept drift reduces effectiveness over time as ransomware behavior changes.
- **Resource Constraints:** Behavioral and hybrid analysis, especially in real-time, can be CPU and memory-intensive, and may not be suitable for all environments, particularly IoT devices.
- **Dataset Limitations:** There is a lack of public, comprehensive, and up-to-date ransomware datasets, leading to challenges in benchmarking and validation.
- **Narrow Focus in Research:** Most research concentrates on file-encrypting (crypto) ransomware, often overlooking more recent attack tactics like data exfiltration or fileless ransomware.

Prevention Strategies

Key Methods

- **Access Controls:** Limiting application privileges to prevent unauthorized file or resource access, including runtime user authentication and biometric/CAPTCHA protection.
- **Regular Patching & Hardening:** Timely software updating and system hardening to close vulnerabilities exploited by ransomware.
- **File System and Network Segmentation:** Restricting access to sensitive areas and segmenting networks to minimize lateral movement post-infection.

- **Backup Strategies:** Regular, immutable, and offsite backups to ensure data recovery without ransom payment, along with tools to detect encrypted or suspicious backup files to avoid backup poisoning or reinfection.
- **Honeypots and Decoy Files:** Using decoys to distract and detect ransomware activities before actual harm.

Strengths

- **Prevention of Infection:** Patching and access controls can dramatically reduce infection vectors. Network segmentation contains any breach.
- **User Awareness:** Security training against phishing, social engineering, and suspicious attachments enhances resilience against the leading infection vector.
- **Resilience through Backups:** Robust backup strategies provide a reliable recovery option and reduce ransom incentives.

Weaknesses

- **Human Factor:** Social engineering and phishing remain effective due to human error, and many organizations still lack disciplined patching and training regimes.
- **Insider Threats:** Prevention strategies are less effective if insiders deliberately aid attackers.
- **Backup Limitations:** Ransomware may specifically target backups, encrypt online/offsite backups, or infect shadow copies.
- **Zero-Day Threats:** Signature and rule-based preventive measures lag behind the latest variants, and novel attack types (e.g., data exfiltration, fileless attacks) often bypass traditional defenses.

5.2 Mitigation Strategies

Major Techniques

- **Key Escrow/Interception:** Captures keys used by ransomware during encryption to facilitate recovery without ransom.
- **Network-Based Segmentation and Blocking:** Use of software-defined networking (SDN) to identify and block malicious communications and isolate infected units in real-time.
- **Automated Backup and Data Recovery:** Solutions that automatically back up changed files and quickly restore pre-attack states (sometimes at the storage hardware level).
- **Forensics and Incident Response:** Detailed logging, rapid detection, post-attack forensic analysis, and managed incident response protocols.
- **Data-Centric Mitigation:** Migration towards approaches that prioritize data protection (including exfiltration monitoring and data loss prevention) rather than just encryption-focused defense.

Strengths

- **Rapid Response:** Automated solutions allow timely isolation of infected systems, potential recovery of encrypted files, and disruption of attacker activities.
- **Business Continuity:** Effective mitigation reduces downtime, limits data loss, and helps avoid ransom payments.

Weaknesses

- **Limits of Key Capture:** Not all ransomware relies on keys handled in ways interceptable by defensive tools, and advanced strains protect their keys well.
- **Evolving Attack Tactics:** Newer ransomware strains increasingly focus on *data exfiltration* and *destruction*, for which traditional mitigation approaches (key retrieval, backup restoration) offer limited benefit. Legal, reputational, and privacy risks from data leaks outpace those from data loss alone.
- **Forensic/Automated Response Overhead:** Intensive monitoring and forensic investigation can increase system overhead and may impact user experience or mission-critical processes.
- **External Validity Issues:** Many mitigation approaches proposed in academic research are not sufficiently validated in real-world conditions or against the latest ransomware techniques (especially those focused on exfiltration or state-sponsored attacks).

