Ransomware Reloaded: Re-examining Its Trend, Research and Mitigation in the Era of Data Exfiltration

TIMOTHY MCINTOSH, RMIT University, Melbourne, Australia and Cyberoo Pty Ltd, Surrey Hills, Australia
TEO SUSNJAK, Massey University, Auckland, New Zealand
TONG LIU, Massey University, Auckland, New Zealand
DAN XU, ANZ Bank, Melbourne, Australia
PAUL WATTERS, Cyberstronomy Pty Ltd, Ballarat, Australia
DONGWEI LIU, Coles Group Ltd, Hawthorn East, Australia
YAQI HAO, Cyberoo Pty Ltd, Surrey Hills, Australia
ALEX NG, Federation University, Ballarat, Australia
MALKA HALGAMUGE, RMIT University, Melbourne, Australia

Ransomware has grown to be a dominant cybersecurity threat by exfiltrating, encrypting, or destroying valuable user data and causing numerous disruptions to victims. The severity of the ransomware endemic has generated research interest from both the academia and the industry. However, many studies held stereotypical assumptions about ransomware, used unverified, outdated, and limited self-collected ransomware samples, and did not consider government strategies, industry guidelines, or cyber intelligence. We observed that ransomware no longer exists simply as an executable file or limits to encrypting files (data loss); data exfiltration (data breach) is the new norm, espionage is an emerging theme, and the industry is shifting focus from technical advancements to cyber governance and resilience. We created a ransomware innovation adoption curve, critically evaluated 212 academic studies published during 2020 and 2023, and cross-verified them against various government strategies, industry reports, and cyber intelligence on ransomware. We concluded that many studies were becoming irrelevant to the contemporary ransomware reality and called for the redirection of ransomware research to align with the continuous ransomware evolution in the industry. We proposed to address data exfiltration as priority over data encryption, to consider ransomware in a business-practical manner, and recommended research collaboration with the industry.

CCS Concepts: • **Security and privacy** → *Trusted computing*; **Malware and its mitigation**; *Intrusion detection systems;*

Additional Key Words and Phrases: Ransomware, ransomware detection, ransomware defense, ransomware prevention

Authors' Contact Information: Timothy McIntosh (Corresponding author), RMIT University, Melbourne, Victoria, Australia and Cyberoo Pty Ltd, Surrey Hills, Victoria, Australia; e-mail: timothy.mcintosh@rmit.edu.au; Teo Susnjak, Massey University, Auckland, New Zealand; Tong Liu, Massey University, Auckland, New Zealand; Dan Xu, ANZ Bank, Melbourne, Victoria, Australia; Paul Watters, Cyberstronomy Pty Ltd, Ballarat, Victoria, Australia; Dongwei Liu, Coles Group Ltd, Hawthorn East, Victoria, Australia; Yaqi Hao, Cyberoo Pty Ltd, Surrey Hills, New South Wales, Australia; Alex Ng, Federation University, Ballarat, Victoria, Australia; Malka Halgamuge, RMIT University, Melbourne, Australia.

ACM 0360-0300/2024/10-ART18
https://doi.org/10.1145/3691340

ACM Reference Format:
Timothy McIntosh, Teo Susnjak, Tong Liu, Dan Xu, Paul Watters, Dongwei Liu, Yaqi Hao, Alex Ng, and Malka Halgamuge. 2024. Ransomware Reloaded: Re-examining Its Trend, Research and Mitigation in the Era of Data Exfiltration. *ACM Comput. Surv.* 57, 1, Article 18 (October 2024), 40 pages. https://doi.org/10.1145/3691340

1 Introduction

Ransomware, also known as the malware that extorts ransom payments since its conceptual inception in Reference [227], has to date caused major havoc for both organizations and individuals by disrupting users' exclusive access to data and extorting ransom payments [152]. Since taking off in 2010, ransomware originally appeared as "locker ransomware" to lock ***User Interfaces*** **(UIs)**, or as "crypto-ransomware" to stealthily encrypt user files, and its attacks used to be automated, opportunistic, and non-selective [72, 152]. However, aggressive and protective measures (e.g., better data backup and protection, network and ***Operating System*** **(OS)** hardening, adoption of cloud technology, sanctions and arrests of cyber-criminals and facilitators), taken by governments, law-enforcement agencies, cybersecurity vendors, and private enterprises, have prompted ransomware actors to evolve their strategies and business models [132]. The *Maze* ransomware was one of the first known variants to perform data exfiltration (data theft) to blackmail victims with data breach and privacy breach, and has been active since November 2019 or earlier.[1] Other novel attack vectors found in more recent ransomware variants include selective big-game hunting [75], human-operated ransomware,[2] ***Distributed Denial-Of-Service*** **(DDoS)** attacks,[3] privilege escalation against antivirus and ***Endpoint Detection and Response*** **(EDR)**,[4] and data breach amplification [75]. Some geopolitical events, e.g., the war between Russia and Ukraine since 2022, have prompted nation states to increasingly use ransomware with data theft extortion to frustrate attrition without necessarily prioritizing monetary extortion [163]. The IBM's X-Force Threat Intelligence Index 2023 indicates that although there was a minor decrease (4 percentage points) in the number of ransomware incidents from 2021 to 2022, it still represents a significant proportion of attacks [111]. Furthermore, the average time taken to carry out a ransomware attack decreased significantly, from two months in 2019 to less than four days in 2021 [111]. It is highly likely that those factors aforementioned will continue to make ransomware actors rethink their business models and result in gradual changes in ransomware to become more sophisticated, selective, and targeted.

The recurrent ransomware attacks and its extent of damages have prompted prolonged interest in both the industry and the academia to invest in ransomware research (Figure 1). Most of the earlier research from both the industry (e.g., Symantec[5] and Sophos[6]) and academia (e.g., References [73, 125]) focused on the notion of crypto-ransomware and its encryption mechanism, and its technical indicators of attacks, collected from either ransomware incidents or detection telemetry. Since the emergence of novel attack vectors that were no longer encryption-related, especially data

[1] https://www.kaspersky.com/resource-center/definitions/what-is-maze-ransomware

[2] https://www.microsoft.com/en-us/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/

[3] https://www.cloudflare.com/en-au/learning/ddos/ransom-ddos-attack/

[4] https://www.trendmicro.com/en_us/research/22/h/ransomware-actor-abuses-genshin-impact-anti-cheat-driver-to-kill-antivirus.html

[5] https://community.broadcom.com/symantecenterprise/communities/community-home/librarydocuments/viewdocument?DocumentKey=ee3df1cb-b129-4cf0-94e6-36bd616a93c8

[6] https://news.sophos.com/en-us/2015/12/17/the-current-state-of-ransomware-cryptowall/

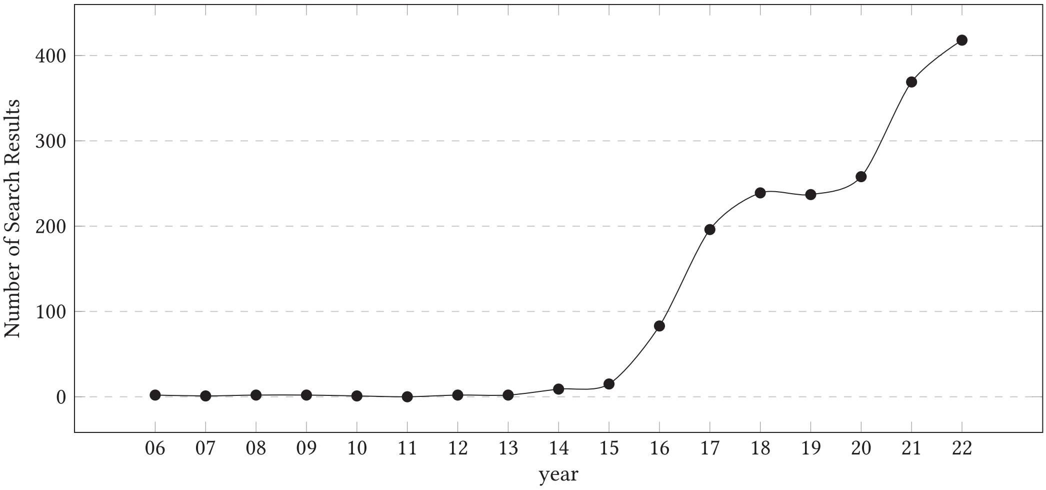

Fig. 1. The article counts with titles containing the keyword "ransomware" per year on Google Scholar.

exfiltration, industry research (e.g., References [75, 99, 110, 132, 161–163]) has branched out to consider other equally valuable data sources to analyze ransomware campaigns and groups, including ransomware business models, ransom negotiations, data protection, cyber intelligence, and organizational cybersecurity risk management [75, 99, 132, 163]. More industry experts have started to conclude and/or agree that ransomware mitigation is no longer solely a technical problem, but a business problem involving cybersecurity risk management against vulnerabilities, cyber intrusions, and data breach.

In our earlier survey [152] in February 2020, we correctly predicted that (1) ransomware with data extortion and other novel attack vectors would take off to surpass crypto-ransomware, and (2) recombinations of different ***Machine Learning*** **(ML)** algorithms with different self-constructed ransomware datasets would produce even more such studies, but their external validity (i.e., the extent to which the findings of studies could be generalized to real-world situations) could not be guaranteed. Nevertheless, we have been perplexed by the ongoing trend that the majority of academic research articles published between 2020 (*Maze* ransomware performing data exfiltration) and February 2023 (time of this survey) have continued to still focus merely on the opportunistic non-selective encryption behavior of earlier crypto-ransomware, have used ransomware samples mostly predating the data extortion phase, and have nearly all claimed their superiority in mitigating ransomware over other academic studies (and sometimes even over commercial antivirus), despite their vastly different methodologies. Very few of them considered ransomware with data extortion or other novel attack vectors. Very few realized that many larger organizations tend to deploy EDR (instead of antivirus with limited functionalities or heuristics), to sign up with ***Security Operations Centers*** **(SOCs)** with "eyes on glass" cybersecurity monitoring, and to implement comprehensive ***Governance, Risk & Compliance*** **(GRC)** to manage ransomware-related data breaches as business risks. It seems our predictions in Reference [152] that researchers would continue to focus on producing papers on data encryption, rather than transitioning to research on data exfiltration, have been confirmed. As a result, we have decided to conduct another survey on the most recent research in ransomware, to re-examine its latest trends, and the relevance of newly published studies on ransomware.

The major contributions of this survey include:

- ✓ We compiled the ransomware evolution history according to industry sources and applied *Rogers' Innovation Adoption Curve*. We demonstrated the shift from data encryption to data exfiltration and predicted the potential rise of destructive ransomware with espionage.
- ✓ We reviewed 212 academic studies (196 primary research studies and 16 surveys) published between 2020 and February 2023, cross-verifying them against government strategies, industry reports, and cyber intelligence. We found that most academic research has become less relevant in the era of ransomware double extortion with data exfiltration, highlighting the need for current research to prioritize this threat, and we called for realignment of ransomware academic research to industry trends.
- ✓ We proposed integrating ransomware risk management into organizational cybersecurity risk management, emphasizing the importance of government strategies, industry reports, guidelines, and cyber intelligence in ransomware research and mitigation.
- ✓ We discussed innovative research prospects, including the role of generative AI, focusing on practical and regulatory-compliant approaches to address the evolving ransomware threat landscape.

The rest of the survey is organized as follows: Section 2 compares our survey with other ransomware surveys recently published, especially in the areas of coverage of new ransomware attack vectors and information. Section 3 presents the factors that have motivated the research that has led to this survey. Section 4 introduces the new ransomware threat landscape with data exfiltration. Section 5 demonstrates the misalignment of existing academic ransomware research with the current ransomware threat landscape. Section 6 lists our survey insights, discussions, and reflections. Section 7 concludes the survey and suggests future research directions.