5.3 Trends & Future Directions

- **Ransomware tactics have shifted** from simple encryption to double extortion (encryption plus data exfiltration) and now to destructive and espionage-focused attacks. Consequently, both academic and industry strategies must quickly update their emphasis from file-centric to data-centric and business-centric resilience.
- **Collaboration and integration:** Defending against ransomware now requires not only technical countermeasures but integration with business processes, regulatory frameworks, security governance, and industry intelligence.
- **Emergence of AI and adversarial AI/ML:** Both defensive and offensive use of generative and adversarial AI create challenges for developing robust, future-proof detection and mitigation systems.
- **Research Gaps:** There is a misalignment between academic research (often focused largely on crypto-ransomware) and the current landscape dominated by exfiltration and multi-pronged attacks. More practical, externally validated, and business-practical solutions are critically needed.

Strategy Type	Strengths	Weaknesses	Research/Practical Notes
Detection	High ML accuracy; adaptable; extensive behavioral and static methods	Evasion via obfuscation/concept drift; resource-intensive; limited real-world datasets; focus mostly on encryption	Research must address adversarial ML, concept drift, data exfiltration
Prevention	Patching, access controls, training, backup = strong foundation	Human/insider error; backup targeting; gaps in stopping exfiltration/fileless/zero-days	Integrate business/user awareness, regulatory needs, modern attack vectors
Mitigation	Automates response; limits damage, supports recovery, leverages SDN/backup/forensics	Limited by ransomware evolution (esp. exfiltration); forensic overhead; key escrow often circumvented	Must evaluate efficacy against exfiltration, double extortion, destructive attacks

Conclusions

- **Prevention and resilience**—through patching, segmentation, restricting privileges, and robust backup—remain foundational but are insufficient alone.
- **Detection systems** must continuously evolve, embrace adversarial resilience, and incorporate both behavioral and data-centric signals.
- **Mitigation** needs to prioritize organizational/data-centric risk management, consider regulatory compliance, and establish incident response plans that address modern threats (including exfiltration and destruction).
- There is a critical need for **practical, business-oriented, and externally validated solutions** aligned with the current and future landscape of ransomware threats.

6 Research Gaps and Future Directions

6.1 Prevailing Assumptions

Many studies continue to operate under several outdated beliefs about how ransomware behaves. First, it is often assumed that ransomware solely encrypts files on local hard drives and launches aggressive, automated, and indiscriminate attacks [42, 43, 44, 17, 45]. In reality, modern variants typically prioritize data exfiltration over encryption and

conduct highly selective, human-driven intrusions to remain stealthy [2]. Likewise, file entropy has been treated as a dependable indicator of encryption, even though current strains can perform partial encryption or employ encodings such as Base64 to mask entropy changes [46, 47]. It is also assumed that ransomware generates unique encryption keys solely in OS memory; yet many families fetch keys from their command-and-control servers, or dispense with encryption entirely when only exfiltrating data [48, 49, 50, 51]. Further, ransomware is no longer confined to executable files on local storage but can exist as fileless malware or purely human-operated intrusions [52, 53, 6, 54, 55]. Finally, although Bitcoin was once the default payment currency [56, 57, 58, 59, 60], groups such as Sodinokibi and DarkSide now accept privacy-focused alternatives like Monero to thwart tracing.

Recommendations for Future Research in the Ransomware 3.0 Era

To counter the rapidly evolving **Ransomware 3.0** landscape—marked by triple-extortion, geopolitical motives, and AI-driven stealth—future work should be organized along the following **five strategic axes**:

1. Data-Centric Defense Layer

- Real-time **Data-Loss Prevention (DLP)** pipelines that detect exfiltration before encryption commences.
- **Zero-trust micro-segmentation** with dynamic policy enforcement to isolate critical assets during lateral movement.
- **Canary datasets** and **deception grids** to bait attackers into revealing their presence early.

2. Adversarial-Resilient Machine Learning

- **Self-updating ML models** trained on streaming telemetry (API calls, file-I/O, network flows) to survive concept drift.
- **Adversarial-training frameworks** that simulate obfuscation, packing, and polymorphism to harden detectors.
- **Explainable AI (XAI)** techniques for rapid triage and root-cause analysis during incident response.

3. Cross-Domain Orchestration & Governance

- **Integrated playbooks** that merge SOC, legal, PR, and supply-chain teams for coordinated triple-extortion response.
- **Regulatory compliance dashboards** (GDPR, HIPAA, SEC) that quantify breach costs to counter ransom pressure.