2 Related Work

Sixteen surveys [16, 23, 27, 47, 50, 52, 89, 106, 115, 117, 152, 169, 180, 188, 204, 213] between 2020 and February 2023 were found to have extensively surveyed other primary ransomware research and were listed in Table 1. We observed that the topics covered in a research survey paper were dependent on the availability, quality, and scope of the primary research articles that had been surveyed. Therefore, it is important for ransomware surveys to carefully select the primary research articles that will be included in their survey, taking into consideration the latest ransomware development and evolution. Although all surveys covered the topic of crypto-ransomware, we only observed three surveys [115, 152, 180] that covered the topic of data exfiltration. Among which, Reference [152] correctly predicted the diminishing of crypto-ransomware and the uprising of ransomware with data exfiltration, but did not predict the transition from attacking personal users to businesses and organizations. References [115, 180] both stated the emerging problem of data exfiltration in brief, but did not explore it in depth, nor predicted its trend to overtake data encryption. Of other studies [16, 23, 27, 47, 50, 52, 89, 106, 117, 169, 188, 204, 213] that focused on crypto-ransomware and did not explore ransomware data exfiltration, Reference [16] only summarized the range of primary research they surveyed without critiquing on research gap or predict future trends or research directions, whereas Reference [117] recommended mitigation strategies against ransomware, but the recommendations were based on common knowledge and not supported by evidence in their survey.

To the best of our knowledge, this survey is innovative in the following areas, not seen in previous ransomware surveys:

Table 1. Comparison of Different Studies on Ransomware Surveys between 2020 and February 2023 and against This Survey

Ref.	Date	Core features covered		Existing research gap critiqued	Future trends reasonably predicted	Future research direction suggested and justified	Regulatory compliance considerations	Generative AI in cybersecurity
		Encryption	Exfiltration					
[27]	2020 Q1	✓		△				
[52]	2020 Q1	✓		△				
[50]	2020 Q1	✓		✓	△	✓		
[106]	2020 Q2	△		△	△			
[169]	2020 Q4	✓		✓	△	△		
[89]	2020 Q4	✓		✓	△	✓		
[188]	2021 Q1	✓		△		△		
[152]	2021 Q2	✓	✓	✓	✓	✓		
[47]	2021 Q3	✓		✓		✓		
[117]	2021 Q4	✓		△	△	△		
[213]	2021 Q4	✓		△		△		
[180]	2021 Q4	✓	✓	△	✓	△		
[23]	2022 Q1	✓		✓				
[16]	2022 Q2	✓						
[115]	2022 Q3	✓	✓	△	×	△		
[204]	2022 Q3	✓		×	△	×		
This survey	2023 Q1	✓	✓	✓	✓	✓	✓	✓

(✓: Done Extensively; △: Attempted but Can Be Improved).

- We not only examined what was presented in the primary research about ransomware studies, but also cross-verified them with the latest information from the contemporary ransomware landscape.
- We considered the innovation, adoption, and obsolescence of different ransomware attack techniques and mapped them to an approximate timeline.
- We referenced government and industry research from more reliable sources to supplement information from academic studies.
- We included regulatory compliance considerations, emphasizing how proposed ransomware mitigation solutions align with evolving privacy and data breach laws.
- We discussed the role of generative AI in cybersecurity, highlighting its potential for innovative ransomware mitigation strategies.

We believe this survey will provide new and valuable information to future ransomware research by offering a comprehensive and up-to-date analysis that addresses current deficiencies and explores future directions.

3 Research Motivation

In this section, the background information to motivate this survey is presented. In our previous survey [152], we noticed that many academic studies (1) used "ransomware" and "crypto-ransomware" interchangeably; (2) failed to define benign or ransomware-like activities; (3) misused terminologies of mitigation strategies; and (4) did not effectively compare and evaluate the effectiveness of their studies. Since our previous survey, we have noticed even more common issues with more recent studies surveyed.

3.1 Stereotypical Assumptions of Ransomware Attack Strategies

Since *Maze* ransomware in 2019, there have been many government strategies and industry reports or guidelines published on ransomware research and its mitigation, most of which have noticed data exfiltration as part of the new ransomware tactics and warned the public to be prepared. In July 2020, Hiscox Insurance (UK) appeared to be the first industry report surveyed by us to alert that the combination of file encryption and data exfiltration via a watering-hole technique were netting increased success by ransomware attacks.[7] In September 2020, the ***Cybersecurity***

[7] https://www.hiscox.co.uk/sites/uk/files/documents/2020-07/20816-Data-exflitration-guide-final.pdf

Table 2. Common Stereotypical Assumptions on Ransomware

Misconception about ransomware	The new reality
Ransomware only performs file encryption, and their attacks are often aggressive, automated, and non-selective (e.g., References [112, 114, 115, 147, 236]).	Newer ransomware prefers data exfiltration to file encryption, and the attacks are more selective, human-operated, and stealthy [72, 76, 163].
Data attacked by ransomware are only stored in files on hard drives of personal computers, not in cloud or databases (e.g., References [35, 37, 93, 97, 108, 164, 204, 237]).	Ransomware could encrypt or exfiltrate data from cloud storage or databases, without incurring local file system activities [76, 111, 163]. Certain direct disk operations can bypass IRP checks.[1]
Entropy is a reliable indicator of file encryption (e.g., References [79, 136, 236]).	Ransomware can perform partial file encryption to minimize file entropy changes or apply encoding (e.g., Base64) to manipulate entropy values [150].
Ransomware only generates unique encryption keys in the OS memory, not obtained from its C&C centers (e.g., References [39, 40, 70]).	Ransomware could obtain unique encryption keys directly from its C&C [91] or does not require encryption keys if only performing data exfiltration.
Ransomware only exists as executable files on the storage (e.g., References [144, 211, 212]).	Ransomware can exist as fileless ransomware or purely as intrusion activities of human-operated ransomware [152, 163].
Ransomware only extorts bitcoin payments (e.g., References [11, 26, 62, 172, 215]).	Ransomware such as *Sodinokibi* and *Darkside* accepted Monero to minimize payment traceability.

[1] https://learn.microsoft.com/en-us/windows-hardware/drivers/ifs/bypassio

and Infrastructure Security Agency **(CISA)** of the USA government warned that, occasionally, nefarious individuals may exploit their granted access to steal data and then coerce the victim into paying a ransom by threatening to disclose the information publicly, thereby attempting to extract more money from them and compel them to comply [76]. However, most academic studies after the emergence of *Maze* ransomware performing data exfiltration still appeared to make the stereotypical assumptions on ransomware, as listed in Table 2.

We believe in the importance of keeping up with the constantly changing and advancing nature of ransomware, and that any research or analysis conducted on ransomware should strive to incorporate the most recent developments and characteristics of ransomware. By doing so, researchers and analysts can gain a more comprehensive and up-to-date understanding of the various tactics and techniques employed by ransomware and keep pace with the evolving nature of ransomware and remain better prepared to respond to the ever-changing threat landscape.

3.2 Usage of Unverified, Outdated, and Limited Self-collected Ransomware Samples or Self-constructed Datasets

We were concerned with the frequently seen usage of unverified, outdated, and limited self-collected ransomware samples or self-constructed datasets by some studies, without their further assessment on the validity of their samples or datasets. The difficulty of collecting ransomware samples has been acknowledged, that there is no universal ransomware sample datasets that can represent all ransomware variants, not to say that it is often difficult or impossible to collect samples of certain ransomware variants that do not exist as executable files [152]. Nonetheless, many researchers simply decided to either self-collect ransomware samples from any storage platforms (such as VirusTotal, VirusShare) they could get to (e.g., References [137, 159, 236]), used self-constructed datasets of ransomware access patterns (e.g., References [78, 79, 104]), or resorted to simulations (e.g., References [4, 139, 140, 171, 179]). Many studies claimed to have been evaluated against *WannaCry* (May 2017), *NotPetya* (June 2017), and *GandCrab* (January 2018), possibly due to them causing some of the most notable crypto-ransomware attacks. The average age of ransomware samples used by many studies ranged between three to four years old. However, in Reference [236], published in 2022, authors used *TeslaCrypt* (early 2015) and *Cerber* (early 2016).

Table 3. A List of Anti-ransomware Modules by Some Commercial Antivirus Products

Security Vendor and Product	Anti-ransomware Module
AVG	Ransomware Protection
Avira	Anti-ransomware
Bitdefender	Ransomware Remediation
ESET	PROTECT Advanced
Kaspersky	Anti-ransomware
Microsoft Windows Defender	Controlled Folder Access
Trend Micro	Folder Shield

In Reference [104], authors used seven ransomware variants between 2015 and 2021 to construct access patterns to storage devices. Six of those seven variants were crypto-ransomware only, and it was unknown whether their *Darkside* sample was able to exfiltrate data, given that data exfiltration was never mentioned in their study.

According to Reference [184], a study should strive to achieve both internal validity (the extent to which a study accurately measures the intended variables) and external validity (the extent to which the results of a study can be generalized to the larger population). Using historical ransomware samples could be a useful method for verifying newer, general-purpose ML data-mining algorithms that can detect old, current, and future ransomware variants. However, to date, no such algorithm has been developed. Many authors have only generated a feature matrix and applied ML algorithms to it without specifically addressing the problem of detecting ransomware variants. Given that some ransomware groups have ceased operation and that newer ransomware variants now employ very different attack models, using outdated ransomware samples or datasets could jeopardize both the internal validity (whether there is a causal relationship between observed features and ransomware behaviors) and external validity (whether the result of the study applies to all the active ransomware attacks in the wild) of those studies.

3.3 Compartmentalized View of Commercial Antivirus Products

Many recent ransomware studies (e.g., References [8, 9, 20, 21, 47, 159, 190, 212]) appeared to have formed compartmentalized view of commercial antivirus products before claiming their superiority over commercial antivirus. Some studies (e.g., References [20, 21, 190, 212]) appeared to have considered antivirus products as simply static scanners, or they might not have adequately considered the convergent and synergistic effect of multiple technologies (i.e., malware scanner, real-time protection with behavioral analysis and advanced heuristics, firewall, anti-ransomware modules, kernel protection, sandboxing, and cloud-based analysis). If a newly crafted ransomware variant is not detected as positive by VirusTotal, a website that only performs static analysis based on the hash values of submitted files, then it simply means the scanning engines of participating antivirus products cannot recognize the sample via static analysis. It does not mean the ransomware will not be thwarted by antivirus during runtime with other technologies. Some studies (e.g., References [20, 21, 47]) seemed to be unaware of existing anti-ransomware modules by antivirus vendors (Table 3). In References [151, 153], we evaluated the effects of those anti-ransomware modules, which were able to fully block file encryption activities of simulated ransomware encryption activities against files in their protected folders. Some studies (e.g., References [9, 159]) did not realize that many cloud storage providers (e.g., Microsoft OneDrive, Amazon AWS) implement cloud-based crypto-ransomware detection of likely encryption activities, with file version control and reversal. Some studies (e.g., References [8, 9]) decided to take antivirus labels as ground truth by labeling their collected ransomware samples the same as their chosen antivirus did, whereas different antivirus products can label the same ransomware samples differently [56, 57]. Research developed with compartmentalized view of commercial antivirus products is likely to have internal bias against antivirus products and thus may not provide a comprehensive and objective comparison of the effectiveness and limitations of their own anti-ransomware proposals in real-world scenarios.

3.4 No Consideration of Government Strategies, Industry Guidelines, or Cyber Intelligence

Many recent studies we surveyed had not considered government strategies, industry guidelines, or cyber intelligence, apart from a few socioeconomic studies (e.g., References [72, 98, 135, 160, 228]). In our survey, we thoroughly examined government strategies (e.g., References [76, 175, 176]), which were often compiled by national cyber departments equipped with some of the best experts in the field of cybersecurity. Such strategies have proven success in protecting critical infrastructure, sensitive information, and citizens' privacy. For example, the Australian Government's Ransomware Action Plan provided a comprehensive framework for prevention, detection, and response to ransomware attacks. We also considered guidelines and standards developed by reputable industry organizations such as the ***International Organization for Standardization* (ISO),** the ***National Institute of Standards and Technology*** **(NIST)**, and the ***Information Systems Audit and Control Association*** **(ISACA)**. Their guidelines were based on industry best practices, were frequently updated to reflect changes in the threat landscape, and were subject to rigorous review and validation processes. The NIST Cybersecurity Framework, for instance, offered a robust set of guidelines that helps organizations manage and reduce cybersecurity risks. Additionally, we integrated cyber intelligence from reliable sources, which were based on accurate and diverse information analyzed by experienced analysts. Cyber intelligence could help organizations and governments identify, prevent, and respond to fast-emerging cyber threats effectively. For example, in mid-2022, *CyberCX Intelligence* was one of the first to report the adoption of (1) the ***InterPlanetary File System*** **(IPFS)** by ransomware; (2) the availability of "Command and Control as a Service," allowing threat actors to inject any payload into any device with local code execution; and (3) the trend of data breach amplification, when *Alphv* and *Lockbit* established clearnet sites with search functions for "customers" to selectively "shop" for stolen data. Our additional considerations of government strategies, industry guidelines, and cyber intelligence provided us with a comprehensive view of ransomware development and its mitigation strategies, allowing us to identify trends, best practices, and areas needing further research and to offer a more holistic understanding of the ransomware landscape.

4 Data Exfiltration: The New Ransomware Reality

In this section, we present the new ransomware reality in the new era of double extortion with data exfiltration. We have collated the information using multiple sources, including government strategies, industry insights, and cyber intelligence.

4.1 Technical Background and Evolution of Ransomware

Ransomware has undergone significant evolution since its inception, reshaping its definition and impact in ways not fully captured by previous surveys. This comprehensive outline of ransomware's evolution highlights its dynamic nature and the continuous adaptation required in defensive strategies, and understanding such stages is crucial for grasping the current and future threat landscape. The development of ransomware can be categorized into three major stages:

(1) **Crypto-ransomware:** Initially, ransomware primarily involved encrypting the victim's files and demanding a ransom for the decryption key [155]. This form, known as

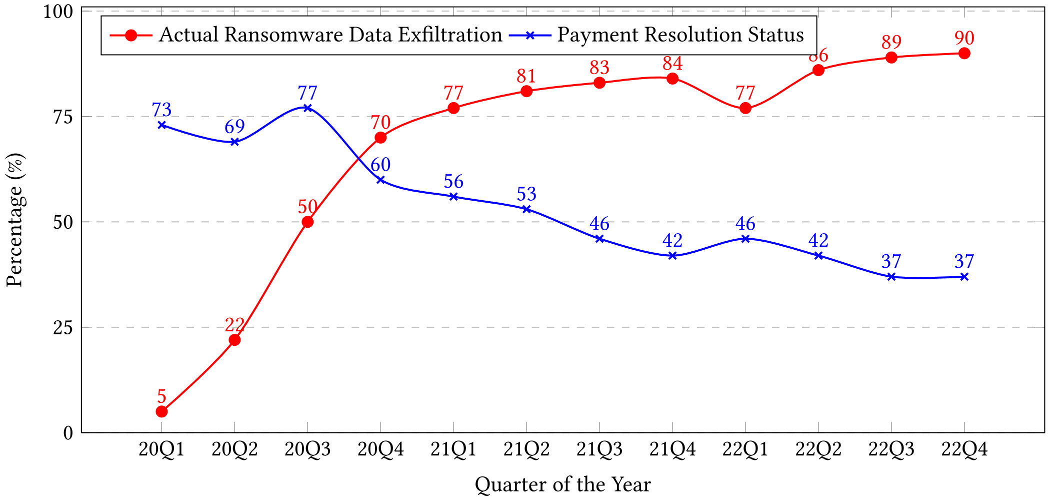

Fig. 2. Trend of ransomware data exfiltration and payment resolution status.

crypto-ransomware, threatened *data loss* if the ransom was not paid, exemplified by notorious attacks such as CryptoLocker and WannaCry [150].

(2) **Data Exfiltration Ransomware:** As defensive measures against file encryption improved, attackers adapted by incorporating data theft into their operations. Data exfiltration ransomware may or may not encrypt files, but exfiltrates sensitive data, threatening to release it publicly or sell it unless the ransom is paid to suppress such *data breach* [151]. This evolution introduced a dual-threat model, significantly increasing the leverage over victims, as seen in attacks by groups like Maze and REvil [152].

(3) **Destructive Ransomware with Espionage:** The latest and most sophisticated form of ransomware includes elements of espionage, where attackers maintain long-term access to compromised systems, conducting surveillance and data gathering [153, 154]. This form poses a severe threat by combining financial extortion with potential state-sponsored espionage, such as Bronze Starlight and Colorful Panda, projecting a future where ransomware is used for cyber warfare and long-term strategic gains [154].

4.2 Percentage of Ransomware with Data Exfiltration

We collated data from various sources, including government strategies [76, 175, 176], industry reports[8] [110, 111, 132, 161–163], and cyber intelligence [75] and constructed Figure 2 to illustrate the trend (changes in percentage) of ransomware data exfiltration and payments collected. In the past four years, despite a sharp increase in the percentage of ransomware performing data exfiltration (data theft), from 5% in Q1 of 2020 to 90% in Q4 of 2022, there has been a significant decrease in the tendency of ransomware victims to pay a ransom. The percentage of victims who paid a ransom dropped from 85% in Q1 of 2019 to 37% in Q4 of 2022. The ongoing fight against ransomware is not expected to be resolved in the next quarter. However, if the current trend persists, the frequency and severity of ransomware could be vastly different in a few years.

There were no available, consistent, and intact data on the percentage of ransomware still performing data encryption over time. However, if a ransomware attack significantly disrupts large corporations, then it can draw the attention of law enforcement and even trigger geopolitical

[8] https://www.coveware.com/ransomware-quarterly-reports

responses from the attacker's home country. However, data theft without encryption does not cause operational disruptions but enables the threat actor to blackmail the victim. Given that (1) valuable data must be exfiltrated first before any encryption, (2) most organizations now have comprehensive data backups, and (3) victims are becoming less likely to pay ransom, we believe it is fair to conclude that even if ransomware still performs data encryption, it is becoming less damaging and less relevant during ransomware attack incident management and response.

Other notable observations of ransomware trends over time by Coveware™ include:

- **2020 Q1:** Ransomware such as *Sodinokibi* attacked IT ***Managed Service Providers*** **(MSPs)**, by using ***Remote Monitoring and Management*** **(RMM)** to deploy their ransomware payload. "Work From Home" network configurations during COVID-19 resulted in increased attack surface and more ransomware attacks.[9]
- **2020 Q2:** Increased ***Remote Desktop Protocol*** **(RDP)** intrusions and email phishing as attack vectors; 30% of all ransomware incidents involved threats of releasing stolen data, while in 22% of the cases, the data were actually stolen.[10]
- **2020 Q3:** Stolen data from victims were held by multiple parties and were not credibly destroyed by cybercriminals even after receiving ransom payments.[11]
- **2020 Q4:** Fewer companies pay data exfiltration extortion demands, resulting in overall drop in ransomware payments. Data destruction instead of data encryption, after data exfiltration, is taking off to become more common.[12]
- **2021 Q1:** Ransomware actors were increasingly defaulting on their data promise of destroying stolen data after receiving payments, making paying ransom less attractive to attempt to suppress a data leak.[13]
- **2021 Q2:** Underwriting standards for cyber insurance against ransomware are hardening, requiring organizational due diligence, such as MFA, EDR, and network segmentation. RaaS increasingly targeted Linux and attracted attention of global governments.[14]
- **2021 Q3:** Ransomware shifted to target mid-sized organizations. Governments and law-enforcement agencies are taking actions, increasing the cost to ransomware actors.[15]
- **2021 Q4:** The USA government agencies were required to implement "zero trust" against ransomware. Ransomware groups were refining their tactics due to increased pressure from law enforcement.[16]
- **2022 Q1:** *Conti* ransomware group pledged their support for the Russian government during the war between Ukraine and Russia and threatened "enemy states" of Russia with ransomware espionage without monetary extortion.[17]
- **2022 Q2:** Ransomware threat actors were shifting their focus from "big game" hunting to "big shame" hunting and attacked Windows, Linux, and VMWare ESXi platforms.[18]

[9] https://www.coveware.com/blog/q1-2020-ransomware-marketplace-report

[10] https://www.coveware.com/blog/q2-2020-ransomware-marketplace-report

[11] https://www.coveware.com/blog/q3-2020-ransomware-marketplace-report

[12] https://www.coveware.com/blog/2021/2/18/q4-doxxing-victim-trends-industrial-sector-emerges-as-primary-ransom-non-payor

[13] https://www.coveware.com/blog/ransomware-attack-vectors-shift-as-new-software-vulnerability-exploits-abound

[14] https://www.coveware.com/blog/2021/7/23/q2-ransom-payment-amounts-decline-as-ransomware-becomes-a-national-security-priority

[15] https://www.coveware.com/blog/2021/10/20/ransomware-attacks-continue-as-pressure-mounts

[16] https://www.coveware.com/blog/2022/2/2/law-enforcement-pressure-forces-ransomware-groups-to-refine-tactics-in-q4-2021

[17] https://www.coveware.com/blog/2022/3/25/how-the-russianukraine-war-may-lead-to-an-explosion-in-ransomware-attacks

[18] https://www.coveware.com/blog/2022/5/3/ransomware-threat-actors-pivot-from-big-game-to-big-shame-hunting

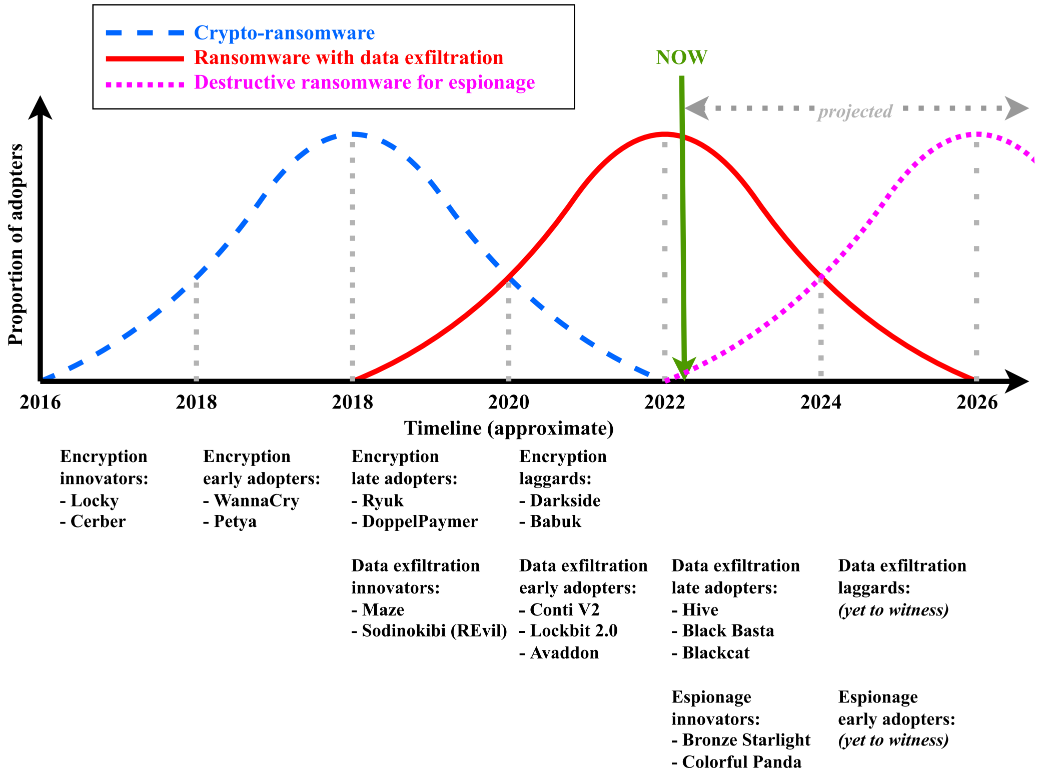

Fig. 3. Ransomware innovation adoption curve.

- **2022 Q3:** Increased level of re-extortion (i.e., the same adversary who extorted money from companies demanded payment again after a few days or weeks, even though the initial agreed-upon amount had been paid). Data destruction during ransomware attacks continued to occur, whether deliberately or accidentally.[19]
- **2022 Q4:** Record-low amounts of ransomware payments were attributed to better security measures and data backups and less victims paying ransom.[20]

4.3 Applying Rogers' Innovation Adoption Curve to Ransomware

Based on our observations, research, and understanding of ransomware, we applied the *Rogers' Innovation Diffusion theory* [220] (named after Everett Rogers) and created a double-curved *Ransomware Innovation Adoption Curve* (Figure 3) to illustrate the evolution journey of crypto-ransomware and ransomware with data exfiltration. The innovation adoption curve consists of four stages for each type of ransomware attack vector:

- **Innovators:** At this stage, the attack vector is new and most victims are unprepared. Consequently, the attack success rate is high. This stage was exemplified by the emergence of crypto-ransomware, where encryption-based attacks caught many organizations off-guard.