- **Threat-sharing consortiums** that anonymize and distribute IoCs across sectors in near-real-time.

4. Post-Quantum & Advanced Cryptography

- **Quantum-resistant backup encryption** to invalidate future decryption demands.
- **Key-escrow alternatives** leveraging threshold cryptography for **self-recovery** without ransom payment.
- **Firmware-level integrity attestation** for IoT/OT devices to prevent bootloader-level hostage scenarios.

5. Human-Centric & Insider-Threat Mitigation

- **Continuous security-awareness simulations** targeting phishing, vishing, and supply-chain deception.
- **Behavioral analytics** on privileged users to detect insider collusion or credential misuse.
- **Secure remote-work ecosystems** (SASE, ZTNA) that harden the distributed workforce against BGH campaigns.

7 Conclusion

This survey gives an up-to-date version of ransomware's progress, structure, and defensive measures. We highlighted the fact that over time, the ransomware has become a complex threat and more. The evolution of ransomware was significant from the early types (locker and crypto) to the modern stage, which emphasizes the multi-extortion techniques like encryption, data theft, and applying DDoS attacks or even offering the ransomware as a service, Raas, which has lowered the barriers for attackers and increased campaign variety and sophistication. We highlighted ransomware 3.0 as the new generation characterized by human-operated attacks, rapid execution, use of zero-day vulnerabilities, lateral movement, and stealthy data exfiltration to maximize damage. For the Detection strategies, we noticed that the majority of the researchers focused on machine learning as the major technique, along with behavioural profiling and hybrid static/dynamic analysis. The major defect for the detection strategies is the lack of real real-world, organized dataset. Prevention measures were also covered by this survey. The researchers focused on several techniques such as network segmentation, strict access control, and immutable backups...etc. However, insider threat remains a major risk. For mitigation, we highlighted several approaches such as rapid incident response, forensic analysis, and automated recovery. Future work should focus on data-centric protection, resilient ML, legal coordination, quantum-safe cryptography, and stronger security awareness, while addressing the gap between academic focus on older models and today's exfiltration-driven threats. Overall, the survey highlights the importance of adaptive defense strategies to keep pace with the evolving nature of ransomware and the need to refocus research efforts on Ransomware 3.0.

References

[1] Mingcan Cen, Frank Jiang, Xingsheng Qin, Qinghong Jiang, and Robin Doss. Ransomware early detection: A survey. *Computer Networks*, 239:110138, 2024.

[2] Lena Y. Connolly, Michael Lang, Paul Taylor, and Phillip J. Corner. The evolving threat of ransomware: From extortion to blackmail. *Preprints*, 2021070149, 2021.

[3] Timothy McIntosh, Teo Susnjak, Tong Liu, Dan Xu, Paul Watters, Dongwei Liu, Yaqi Hao, Alex Ng, and Malka Halgamuge. Ransomware reloaded: Re-examining its trend, research and mitigation in the era of data exfiltration. *ACM Computing Surveys*, 57(1):18, 2024.

[4] Quintin Kerns, Bryson Payne, and Tamirat Abegaz. Double-extortion ransomware: A technical analysis of maze ransomware. In *Proceedings of the Future Technologies Conference (FTC) 2021, Volume 3*, volume 360 of *Lecture Notes in Networks and Systems*, pages 82–94. Springer, Cham, 2021.

[5] TechTarget. What is hive ransomware? `https://www.techtarget.com/searchsecurity/definition/Hive-ransomware`. Accessed: 2025-07-08.

[6] Microsoft. Microsoft Digital Defense Report 2022. Technical report, Microsoft Research, 2022.

[7] Syed Rameem Zahra and Mohammad Ahsan Chishti. Ransomware and internet of things: A new security nightmare. In *2019 9th international conference on cloud computing, data science & engineering (confluence)*, pages 551–555. IEEE, 2019.

[8] Ibrahim Nadir and Taimur Bakhshi. Contemporary cybercrime: A taxonomy of ransomware threats & mitigation techniques. In *2018 International Conference on Computing, Mathematics and Engineering Technologies (iCoMET)*, pages 1–7. IEEE, 2018.