[19] https://www.coveware.com/blog/2022/10/26/q3-2022-quarterly-report

[20] https://www.coveware.com/blog/2023/1/19/improved-security-and-backups-result-in-record-low-number-of-ransomware-payments

Innovators include early ransomware variants such as CryptoLocker and WannaCry, which caused widespread damage due to the lack of effective countermeasures.

- **Early Adopters:** Motivated by the success of the innovators, other ransomware actors begin to copy and improve the attack vector. The number of successful attacks increases as more attackers join the crime. This stage also sees potential targets starting to implement initial countermeasures. The early adoption of data exfiltration techniques by ransomware groups like Maze represents this stage, where attackers began to combine data theft with encryption to enhance their leverage over victims.
- **Late Adopters:** As many potential targets proactively take countermeasures to mitigate the risk of this type of attack, attackers are forced to evolve their strategies. However, the attack success rate starts to drop. Currently, ransomware with data exfiltration is in this stage as organizations improve their defenses against both encryption and data theft. The plateau in the percentage of ransomware attacks involving data exfiltration indicates that this tactic is facing increased resistance.
- **Laggards:** When most potential targets have adopted mature mitigation strategies against this type of attack, many attackers choose to abandon this strategy and switch to other vectors. However, some attackers may still continue to search for unprepared victims, leading to a continued drop in the attack success rate. Crypto-ransomware is currently in this stage, as evidenced by the reduced impact and success of purely encryption-based attacks. This is supported by the increasing number of victims relying on backups to restore data without paying ransoms.

We believe crypto-ransomware attackers or groups are in the “laggard” stage, as an increasing number of their victims have proper backups to restore encrypted data without paying the ransom. This is likely to be supported by the fact that the *Darkside* ransomware group have had to frequently resort to “re-extortion,” possibly due to financial strains because of less successful attacks. However, we are likely to have just entered the “late adoption” stage of ransomware with data exfiltration, because the percentage of ransomware performing data exfiltration is known to have plateaued, and fewer and fewer victims are refusing to pay ransom. It is probable that we have recently transitioned into the “innovator” stage of destructive ransomware for espionage, as at least two groups (*Bronze Starlight* and *Colorful Panda*), likely state-sponsored, were found to have used ransomware for political espionage on military industrial complex enterprises and public institutions in several countries. We are yet to witness when ransomware with data exfiltration is likely to subside and when destructive ransomware for espionage will take off.

4.4 Potential Evolution

While it is difficult to predict the exact future trends of ransomware attacks, based on past patterns and emerging technologies, we have predicted some potential scenarios:

- **More Targeted Attacks:** Ransomware attackers may shift from mass attacks to more targeted attacks, focusing on specific organizations (e.g., critical infrastructures or organizations known to have weak cyber defense) or individuals (e.g., high-net-worth individuals, celebrities, or high-ranking politicians) with more valuable or sensitive data. This could involve using advanced reconnaissance techniques to gather information on the target and tailor the attack to their specific vulnerabilities.
- **Greater Focus on Data Theft:** Ransomware attackers have already started focusing more on stealing data in addition to encrypting it (and will continue to do so), using the threat of data exposure as a leverage to increase the ransom demand.

- **More Sophisticated Exfiltration and Encryption Methods:** Ransomware attackers may start using more sophisticated exfiltration and encryption methods to make it even harder for victims to notice their data theft or to recover their data without paying the ransom. It is entirely possible that ransomware criminals could selectively exfiltrate sensitive data and encrypt what is not easily replaceable but not as sensitive.
- **Data Breach Amplification:** Ransomware attackers with stolen data could auction the data for the highest price and attract buyers that may be the competitors of the victims or other fraudsters.
- **Multi-purpose Extortion:** Ransomware can be used more frequently for espionage based on political or religious ideologies, without necessarily extorting monetary payments.
- **Increasing Use of AI and Automation:** Ransomware attackers may start using **artificial intelligence (AI)** and automation to identify vulnerabilities and deploy attacks more quickly and efficiently. This could make it harder for organizations to detect and respond to attacks.

To mitigate the impact of these potential trends, organizations should continue to prioritize their cybersecurity efforts, including regular backups of critical data, employee training, and proactive vulnerability assessments, patch management, and intrusion detection and prevention.

5 The Misalignment of Existing Ransomware Research with the Current Ransomware Threat Landscape

In this section, we align the progress of ransomware evolution in the real world with our constructed timeline of academic ransomware studies to demonstrate the apparent misalignment of them with the current ransomware threat landscape. While our previous survey extensively analyzed attack methods and defense mechanisms, the focus of this current survey is to highlight the misalignment between academic research on ransomware and the practical evolution of ransomware in the industry.

5.1 Definitions of Five Categories

In this survey, the ransomware research articles surveyed by us are classified into the following five categories:

- **Socioeconomics:** studies to explore the socioeconomic aspects of ransomware attacks, such as people's behaviors and cyber hygiene, or organizational management decisions on ransomware risk management, without dealing with the technical aspects of ransomware or its mitigation.
- **Concept:** studies to investigate or analysis of a particular idea or concept that could shape the future of ransomware evolution, but has not been realized yet.
- **Investigation:** studies to investigate the technical aspects of ransomware, such as the encryption mechanism, its source code, or its payment traces on the blockchain network without proposing how to mitigate ransomware.
- **Mitigation:** studies to claim to be able to prevent, defend against, or detect ransomware or its attack indicators.
- **Survey:** studies to summarize and/or critique the findings of other existing primary research on ransomware.

While further subcategories could theoretically provide more granular insights into attack strategies and models, our survey aims to redirect focus on the broader issue of misalignment, especially when proper file backups with proper version controls could sufficiently mitigate file encryption by ransomware, and mature simple industry solutions are now prevalent (e.g., Table 3 and Microsoft OneDrive). We believe the existing five categories sufficiently capture the scope of

Table 4. Academic Article Selection Criteria

Criterion	Condition
Article date (revision, submission, or publication)	Available, and between January 2020–February 2023
Search Engine availability	Available in *Google Scholar* search results
Excluded publication types	Excluding citations, patents, textbooks, and communication articles
Language	English only
Title	Contains "ransomware"
Peer review	Declared as peer-reviewed only
Quality indicators (content)	Clarity and organization. Presence of comprehensive literature review. Properly explained methodology. No major ethical concerns.
Quality indicators (presentation)	No mismatched references, major grammar, or spelling mistakes

research and highlight areas needing redirection without delving into redundant details already covered extensively in prior ransomware surveys.

5.2 Article Selection and Evaluation Criteria

Because our previous survey [152] was produced in February 2020, shortly after the emergence of *Maze* ransomware performing data exfiltration, we decided to review only ransomware studies published since 2020 to review the validity and relevance of those studies and whether they would consider data exfiltration. To best determine the date of each article, we used its revision date whenever possible. If its revision date was unavailable, or no revision was required, then we used its initial submission date. If neither the revision nor the submission date was available, then we used its date of publication or its conference date. A full list of article selection criteria is in Table 4. We collected our academic studies using the following detailed methodology:

5.2.1 Search Strategy. We performed comprehensive searches using *Google Scholar*, targeting articles containing the term "ransomware" in their titles. We refined our searches to include articles published or revised between January 2020 and February 2023, corresponding to the period of transition away from crypto-ransomware. The search results were filtered to exclude citations, patents, textbooks, and communication articles, focusing solely on peer-reviewed papers.

5.2.2 Selection Process. The selection process involved multiple stages:

(1) **Initial Screening:** Titles and abstracts of the search results were screened for relevance. Only articles explicitly related to ransomware were retained.
(2) **Full-text Review:** The full texts of the retained articles were reviewed to ensure they met the inclusion criteria outlined in Table 4.
(3) **Feature Identification:** Each selected article was examined to identify the presence of core and optional features relevant to ransomware, such as encryption, data exfiltration, ML applications, entropy analysis, API/IRP activities, DDoS, and other optional features.

5.2.3 Feature Markers. After initial selection, the articles were identified with the following feature markers, selected according to the survey results of References [152, 180]:

- **core features:**
  - **encryption:** Does the study recognize and investigate crypto-ransomware?
  - **exfiltration:** Does the study recognize and investigate ransomware preforming data exfiltration?
- **ML:** Does the study use or promote ML to investigate or mitigate ransomware?
- **optional features:**
  - **entropy:** Does the study consider or propose file entropy analysis to investigate or mitigate ransomware?

- **API/IRP:** Does the study consider or propose ***Application Program Interfaces*** **(APIs)** of the payload or its file system activities, e.g., ***Input/output Request Packets*** **(IRPs)**, to investigate or mitigate ransomware?
- **DDoS:** Does the study mention ransomware performing DDoS as one of the extortion methods, which is currently being trialed by *Alphv* and *Lockbit* groups?
- **other features:** Does the study investigate optional features of ransomware that are not determinant nor essential components of its attack mechanisms, such as usage of particular network protocols, transactions on the bitcoin blockchain, or display of ransom messages on the client computers?

In Tables 5–8, if a ransomware feature is explicitly covered in an article (indicated by the article reference in the first column), as assessed by us, then the symbol "✓" is used. If the feature is implicitly implied (i.e., an article does not discuss file encryption by ransomware but uses only crypto-ransomware samples), then the symbol "△" is used.

5.3 Performance Metric: Completeness of Core Features Covered

To objectively compare the surveyed publications, we propose a performance metric called "Completeness of Core Features Covered," which assesses the presence of two essential ransomware features: *encryption* and *exfiltration*. A proper ransomware study should comprehensively address both features to reflect the latest trends and understand the full scope of ransomware threats. A score of 1 if the feature is explicitly present (✓), 0.5 if implicitly present (△), and 0 if absent. The scores for each feature are summed to provide an overall completeness score ranging from 0 to 2 for each publication, from a minimum of 0 (no coverage of core features) to a maximum of 2 (full coverage of both core features). Focusing solely on these core features ensures the metric's universality across all ransomware studies, as these features are fundamental to modern ransomware's operation and impact. By contrast, optional features may not be universally applicable or necessary for a foundational understanding of ransomware. Not fully addressing these core features suggests that the authors might be relying on outdated research paradigms without critically re-examining the evolving ransomware landscape. Given the volume of articles reviewed, this metric remains simple and concise, facilitating straightforward comparison and evaluation.

5.4 Different Types of Ransomware Studies

In contrast to our previous survey that delved into detailed attack methods and mitigation strategies, this survey categorizes existing ransomware research to emphasize the gap between academic studies and real-world ransomware evolution. The 196 primary research ransomware studies are critiqued as follows, grouped into four categories, based on their research perspective in ransomware:

5.4.1 Socioeconomic Studies. Twenty-five studies [26, 36, 43–45, 48, 49, 64, 65, 71, 72, 86, 98, 100, 102, 107, 135, 143, 158, 160, 168, 173, 191, 215, 225, 226, 228, 232] were surveyed to have studied the socioeconomic aspects of ransomware and its attacks and were listed in Table 5 in the Supplementary Material. Of which, References [36, 43, 135, 143, 160, 168] mentioned ransomware performing data exfiltration. Reference [135] observed the trend of increased ransomware attacks since COVID-19 and attributed it to the increased attack surface due to working-from-home arrangements, but most of its recommendations were technical in nature and generic to any cybersecurity threats. Reference [143] mentioned the data exfiltration by *Darkside* ransomware but only covered automated attacks via OTA updates on the platform of connected vehicles. Reference [36] modeled the risk of ransomware among organizations and suggested that refusing to pay the ransom overall helped victims to recover from ransomware attacks but only tested their hypothesis on simulated case studies. Reference [160] mentioned ransomware data exfiltration, but their quantitative study used regression analysis to examine the relationship between ransom amounts requested, payments made, and financial losses incurred. References [43, 168] both delved into cyber insurance against ransomware but did not mention the increased hardening of their underwriting standards, including requiring increased level of organizational due diligence, and did not note that more insured ransomware victims had been denied payouts.[21] References [26, 158, 215] all wrongfully assumed that ransomware only took bitcoin as payments. Reference [45] proposed to use web search logs to study ransomware attacks, which was reactive and prone to data errors and noise in analyses. References [72, 100, 225] all investigated the human elements of ransomware victims, particularly the decision-making processes of individuals on whether to pay the ransom, without supplying evidence to intercept ransomware attacks. References [48, 98, 173] examined how organizations could be motivated to combat ransomware attacks but did not suggest effective countermeasures against data exfiltration. Other studies in this category [44, 49, 64, 65, 71, 86, 102, 107, 191, 226, 228, 232] all focused on the socioeconomic effects of crypto-ransomware encryption, making them less relevant to more recent ransomware performing data exfiltration.