[9] Craig Beaman, Ashley Barkworth, Toluwalope David Akande, Saqib Hakak, and Muhammad Khurram Khan. Ransomware: Recent advances, analysis, challenges and future research directions. *Computers & security*, 111:102490, 2021.

[10] Routa Moussaileb, Renzo E Navas, and Nora Cuppens. Watch out! doxware on the way.... *Journal of Information Security and Applications*, 55:102668, 2020.

[11] CS Anand and Ravi Shanker. Advancing crypto ransomware with multi level extortion: A peril to critical infrastructure. In *2023 2nd International Conference for Innovation in Technology (INOCON)*, pages 1–5. IEEE, 2023.

[12] Amin Kharraz and Engin Kirda. Redemption: Real-time protection against ransomware at end-hosts. In *International Symposium on Research in Attacks, Intrusions, and Defenses*, pages 98–119. Springer, 2017.

[13] KAO Da-Yu, Shou-Ching Hsiao, and TSO Raylin. Analyzing wannacry ransomware considering the weapons and exploits. In *2019 21st International Conference on Advanced Communication Technology (ICACT)*, pages 1098–1107. IEEE, 2019.

[14] Kavitha Kunku, ANK Zaman, and Kaushik Roy. Ransomware detection and classification using machine learning. In *2023 IEEE Symposium Series on Computational Intelligence (SSCI)*, pages 862–866. IEEE, 2023.

[15] Indra Chaudhary and Suyash Adhikari. Ransomware detection using machine learning techniques. *Researcher CAB: A Journal for Research and Development*, 3(1):96–114, 2024.

[16] Shayma Jawad and Hanaa Mohsin Ahmed. Machine learning approaches to ransomware detection: A comprehensive review. *International Journal of Safety & Security Engineering*, 14(6), 2024.

[17] Mohammad Masum, Md Jobair Hossain Faruk, Hossain Shahriar, Kai Qian, Dan Lo, and Muhaiminul Islam Adnan. Ransomware classification and detection with machine learning algorithms. In *2022 IEEE 12th annual computing and communication workshop and conference (CCWC)*, pages 0316–0322. IEEE, 2022.

[18] Amjad Hussain, Ayesha Saadia, Musaed Alhussein, Ammara Gul, and Khursheed Aurangzeb. Enhancing ransomware defense: deep learning-based detection and family-wise classification of evolving threats. *PeerJ Computer Science*, 10:e2546, 2024.

[19] Ricardo Misael Ayala Molina, Sadegh Torabi, Khaled Sarieddine, Elias Bou-Harb, Nizar Bouguila, and Chadi Assi. On ransomware family attribution using pre-attack paranoia activities. *IEEE transactions on network and service management*, 19(1):19–36, 2021.

[20] Eduardo Berrueta, Daniel Morato, Eduardo Magaña, and Mikel Izal. A survey on detection techniques for cryptographic ransomware. *IEEE Access*, 7:144925–144944, 2019.

[21] Pavel Novak, Patrik Kaura, Vaclav Oujezsky, and Tomas Horvath. Ransomware file detection using hashes and machine learning. In *2023 15th International Congress on Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT)*, pages 107–110. IEEE, 2023.

[22] Umara Urooj, Bander Ali Saleh Al-Rimy, Anazida Zainal, Fuad A Ghaleb, and Murad A Rassam. Ransomware detection using the dynamic analysis and machine learning: A survey and research directions. *Applied Sciences*, 12(1):172, 2021.

[23] Benjamin Pesem, James Fairweather, and Thomas Pennington. Opcode memory analysis: A data-centric machine learning framework for early detection and attribution of ransomware. 2024.

[24] P Mohan Anand, PV Sai Charan, Hrushikesh Chunduri, and Sandeep K Shukla. Rtr-shield: Early detection of ransomware using registry and trap files. In *International Conference on Information Security Practice and Experience*, pages 209–229. Springer, 2023.

[25] Qian Chen, Sheikh Rabiul Islam, Henry Haswell, and Robert A Bridges. Automated ransomware behavior analysis: Pattern extraction and early detection. In *International Conference on Science of Cyber Security*, pages 199–214. Springer, 2019.

[26] Valeria Miranem, Giovanni Petrescu, Dominic Schelling, and Alejandro Vasiliev. Ransomware detection on windows systems using file system activities and a hybrid machine learning approach. 2024.

[27] Fei Tang, Boyang Ma, Jinku Li, Fengwei Zhang, Jipeng Su, and Jianfeng Ma. Ransomspector: An introspection-based approach to detect crypto ransomware. *Computers & Security*, 97:101997, 2020.

[28] Aakanksha Wiles, Floreda Colombo, and Rhyanna Mascorro. Ransomware detection using network traffic analysis and generative adversarial networks. 2024.

[29] Kumar Thummapudi, Palden Lama, and Rajendra V. Boppana. Detection of ransomware attacks using processor and disk usage data. *IEEE Access*, 11:51395–51407, 2023.

[30] Ali AlSabeh, Haidar Safa, Elias Bou-Harb, and Jorge Crichigno. Exploiting ransomware paranoia for execution prevention. In *ICC 2020-2020 IEEE International Conference on Communications (ICC)*, pages 1–6. IEEE, 2020.

[31] Or Ami, Yuval Elovici, and Danny Hendler. Ransomware prevention using application authentication-based file access control. In *Proceedings of the 33rd Annual ACM Symposium on Applied Computing*, pages 1610–1619, 2018.

[32] Kyungroul Lee, Kangbin Yim, and Jung Taek Seo. Ransomware prevention technique using key backup. *Concurrency and Computation: Practice and Experience*, 30(3):e4337, 2018.

[33] Suhyeon Lee, Huy Kang Kim, and Kyounggon Kim. Ransomware protection using the moving target defense perspective. *Computers & Electrical Engineering*, 78:288–299, 2019.

[34] Azka Wani and S Revathi. Ransomware protection in lot using software defined networking. *Int. J. Electr. Comput. Eng*, 10(3):3166–3175, 2020.

[35] Krzysztof Cabaj, Marcin Gregorczyk, and Wojciech Mazurczyk. Software-defined networking-based crypto ransomware detection using http traffic characteristics. *Computers & Electrical Engineering*, 66:353–368, 2018.

[36] Eugene Kolodenker, William Koch, Gianluca Stringhini, and Manuel Egele. Paybreak: Defense against cryptographic ransomware. In *Proceedings of the 2017 ACM on Asia conference on computer and communications security*, pages 599–611, 2017.

[37] Lorenzo Fernandez Maimo, Alberto Huertas Celdran, Angel L Perales Gomez, Felix J Garcia Clemente, James Weimer, and Insup Lee. Intelligent and dynamic ransomware spread detection and mitigation in integrated clinical environments. *Sensors*, 19(5):1114, 2019.

[38] Maxat Akbanov, Vassilios G Vassilakis, and Michael D Logothetis. Ransomware detection and mitigation using software-defined networking: The case of wannacry. *Computers & Electrical Engineering*, 76:111–121, 2019.

[39] Elpida Rouka, Celyn Birkinshaw, and Vassilios G Vassilakis. Sdn-based malware detection and mitigation: The case of expetr ransomware. In *2020 IEEE International Conference on Informatics, IoT, and Enabling Technologies (ICIoT)*, pages 150–155. IEEE, 2020.

[40] Simon R Davies, Richard Macfarlane, and William J Buchanan. Evaluation of live forensic techniques in ransomware attack mitigation. *Forensic Science International: Digital Investigation*, 33:300979, 2020.

[41] Farnood Faghihi and Mohammad Zulkernine. Ransomcare: Data-centric detection and mitigation against smartphone crypto-ransomware. *Computer Networks*, 191:108011, 2021.

[42] Abayomi Jegede, Ayotinde Fadele, Monday Onoja, Gilbert Aimufua, and Ismaila Jesse Mazadu. Trends and future directions in automated ransomware detection. *J. Comput. Soc. Inform*, 1(2):17–41, 2022.

[43] M Izham Jaya and Mohd Faizal Ab Razak. Dynamic ransomware detection for windows platform using machine learning classifiers. *JOIV: International Journal on Informatics Visualization*, 6(2-2):469–474, 2022.