5.4.2 Concept. Fifteen studies [10, 18, 20, 21, 42, 59, 60, 69, 101, 136, 139, 140, 148, 210, 235] were found to have explored proof-of-concept ransomware evolution and were listed in Table 6 in the Supplementary Material. Of which, Reference [139] was the first study surveyed by us to mention data exfiltration and correctly predicted that common defensive measures against crypto-ransomware, such as data backup and refusing to pay the ransom, would not be effective against data-selling ransomware but stopped short of explaining how to determine which data to exfiltrate. In Reference [140], the same authors further explored the economic viability of data encryption and data exfiltration but assumed ransom payments could always suppress their data breaches. Reference [60] created a proof-of-concept lock ransomware on industry ***Internet of Things*** **(IoTs)** but did not consider non-locking data exfiltration. Reference [59] prototyped a data exfiltration ransomware on IoT devices, but their proof-of-concept ransomware was automated to exfiltrate all data on the IoT devices (thus increasing the risk of attack failures) and was unable to efficiently evaluate which valuable data to exfiltrate. Reference [69] proposed how to bypass whitelist-based ransomware mitigation but relied on OS APIs and did not consider human-operated cyber intrusions disabling security software. Other studies in this category [10, 18, 20, 21, 42, 101, 136, 148, 210, 235] all suggested ways of circumventing encryption-based ransomware mitigation without considering data exfiltration. To summarize, while proof-of-concept studies may examine novel ideas that could shape the future of ransomware evolution, most failed to notice changes in ransomware that had already occurred at their time of publication.

5.4.3 Investigation. Thirty-five studies [11, 29, 39, 40, 54, 58, 63, 70, 77, 78, 80, 81, 83, 90, 96, 104, 118, 120, 126, 127, 131, 138, 145, 149, 157, 167, 177, 181, 194, 196, 207, 214, 223, 224, 229] were found to have investigated the technical aspects of ransomware and were listed in Table 7 in the Supplementary Material. Reference [207] mentioned "personality theft" with healthcare data, possibly meaning a data breach, but did not specifically mention data exfiltration. Reference [120] clearly coined "double-extortion ransomware," mentioned both file encryption and data leak, and referred to *Maze* ransomware, but only investigated the technical aspects of *Maze* ransomware without examining its business model or the prevalence of data exfiltration among other ransomware variants. Reference [63] investigated a case study in which *Babuk* ransomware attacked via both encryption and data exfiltration; the authors suggested combating ransomware at government levels but did not suggest technical countermeasures and did not examine the prevalence of data exfiltration

[21] https://ia.acs.org.au/article/2022/ransomware-victim-denied-insurance-pay-out.html

among other ransomware variants. Other studies in this category [11, 29, 39, 40, 54, 58, 70, 77, 78, 80, 81, 83, 90, 96, 104, 118, 126, 127, 131, 138, 145, 149, 157, 167, 177, 181, 194, 196, 214, 223, 224, 229] all investigated crypto-ransomware without considering data exfiltration. While ransomware investigation studies revealed more of their chosen technical aspects of ransomware of their choice, most did not explore at the technical level how ransomware could exfiltrate information to perform data theft.

5.4.4 Mitigation. Of the 123 studies [1–9, 12–15, 17, 19, 22, 24, 25, 28, 30–35, 37, 38, 46, 51, 53, 55, 61, 62, 66–68, 74, 79, 82, 84, 85, 87, 88, 91–95, 97, 103, 105, 108, 109, 112–114, 116, 119, 121–124, 128–130, 133, 134, 137, 141, 142, 144, 146, 147, 151, 153, 159, 164–166, 170–172, 174, 178, 179, 182, 183, 185–187, 189, 190, 192, 193, 195, 197–203, 205, 206, 208, 209, 211, 212, 216–219, 221, 222, 230, 231, 233, 234, 236–238] listed in Table 8 in the Supplementary Material, only References [153, 171] addressed data exfiltration, but both relied on simulation to verify their proposals; they could instead consider ***Penetration Testing*** **(PenTest)**, an industry standard of assessing resilience against data breaches. References [105, 109, 222] briefly noted data exfiltration in their introductions to ransomware but still focused on mitigating data encryption and did not specifically address data exfiltration as a separate feature. All other studies [1–9, 12–15, 17, 19, 22, 24, 25, 28, 30–35, 37, 38, 46, 51, 53, 55, 61, 62, 66–68, 74, 79, 82, 84, 85, 87, 88, 91–95, 97, 103, 108, 112–114, 116, 119, 121–124, 128–130, 133, 134, 137, 141, 142, 144, 146, 147, 151, 159, 164–166, 170, 172, 174, 178, 179, 182, 183, 185–187, 189, 190, 192, 193, 195, 197–203, 205, 206, 208, 209, 211, 212, 216–219, 221, 230, 231, 233, 234, 236–238] cited previous ransomware definitions, which had identified ransomware only as crypto-ransomware as ground truth, without further questioning their accuracy or contemporaneity, so they did not investigate ransomware data exfiltration. Among them, References [1–9, 12–15, 19, 25, 31, 32, 34, 35, 37, 46, 51, 53, 55, 61, 62, 82, 87, 88, 91–95, 103, 105, 113, 114, 121, 122, 124, 128–130, 133, 141, 142, 144, 146, 147, 159, 165, 166, 170, 172, 174, 178, 182, 183, 185, 189, 190, 193, 195, 197–199, 202, 203, 205, 206, 211, 212, 217–219, 221, 222, 230, 231, 233, 234, 236, 238] all took blackbox approaches to apply ML on crypto-ransomware (without considering data exfiltration), fully relied on ML to automatically detect and differentiate their samples, and did not evaluate the external validity of their studies on ransomware in the wild. Many of those studies used optional features of ransomware that only existed in some of the variants. References [32, 67, 79, 85, 105, 112, 116, 134, 208, 236] chose to use entropy values to confirm data encryption, while entropy had already been proven to be an unreliable indicator of data encryption [150]. References [5, 8, 9, 13, 19, 24, 28, 30, 32, 37, 38, 53, 66–68, 74, 82, 84, 88, 97, 108, 109, 113, 129, 137, 165, 166, 183, 185, 186, 192, 200, 201, 206, 208, 209, 211, 212, 234, 237] investigated API calls or IRP activities of crypto-ransomware attacks on personal computers without recognizing that exfiltrating data from databases or cloud storage could circumvent local API calls and that certain direct disk operations could evade IRP checks. References [7, 12, 22, 25, 33, 51, 62, 103, 124, 179, 189, 202, 209, 217] centered on optional features of some crypto-ransomware variants, such as the observed specific network ports used by their C&C traffic or the usage of the bitcoin blockchain, yet those optional features were only valid for the variants observed by those authors and not critical features for the success of ransomware extortion.

5.5 Summary of Findings

The academic community, sidetracked by combinatorially assessing different combinations of ML algorithms and datasets—producing nominally impressive "detection" rates on crypto-ransomware—collectively missed the real opportunity in the past three years (2020–2022) to keep up with the transition of ransomware from data encryption to data exfiltration. The ML studies have largely failed to produce meaningful, externally valid results that contribute to the mitigation

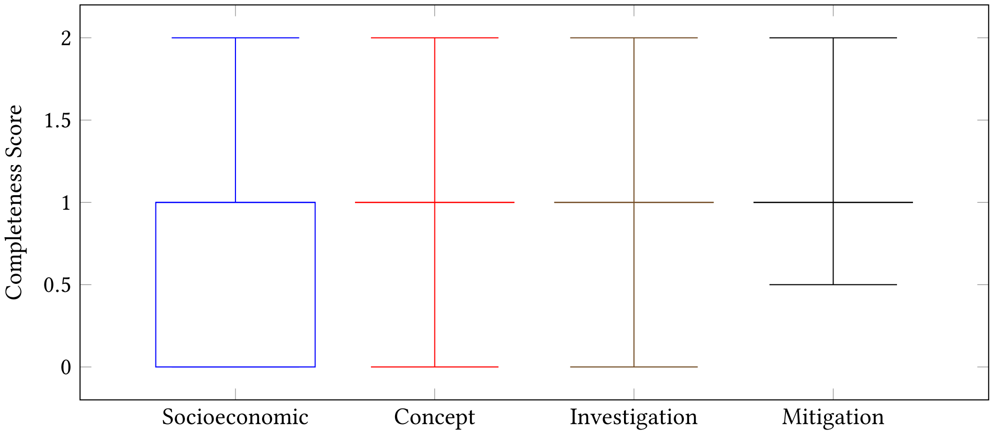

Fig. 4. Completeness scores across different research focus areas.

of actual ransomware in the wild or, most importantly, failed to prevent, deter, or block numerous data breaches of national significance, where data was held for ransom, such as Optus[22] or Medibank[23] in Australia.

Despite data exfiltration ransomware being prevalent since the end of 2019, most of the studies we surveyed from 2020 to 2022 still did not cover data exfiltration ransomware adequately, as evidenced by their low completeness metric scores (Figure 4). This is a significant finding in the research landscape for several reasons:

(1) Many researchers simply cite previous research outcomes and build on them without re-examining whether those cited outcomes are still relevant and up to date.
(2) Novelty and possibility do not necessarily equate to superiority over existing approaches.
(3) Many researchers, particularly in the machine learning community, tend to recombine ML algorithms and datasets without a real-world understanding of ransomware as it is deployed in industry.

Our analysis does not aim to diminish the value of exploring novel attack methods and mitigation techniques, but emphasizes the need for research alignment and practicality with the current ransomware threat landscape.

6 Survey Insights

Based on our review of research articles in Section 5, we have made the following observations.

6.1 Major Themes Identified

We have identified the following four major themes among the ransomware research published since 2020:

6.1.1 Encryption Dominated the Academic Research, Despite Slowly Being Deprecated. Despite being gradually phased out by ransomware in favor of data exfiltration, encryption has remained a dominant area of focus in academic research. We grouped academic studies based on the article dates, superimposed the curves displaying the counts of articles that met selected criteria per quarter, with the trend curve of percentage of actual data exfiltration, and generated Figure 5.

[22] https://www.acma.gov.au/optus-data-breach
[23] https://www.medibank.com.au/health-insurance/info/cyber-security/timeline/

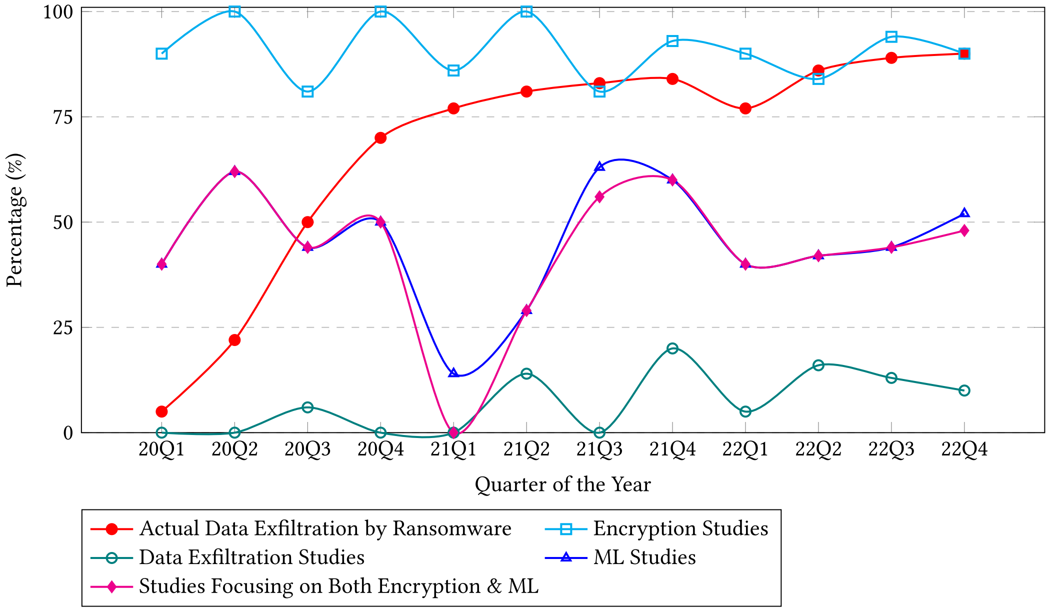

Fig. 5. Percentage of ransomware data exfiltration vs. ransomware academic research focus.