[44] Atef Ibrahim, Usman Tariq, Tariq Ahamed Ahanger, Bilal Tariq, and Fayez Gebali. Retaliation against ransomware in cloud-enabled pureos system. *Mathematics*, 11(1):249, 2023.

[45] Jinting Zhu, Julian Jang-Jaccard, Amardeep Singh, Ian Welch, Harith Al-Sahaf, and Seyit Camtepe. A few-shot meta-learning based siamese neural network using entropy features for ransomware classification. *Computers & Security*, 117:102691, 2022.

[46] Jaehyuk Lee and Kyungroul Lee. A method for neutralizing entropy measurement-based ransomware detection technologies using encoding algorithms. *Entropy*, 24(2):239, 2022.

[47] Simon R Davies, Richard Macfarlane, and William J Buchanan. Comparison of entropy calculation methods for ransomware encrypted file identification. *Entropy*, 24(10):1503, 2022.

[48] Pranshu Bajpai and Richard Enbody. Attacking key management in ransomware. *IT Professional*, 22(2):21–27, 2020.

[49] Pranshu Bajpai and Richard Enbody. An empirical study of key generation in cryptographic ransomware. In *Proceedings of the International Conference on Cyber Security and Protection of Digital Services (Cyber Security'20)*, pages 1–8. IEEE, 2020.

[50] Fabrizio Cicala and Elisa Bertino. Analysis of encryption key generation in modern crypto ransomware. *IEEE Transactions on Dependable and Secure Computing*, 19(2):1239–1253, 2020.

[51] Kurt Friday, Elias Bou-Harb, and Jorge Crichigno. A learning methodology for line-rate ransomware mitigation with p4 switches. In *16th International Conference on Network and System Security (NSS'22)*, pages 120–139. Springer, 2022.

[52] Farnoush Manavi and Ali Hamzeh. A new method for ransomware detection based on pe header using convolutional neural networks. In *17th International ISC Conference on Information Security and Cryptology (ISCISC'20)*, pages 82–87. IEEE, 2020.

[53] Timothy McIntosh, A. S. M. Kayes, Yi-Ping Phoebe Chen, Alex Ng, and Paul Watters. Ransomware mitigation in the modern era: A comprehensive review, research challenges, and future directions. *ACM Computing Surveys*, 54(9):1–36, 2021.

[54] Kohei Tsunewaki, Tomotaka Kimura, and Jun Cheng. Lstm-based ransomware detection using api call information. In *IEEE International Conference on Consumer Electronics–Taiwan*, pages 211–212. IEEE, 2022.

[55] Faizan Ullah, Qaisar Javaid, Abdu Salam, Masood Ahmad, Nadeem Sarwar, Dilawar Shah, and Muhammad Abrar. Modified decision tree technique for ransomware detection at runtime through api calls. *Scientific Programming*, 2020(1):8845833, 2020.

[56] Qasem Abu Al-Haija and Abdulaziz A. Alsulami. High performance classification model to identify ransomware payments for heterogeneous bitcoin networks. *Electronics*, 10(17):2113, 2021.

[57] Suleiman Ali Alsaif. Machine learning-based ransomware classification of bitcoin transactions. *Applied Computational Intelligence and Soft Computing*, 2023(1):6274260, 2023.

[58] Niken Dwi Wahyu Cahyani and Hilal Hudan Nuha. Ransomware detection on bitcoin transactions using artificial neural network methods. In *Proceedings of the 9th International Conference on Information and Communication Technology (ICoICT'21)*, pages 1–5. IEEE, 2021.

[59] Ganapathi Nalinipriya, Maram Balajee, Chittibabu Priya, and Cristin Rajan. Ransomware recognition in blockchain network using water moth flame optimization-aware drnn. *Concurrency and Computation: Practice and Experience*, 34(19):e7047, 2022.

[60] Kai Wang, Jun Pang, Dingjie Chen, Yu Zhao, Dapeng Huang, Chen Chen, and Weili Han. A large-scale empirical analysis of ransomware activities in bitcoin. *ACM Transactions on the Web*, 16(2):1–29, 2021.