We used article revision dates or submission dates whenever possible to best represent their supposed contemporaneity. Give that, on average, an academic study could take several months to be conducted and authored, we expected to see a similar uptick trend of studies focusing on data exfiltration, lagging behind the trend curve of actual data exfiltration by a few months. However, such an up-trending curve of research focus on ransomware data exfiltration was not observed, even three years after the emergence of ransomware with data exfiltration. Instead, both the research interest in crypto-ransomware and that in ransomware with data exfiltration remained relatively stable, averaged at 91% and 7%, respectively. This deviation suggests that there is a gap between the focus of academic research on ransomware and the evolving nature of ransomware threats in the real world. It may be beneficial for researchers to consider a more comprehensive approach that takes into account the changing tactics and techniques of the most recent ransomware attacks.

6.1.2 Machine Learning Widely Misused as Panacea for Ransomware Mitigation, but Cannot Be Thoroughly Evaluated. We observed the continuing trend that the majority of ML studies on ransomware did not attempt to thoroughly investigate the most contemporary ransomware threat landscape, but simply: (1) assumed ransomware only existed as crypto-ransomware encrypting user files and had not changed its business model; (2) obtained some ransomware samples without verifying their similarity to the most recent ones; (3) executed their ML algorithm on their chosen ransomware samples in a blackbox manner; (4) compared their detection results and false positive rates against other blackbox ML studies; (5) claimed their victory against ransomware and their superiority over other studies. This was reflected in Figure 5, when the curve of ML studies and the curve of studies involving both encryption and ML mostly overlapped. We believe the academic community needs to rethink their general approach of ransomware (or even malware) research, given that the samples are difficult or impossible to collect and are often hardly related to newer variants, especially those developed by different ransomware groups using different attack vectors. Those ML studies on ransomware could be used as proof-of-concept of newer machine learning algorithms, but such studies should be discouraged from claiming victory over ransomware, a real-world problem, unless the results of those studies could be extensively verified in real-world scenarios. Our position is that although ML is a revolutionary tool to advance the IT industry (as evident in ChatGPT and Tesla Full Self-driving), we advocate against a blackbox ML approach on ransomware, in which the authors simply create recombinations of various machine learning algorithms and different unverified ransomware samples without taking responsibility for the external validity of their studies, nor contributing to the advancement of the understanding of ransomware or cybersecurity.

6.1.3 Incomprehension or Complete Disregard of Ransomware Business Models. The end goal of ransomware groups is to disrupt the exclusive access of data owners or custodians to their irreplaceable data of value, to threaten with either data loss (via data encryption and sometimes data destruction) or data breach (via data exfiltration) to extort either monetary values or other gains such as political espionage [152]. The disruption can take place in different forms, especially those not already known nor thwarted by existing countermeasures. Some observed features by some studies (such as file encryption, the local generation of encryption keys, and file encryption over the network) are no longer fixed features of ransomware and should not be treated as such. Treating optional features of ransomware as staples is likely to mislead researchers in the wrong research directions. To disrupt the ransomware business model, it is best to intercept the access by ransomware to protected user data while preserving the legitimate and authorized access by benign users or processes.

6.1.4 Lack of Clarity about Goals of Ransomware Mitigation without Being Business-practical. Most studies, especially those in ransomware mitigation, appeared to value detection accuracy over other metrics, which does not always make business sense in the real world. Ransomware attacks, whether they involve data encryption or data exfiltration, should preferably be terminated with urgency, or the extent of its damage could grow with time [152]. However, ransomware mitigation in a business context often requires a balanced tradeoff between security (detection accuracy and mitigation success rate) and usability (user acceptance), taking into consideration the different risk appetites of different industries [71, 72, 98, 228]. Industries with a stronger emphasis on security, e.g., critical infrastructures, may have very low risk appetite and may decide to invest heavily in cybersecurity measures to mitigate any potential risks, even at the cost of higher false positive rates [98]. Other industries that do not tend to hold irreplaceable or mission-critical data, e.g., hospitality or real estate, may wish to tolerate a higher level of false negative rate in exchange for better usability and customer satisfaction [71, 135, 160]. Some ransomware mitigation proposals may theoretically reduce the false positive rates of ransomware to the minimum, but they are not business-practical. For example:

- Intensive memory scans [32, 105, 133] or frequent CPU profiling [35, 61] will cause performance degradation and affect user experience, especially with mission-critical systems like web servers that cannot be shut down or frozen frequently to take snapshots for their proposed thorough forensic analysis.
- Hooking into cryptographic APIs of the OS to preserve all encryption keys [39–42] will require additional safe storage of those extracted keys and may jeopardize the security and reliability of legitimate applications performing benign encryption consented and authorized by the users, e.g., forming HTTPS connections while web browsing.
- A “moving target defense” [123] or tampering with the storage mechanisms of SSDs [38, 68, 210] can create major program compatibility issues with existing software, an issue that many organizations would be reluctant to address with additional budget or resources.

Therefore, we advocate that researchers should consider the practicality of their proposals in the context of business cybersecurity and the potential new issues that their proposals can introduce to the businesses they are trying to help before recommending their proposals to the business world as viable solutions. We also advocate that manuscript reviewers consider the external validity of a study as a primary requirement for good science.

6.2 Discussions

In this subsection, we reflect on the current stage of ransomware research.

6.2.1 Research Claiming to Mitigate Ransomware Should First Address the Current Dominant Attack Method. Ransomware, when it first emerged as a technologically innovative method of exploiting victims, garnered significant attention for its immediate features, particularly device-locking and file encryption, which were considered defining characteristics of ransomware at that time. However, as ransomware evolves, so should research aiming to mitigate ransomware. Attackers are constantly finding new ways to bypass security measures and deploy ransomware, which makes it essential for researchers and cybersecurity professionals to stay up to date with the latest trends and developments. By actively analyzing the most recent variants of ransomware, understanding their methods of distribution, and developing new strategies for preventing and mitigating attacks, researchers can ensure that they are up to date with the latest trends and developments without solely relying on inherited knowledge from previous research. Because data exfiltration has been the current dominant attack method for the past few years and because user data have to be exfiltrated before being encrypted, recent ransomware researchers should aim to address data exfiltration before data encryption. We did not find extensive coverage of DDoS in published research, possibly because DDoS is still an optional attack feature and is only being trialed by two ransomware groups.

6.2.2 Ransomware Management Should Be Part of Organizational Cybersecurity Risk Management. ISACA, in their *Ransomware Readiness Audit Program* conducted in December 2022, emphasized the negative consequences of inadequate ransomware readiness, which may include reduced staff productivity, failure to achieve performance goals, diminished trust of consumers and stakeholders in the security of their data, and a heightened risk of future attacks.[24] Ransomware, as a cybersecurity risk, should be subject to cybersecurity risk management of organizations. Cybersecurity risk management is not about eliminating the risk entirely, because it is impossible to eliminate all cybersecurity risks. No matter how much time, effort, and money an organization invests in cybersecurity, there is always some level of risk that remains, due to new threats and vulnerabilities, human errors, requirements of cost-effectiveness on organizations, and impacts of extreme mitigation strategies on business operations. The goal of ransomware risk management, as part of the general cybersecurity risk management, should be to become ransomware-ready to minimize the impact and likelihood of ransomware risks by identifying, assessing, and prioritizing them and implementing appropriate mitigation measures. It is also important to note that ransomware risk management is not a one-time activity but a continuous process. Researchers can explore how organizations can best manage ransomware risks effectively while also maintaining business continuity and meeting business objectives.

6.2.3 Collaboration with Government and Industry Sources. As ransomware continues to be a growing threat to individuals, organizations, and governments, it is essential for researchers to

[24] https://www.isaca.org/why-isaca/about-us/newsroom/press-releases/2022/isaca-introduces-new-audit-programs-on-identity-and-access-management-and-ransomware-readiness

work collaboratively with industry and government sources to achieve better research outcomes. Collaborating with government agencies can provide academic researchers with access to valuable resources, such as funding, data, and expertise. Government agencies are often at the forefront of addressing cybersecurity threats and can provide insight into the latest tactics and techniques used by attackers. Researchers can also work with industry sources, such as cybersecurity companies, to gain a better understanding of how ransomware operates and how it can be mitigated. By working together, academic researchers, government agencies, and industry sources can share their knowledge and experience to develop more effective strategies for preventing and mitigating ransomware attacks. This collaboration can help to identify emerging threats, develop new technologies, and create more robust defenses against ransomware attacks. In addition, this collaboration can help to bridge the gap between academia and industry/government, leading to the development of more practical and effective solutions to the problems posed by ransomware. By combining theoretical and practical knowledge, researchers can create more comprehensive and effective solutions that can be implemented in the real world.

6.2.4 Leveraging People, Process, and Technology in GRC against Ransomware. The threat of ransomware has become a significant concern for organizations of all sizes and across all industries. To effectively address this threat, researchers could investigate how organizations can best leverage the power of people, process, and technology in their GRC strategies. The "people" aspect of GRC involves communicating effective cybersecurity policies and procedures to employees, providing ongoing training and education on best practices, and ensuring awareness of risks associated with ransomware. The "process" aspect of GRC involves implementing policies and procedures to mitigate the threat of ransomware, including regular security reviews and updates, access controls, risk assessments, and an incident response plan. The "technology" aspect of GRC involves implementing tools and solutions to mitigate the threat of ransomware, such as EDR, SIEM, and cloud-based backup and recovery solutions. By leveraging the power of people, process, and technology in GRC, organizations can take a comprehensive and proactive approach to mitigating the threat of ransomware. This approach can help organizations reduce the risk of an attack, minimize the potential impact of an attack, and ensure business continuity in the event of an attack. In addition, it can help organizations maintain compliance with relevant regulations and standards while also protecting their reputation and brand.

6.3 Innovative Research Prospects

To address the evolving threat of ransomware, especially data exfiltration ransomware, it is essential to explore state-of-the-art research directions that emphasize practicality and regulatory compliance. Innovative research should not indiscriminately apply all possible solutions but focus on those that offer superior effectiveness and feasibility. The following innovative research prospects are identified:

- **Generative Adversarial Networks (GANs) for Simulation:** Using GANs to simulate ransomware attacks can provide insights into potential vulnerabilities and help develop more robust defensive strategies, which allows for realistic testing environments without the risks associated with live ransomware [156].
- **Generative-AI-driven Predictive Analytics:** Leveraging AI to predict potential attack vectors can enhance preemptive measures, as predictive analytics can identify patterns and anomalies that indicate an impending ransomware attack, allowing for timely intervention [154].

- **Automated Incident Response Systems:** Developing generative-AI-powered systems that can automatically detect and respond to ransomware threats can minimize damage and downtime, and such systems should be capable of learning from new attack patterns and adapting their responses accordingly [154].
- **Privacy and Data Protection Compliance:** Ensuring that ransomware mitigation strategies comply with regulatory requirements—such as privacy and data breach laws—is critical, as innovative solutions should be designed with compliance in mind to avoid legal repercussions and ensure data privacy [156].
- **Generative AI for Employee Training:** Utilizing generative AI to create immersive training environments (e.g., VR and AR) can improve employee awareness and preparedness, which can reduce the likelihood of successful ransomware attacks by enhancing the human element of cybersecurity [156].

6.4 Limitations of This Survey

Despite our best attempt to survey as many relevant papers as possible, we hereby declare the possible limitations of this survey.

6.4.1 Validating the Internal and External Validity of Some Studies Presents Challenges. We have encountered difficulties in verifying the validity of certain studies based solely on their manuscripts. Unfortunately, this is a recurring theme already identified in our previous survey [152]. To ensure a study's internal validity, its research method must be thoroughly explained and scrutinized or replicated on various test samples. However, some researchers provided insufficient or no information regarding their research methods, and others did not make their software available. Some studies simply implemented blackbox ML algorithms without supplying implementation details for validation. Hence, evaluating the internal validity of many studies has been difficult or impossible. In terms of external validity, it is determined by the extent to which a study's ransomware samples converge towards the actual ransomware variants in the wild. While some researchers used a wide range of ransomware samples, others used a limited number or relied on simulations, case studies, or datasets created by others, assuming they had covered all the necessary ransomware scenarios. Unfortunately, none of the existing studies has tested with ransomware with data exfiltration (except several studies that performed simulation with data exfiltration), raising doubts about their external validity.

6.4.2 Industry Reports and Cyber Intelligence on Ransomware Cannot Be Fully Validated. While we had to use ransomware statistics from industry reports and cyber intelligence, it was difficult to fully validate industry reports and cyber intelligence on ransomware. While such reports can often provide valuable first-hand information on ransomware, they often rely on sources that cannot be independently verified or are based on confidential information. Furthermore, the data and statistics presented in such reports may not be comprehensive, up-to-date, peer-reviewed, or accurate, as they may only reflect a limited sample size or a particular geographical or industry sector. In some cases, reports on ransomware may be influenced by the interests or biases of the organizations or individuals producing them. Therefore, caution should be exercised when using industry reports and cyber intelligence as a sole basis for understanding the nature and scope of the ransomware threat.

7 Conclusion and Future Work

We conducted an updated survey on ransomware research to evaluate the relevance of recent studies since our previous survey [152]. We examined 212 academic studies (196 primary research articles and 16 surveys) and cross-verified the findings with contemporary government strategies, industry research, and cyber intelligence. Our review revealed that although data encryption is being deprecated by ransomware actors, it still dominates academic research. Machine learning is often misused as a panacea against ransomware in blackbox manners. Many studies overlook or misunderstand ransomware business models, treating it as a purely technical problem or ML exercise. Additionally, numerous studies lack clarity on ransomware mitigation goals and present proposals impractical for business operations.

To address ransomware, a constantly evolving real-world problem, academic researchers must evaluate the latest ransomware threat landscape before citing previous research as ground truth or starting their own studies. The fundamental cause of repeated ransomware attacks is the motivation of ransomware actors to disrupt the exclusive access of legitimate users to their data through either data loss (via encryption or destruction) or data breach (via exfiltration). We propose that researchers prioritize the current dominant attack method, focusing on data exfiltration over data encryption. It is crucial to integrate ransomware risk management into organizational cybersecurity strategies, collaborate with government and industry sources, and leverage people, processes, and technology in GRC against ransomware. Our survey also highlighted innovative research prospects, emphasizing practical and regulatory-compliant approaches to the evolving ransomware threat landscape, including the potential of generative AI. Future research areas include ransomware trend analysis and monitoring, advanced access control to safeguard data, minimizing incentives for cyber extortion, and enhancing organizational cyber resilience. By addressing such areas, researchers can contribute to more effective and comprehensive ransomware mitigation strategies.

Supplementary Material

A Tables of Comparison of Different Ransomware Studies

Table 5. Comparison of Different Socioeconomic Studies on Ransomware between 2020 and February 2023

Ref.	Date	Core features			ML	Optional features			
		Encryption	Exfiltration	Completeness		Entropy	API/IRP	DDoS	Other features
[158]	2020 Q1			0					
[45]	2020 Q3			0					
[49]	2020 Q3	✓		1					
[228]	2020 Q4	✓		1					
[215]	2021 Q3			0	✓				✓
[107]	2022 Q1			0					
[86]	2022 Q1	✓		1					
[191]	2022 Q1	✓		1					
[71]	2022 Q1			0					✓
[65]	2022 Q2			0					
[100]	2022 Q2			0					
[135]	2022 Q2	✓	✓	2					
[44]	2022 Q2	✓		1					
[225]	2022 Q2			0					
[98]	2022 Q3			0					
[64]	2022 Q3	✓		1					
[143]	2022 Q3	△	△	1					
[48]	2022 Q4			0					
[36]	2022 Q4	✓	△	1.5					
[160]	2022 Q4	✓	✓	2					
[43]	2022 Q4	✓	✓	2					
[232]	2022 Q4	✓		1					
[26]	2022 Q4		✓	1					✓
[173]	2022 Q4			0					
[226]	2023 Q1	✓		1					
[168]	2023 Q1	✓	✓	2					

(✓: Explicitly expressed; △: Implicitly indicated).

Table 6. Comparison of Different Studies on Ransomware Concept between 2020 and February 2023

Ref.	Date	Core features			ML	Optional features			
		Encryption	Exfiltration	Completeness		Entropy	API/IRP	DDoS	Other features
[42]	2020 Q2	✓		1					
[60]	2020 Q3			0					
[139]	2020 Q3		✓	1					
[148]	2020 Q4	✓		1					
[20]	2021 Q1	✓		1					
[59]	2021 Q4		✓	1					
[136]	2022 Q1	✓		1		✓			
[140]	2022 Q1	✓	✓	2					
[21]	2022 Q1	✓		1					
[18]	2022 Q1	✓		1					
[10]	2022 Q1	✓		1					
[101]	2022 Q3	✓		1	✓				
[235]	2022 Q3	✓		1					
[210]	2022 Q4	✓		1					
[69]	2023 Q1			0			✓		

(✓: Explicitly expressed; △: Implicitly indicated).

Table 7. Comparison of Different Studies on Ransomware Investigation between 2020 and February 2023

Ref.	Date	Core features			ML	Optional features			
		Encryption	Exfiltration	Completeness		Entropy	API/IRP	DDoS	Other features
[39]	2020 Q1	✓		1					
[77]	2020 Q2	✓		1					
[40]	2020 Q2	✓		1					
[70]	2020 Q2	✓		1					
[138]	2020 Q3	✓		1					
[167]	2020 Q3	✓		1					
[90]	2020 Q4	✓		1					
[145]	2020 Q4	✓		1	✓				
[181]	2020 Q4	△		0.5		✓			
[177]	2021 Q1	✓		1					
[194]	2021 Q1			0	✓		✓		
[78]	2021 Q1	✓		1		✓			
[207]	2021 Q2	△	△	1					
[229]	2021 Q2	✓		1				✓	
[11]	2021 Q3	✓		1	✓				✓
[224]	2021 Q3			0					✓
[80]	2021 Q3	✓		1	✓	✓			
[157]	2021 Q4	✓		1	✓		✓		
[104]	2021 Q4	✓		1		✓			
[120]	2021 Q4	✓	✓	2					
[118]	2021 Q4	✓		1					✓
[149]	2021 Q4	✓		1					✓
[196]	2022 Q1	✓		1					
[63]	2022 Q2		✓	1					
[58]	2022 Q2	✓		1					
[83]	2022 Q2	✓		1					
[126]	2022 Q3	✓		1					
[29]	2022 Q3	✓		1					
[223]	2022 Q3	✓		1					
[214]	2022 Q3	✓		1					
[96]	2022 Q3			0.0		✓			
[81]	2022 Q4	✓		1					
[131]	2022 Q4	△		0.5					
[127]	2022 Q4	✓		1					
[54]	2022 Q4	✓		1	✓				

(✓: Explicitly expressed; △: Implicitly indicated).

Table 8. Comparison of Different Studies on Ransomware Mitigation between 2020 and February 2023

Ref.	Date	Core features			ML	Optional features			
		Encryption	Exfiltration	Completeness		Entropy	API/IRP	DDoS	Other features
[128]	2020 Q1	✓		1	✓				
[199]	2020 Q1	✓		1	✓				
[109]	2020 Q1	✓	△	1.5			✓		
[189]	2020 Q1	△		0.5	✓				✓
[28]	2020 Q1	✓		1			✓		
[119]	2020 Q2	✓		1					
[3]	2020 Q2	✓		1	✓				
[87]	2020 Q2	✓		1	✓				
[170]	2020 Q2	✓		1	✓				
[238]	2020 Q2	✓		1	✓				
[31]	2020 Q2	✓		1	✓				
[9]	2020 Q2	✓		1	✓	✓			
[129]	2020 Q2	✓		1	✓	✓			
[217]	2020 Q2	✓		1	✓				✓
[13]	2020 Q2	✓		1	✓	✓			
[122]	2020 Q2	✓		1	✓				
[190]	2020 Q2	✓		1	✓				
[212]	2020 Q2	✓		1	✓	✓			
[38]	2020 Q2	✓		1		✓			
[24]	2020 Q2	✓		1		✓			
[208]	2020 Q3	✓		1	✓	✓			
[186]	2020 Q3	✓		1		✓			
[37]	2020 Q3	✓		1	✓	✓			
[67]	2020 Q3	✓		1		✓			
[4]	2020 Q3	✓		1	✓				
[144]	2020 Q3	✓		1	✓				
[185]	2020 Q3	✓		1	✓	✓			
[121]	2020 Q3	✓		1	✓				
[35]	2020 Q3	✓		1	✓				
[14]	2020 Q3	✓		1	✓				
[141]	2020 Q4	✓		1	✓				
[187]	2020 Q4	✓		1					
[192]	2020 Q4	✓		1		✓			
[130]	2020 Q4	✓		1	✓				
[174]	2020 Q4	✓		1	✓				
[92]	2020 Q4	✓		1	✓				
[53]	2020 Q4	✓		1	✓	✓			
[182]	2020 Q4	✓		1	✓				
[55]	2020 Q4	✓		1	✓				
[22]	2021 Q1	✓		1					✓
[85]	2021 Q1	✓		1	✓				
[198]	2021 Q2	✓		1	✓				
[116]	2021 Q2	✓		1	✓				
[205]	2021 Q2	✓		1	✓				
[97]	2021 Q2	✓		1		✓			
[151]	2021 Q3	✓		1					
[32]	2021 Q3	✓		1	✓	✓			
[164]	2021 Q3	✓		1					
[183]	2021 Q3	✓		1	✓	✓			
[62]	2021 Q3	✓		1	✓				✓

(Continued)

Table 8. Continued

Ref.	Date	Core features			ML	Optional features			
		Encryption	Exfiltration	Completeness		Entropy	API/IRP	DDoS	Other features
[74]	2021 Q4	✓		1		✓			
[165]	2021 Q4	✓		1	✓	✓			
[46]	2021 Q4	✓		1	✓				
[95]	2021 Q4	✓		1	✓				
[237]	2021 Q4	✓		1		✓			
[6]	2021 Q4	✓		1	✓				
[19]	2021 Q4	✓		1	✓	✓			
[12]	2021 Q4	✓		1	✓				✓
[233]	2021 Q4	✓		1	✓				
[82]	2021 Q4	✓		1	✓	✓			
[8]	2021 Q4	✓		1	✓	✓			
[88]	2021 Q4	✓		1	✓	✓			
[34]	2022 Q1	✓		1	✓				
[147]	2022 Q1	✓		1	✓				
[236]	2022 Q1	✓		1	✓				
[2]	2022 Q1	✓		1	✓				
[216]	2022 Q1	✓		1					
[7]	2022 Q1	△		0.5	✓				✓
[166]	2022 Q1	✓		1	✓	✓			
[201]	2022 Q1	✓		1		✓			
[61]	2022 Q1	△		0.5	✓				
[172]	2022 Q2	✓		1	✓				
[178]	2022 Q2	✓		1	✓				
[66]	2022 Q2	✓		1		✓			
[133]	2022 Q2	✓		1	✓				
[206]	2022 Q2	✓		1	✓	✓			
[222]	2022 Q2	✓	△	1.5	✓				
[179]	2022 Q2	✓		1					✓
[234]	2022 Q2	✓		1	✓	✓			
[33]	2022 Q2	✓		1					✓
[94]	2022 Q2	✓		1	✓				
[137]	2022 Q2	✓		1		✓			
[230]	2022 Q3	✓		1	✓				
[113]	2022 Q3	✓		1	✓	✓			
[211]	2022 Q3	✓		1	✓	✓			
[108]	2022 Q3	✓		1		✓			
[51]	2022 Q3	✓		1	✓				✓
[202]	2022 Q3	✓		1	✓				✓
[30]	2022 Q3	✓		1		✓			
[105]	2022 Q3	✓	△	1.5	✓				
[114]	2022 Q3	✓		1	✓				
[134]	2022 Q3	✓		1		✓			
[197]	2022 Q3	✓		1	✓				
[1]	2022 Q3	✓		1	✓				
[200]	2022 Q3	✓		1		✓			
[84]	2022 Q3	✓		1		✓			
[159]	2022 Q3	✓		1	✓				
[209]	2022 Q4	✓		1		✓		✓	
[218]	2022 Q4	✓		1	✓				
[79]	2022 Q4	✓		1	✓				

(Continued)

Table 8. Continued

Ref.	Date	Core features			ML	Optional features			
		Encryption	Exfiltration	Completeness		Entropy	API/IRP	DDoS	Other features
[171]	2022 Q4	△	✓	1.5					
[195]	2022 Q4	✓		1	✓				
[5]	2022 Q4	✓		1	✓	✓			
[68]	2022 Q4	✓		1		✓			
[193]	2022 Q4	✓		1	✓				
[25]	2022 Q4	✓		1	✓				✓
[17]	2022 Q4	✓		1					
[231]	2022 Q4	✓		1	✓				
[146]	2022 Q4	△		0.5	✓				
[15]	2022 Q4	✓		1	✓				
[142]	2022 Q4	△		0.5	✓				
[91]	2022 Q4	✓		1	✓				
[219]	2022 Q4	✓		1	✓				
[112]	2022 Q4	✓		1		✓			
[203]	2022 Q4	✓		1	✓				
[103]	2022 Q4	△		0.5	✓				✓
[221]	2022 Q4	✓		1	✓				
[123]	2022 Q4	✓		1					
[93]	2023 Q1	✓		1	✓				
[124]	2023 Q1	✓		1	✓				✓
[153]	2023 Q1	✓	✓	2					

(✓: Explicitly expressed; △: Implicitly indicated).

References

[1] Khalid A. Alissa, Dalia H. Elkamchouchi, Khaled Tarmissi, Ayman Yafoz, Raed Alsini, Omar Alghushairy, Abdullah Mohamed, and Mesfer Al Duhayyim. 2022. Dwarf mongoose optimization with machine-learning-driven ransomware detection in internet of things environment. *Appl. Sci.* 12, 19 (2022), 9513.

[2] Muhammad Shabbir Abbasi, Harith Al-Sahaf, Masood Mansoori, and Ian Welch. 2022. Behavior-based ransomware classification: A particle swarm optimization wrapper-based approach for feature selection. *Appl. Soft Comput.* 121 (2022), 108744.

[3] Muhammad Shabbir Abbasi, Harith Al-Sahaf, and Ian Welch. 2020. Particle swarm optimization: A wrapper-based feature selection method for ransomware detection and classification. In *23rd European Conference on Applications of Evolutionary Computation (EvoApplications'20), Held as Part of EvoStar'20.* Springer, 181–196.

[4] Alexander Adamov and Anders Carlsson. 2020. Reinforcement learning for anti-ransomware testing. In *IEEE East-West Design & Test Symposium (EWDTS'20).* IEEE, 1–5.

[5] Masaad Naji Masaad Ahmad and Wael Elmedany. 2022. A review on methods for managing the risk of Android ransomware. In *International Conference on Data Analytics for Business and Industry (ICDABI'22).* IEEE, 773–779.

[6] Muhammad Ejaz Ahmed, Hyoungshick Kim, Seyit Camtepe, and Surya Nepal. 2021. Peeler: Profiling kernel-level events to detect ransomware. In *26th European Symposium on Research in Computer Security (ESORICS'21).* Springer, 240–260.

[7] Usman Ahmed, Jerry Chun-Wei Lin, and Gautam Srivastava. 2022. Mitigating adversarial evasion attacks of ransomware using ensemble learning. *Comput. Electric. Eng.* 100 (2022), 107903.

[8] Yahye Abukar Ahmed, Shamsul Huda, Bander Ali Saleh Al-rimy, Nouf Alharbi, Faisal Saeed, Fuad A. Ghaleb, and Ismail Mohamed Ali. 2022. A weighted minimum redundancy maximum relevance technique for ransomware early detection in industrial IoT. *Sustainability* 14, 3 (2022), 1231.

[9] Yahye Abukar Ahmed, Barış Koçer, Shamsul Huda, Bander Ali Saleh Al-Rimy, and Mohammad Mehedi Hassan. 2020. A system call refinement-based enhanced Minimum Redundancy Maximum Relevance method for ransomware early detection. *J. Netw. Comput. Applic.* 167 (2020), 102753.

[10] Mahmoud Al-Dwairi, Ahmed S. Shatnawi, Osama Al-Khaleel, and Basheer Al-Duwairi. 2022. Ransomware-resilient self-healing XML documents. *Fut. Internet* 14, 4 (2022), 115.

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

[12] Muna Al-Hawawreh, Elena Sitnikova, and Neda Aboutorab. 2021. Asynchronous peer-to-peer federated capability-based targeted ransomware detection model for industrial IoT. *IEEE Access* 9 (2021), 148738–148755.

[13] Bander Ali Saleh Al-rimy, Mohd Aiziani Maarof, Mamoun Alazab, Fawaz Alsolami, Syed Zainudeen Mohd Shaid, Fuad A. Ghaleb, Tawfik Al-Hadhrami, and Abdullah Marish Ali. 2020. A pseudo feedback-based annotated TF-IDF technique for dynamic crypto-ransomware pre-encryption boundary delineation and features extraction. *IEEE Access* 8 (2020), 140586–140598.

[14] Bander Ali Saleh Al-rimy, Mohd Aizaini Maarof, Mamoun Alazab, Syed Zainudeen Mohd Shaid, Fuad A. Ghaleb, Abdulmohsen Almalawi, Abdullah Marish Ali, and Tawfik Al-Hadhrami. 2020. Redundancy coefficient gradual up-weighting-based mutual information feature selection technique for crypto-ransomware early detection. *Future Generation Computer Systems* 115 (2021), 641–658.

[15] Khalid Albulayhi and Qasem Abu Al-Haija. 2022. Early-stage malware and ransomware forecasting in the short-term future using regression-based neural network technique. In *14th International Conference on Computational Intelligence and Communication Networks (CICN'22)*. IEEE, 735–742.

[16] Fatimah Aldauiji, Omar Batarfi, and Manal Bayousif. 2022. Utilizing cyber threat hunting techniques to find ransomware attacks: A survey of the state of the art. *IEEE Access* 10 (2022), 61695–61706.

[17] Anas AlMajali, Ahmad Qaffaf, Natali Alkayid, and Yatin Wadhawan. 2022. Crypto-ransomware detection using selective hashing. In *International Conference on Electrical and Computing Technologies and Applications (ICECTA'22)*. IEEE, 328–331.

[18] Felipe Almeida, Malik Imran, Jaan Raik, and Samuel Pagliarini. 2022. Ransomware attack as hardware Trojan: A feasibility and demonstration study. *IEEE Access* 10 (2022), 44827–44839.

[19] Rana Almohaini, Iman Almomani, and Aala AlKhayer. 2021. Hybrid-based analysis impact on ransomware detection for Android systems. *Appl. Sci.* 11, 22 (2021), 10976.

[20] Iman Almomani, Aala AlKhayer, and Walid El-Shafai. 2021. Novel ransomware hiding model using HEVC steganography approach. *CMC Comput. Mater. Contin.* 70, 2 (2021), 1209–1228.

[21] Iman Almomani, Aala Alkhayer, and Walid El-Shafai. 2022. A crypto-steganography approach for hiding ransomware within HEVC streams in Android IoT devices. *Sensors* 22, 6 (2022), 2281.

[22] Fahad M. Alotaibi and Vassilios G. Vassilakis. 2021. SDN-based detection of self-propagating ransomware: The case of BadRabbit. *IEEE Access* 9 (2021), 28039–28058.

[23] Abdullah Alqahtani and Frederick T. Sheldon. 2022. A survey of crypto ransomware attack detection methodologies: An evolving outlook. *Sensors* 22, 5 (2022), 1837.

[24] Ali AlSabeh, Haidar Safa, Elias Bou-Harb, and Jorge Crichigno. 2020. Exploiting ransomware paranoia for execution prevention. In *IEEE International Conference on Communications (ICC'20)*. IEEE, 1–6.

[25] Ramadhan A. M. Alsaidi, Wael M. S. Yafooz, Hashem Alolofi, Ghilan Al-Madhagy Taufiq-Hail, Abdel-Hamid M. Emara, and Ahmed Abdel-Wahab. 2022. Ransomware detection using machine and deep learning approaches. *Int. J. Advan. Comput. Sci. Applic.* 13, 11 (2022).

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

[27] Hesham Alshaikh, Nagy Ramadan, and Hesham Ahmed Hefny. 2020. Ransomware prevention and mitigation techniques. *Int. J. Comput. Appl* 177, 40 (2020), 31–39.

[28] Samah Alsoghyer and Iman Almomani. 2020. On the effectiveness of application permissions for Android ransomware detection. In *6th Conference on Data Science and Machine Learning Applications (CDMA'20)*. IEEE, 94–99.

[29] Saleh Alzahrani, Yang Xiao, and Wei Sun. 2022. An analysis of conti ransomware leaked source codes. *IEEE Access* 10 (2022), 100178–100193.

[30] P. Mohan Anand, P. V. Sai Charan, and Sandeep K. Shukla. 2022. A comprehensive API call analysis for detecting Windows-based ransomware. In *IEEE International Conference on Cyber Security and Resilience (CSR'22)*. IEEE, 337–344.

[31] Abdullahi Arabo, Remi Dijoux, Timothee Poulain, and Gregoire Chevalier. 2020. Detecting ransomware using process behavior analysis. *Procedia Comput. Sci.* 168 (2020), 289–296.

[32] Asad Arfeen, Muhammad Asim Khan, Obad Zafar, and Usama Ahsan. 2022. Process based volatile memory forensics for ransomware detection. *Concurr. Comput.: Pract. Exper.* 34, 4 (2022), e6672.

[33] Amirthasaravanan Arivunambi and Arjun Paramarthalingam. 2022. A study on two-phase monitoring server for ransomware evaluation and detection in IoT environment. *J. Trends Comput. Sci. Smart Technol.* 4, 2 (2022), 72–82.

[34] Sana Aurangzeb, Haris Anwar, Muhammad Asif Naeem, and Muhammad Aleem. 2022. BigRC-EML: Big-data based ransomware classification using ensemble machine learning. *Clust. Comput.* 25, 5 (2022), 3405–3422.

[35] Sana Aurangzeb, Rao Naveed Bin Rais, Muhammad Aleem, Muhammad Arshad Islam, and Muhammad Azhar Iqbal. 2021. On the classification of Microsoft-Windows ransomware using hardware profile. *PeerJ Comput. Sci.* 7 (2021), e361.

[36] Louise Axon, Arnau Erola, Ioannis Agrafiotis, Ganbayar Uuganbayar, Michael Goldsmith, and Sadie Creese. Ransomware as a predator: Modelling the systemic risk to prey. *Digital Threats: Research and Practice* 4, 4, 1–38.

[37] Md Ahsan Ayub, Andrea Continella, and Ambareen Siraj. 2020. An I/O Request Packet (IRP) driven effective ransomware detection scheme using artificial neural network. In *IEEE 21st International Conference on Information Reuse and Integration for Data Science (IRI'20)*. IEEE Computer Society, 319–324.

[38] Sungha Baek, Youngdon Jung, David Mohaisen, Sungjin Lee, and Daehun Nyang. 2020. SSD-assisted ransomware detection and data recovery techniques. *IEEE Trans. Comput.* 70, 10 (2020), 1762–1776.

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

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

[41] Pranshu Bajpai and Richard Enbody. 2020. Memory forensics against ransomware. In *International Conference on Cyber Security and Protection of Digital Services (Cyber Security'20)*. IEEE, 1–8.

[42] Pranshu Bajpai and Richard Enbody. 2020. Preparing smart cities for ransomware attacks. In *3rd International Conference on Data Intelligence and Security (ICDIS'20)*. IEEE, 127–133.

[43] Tom Baker and Anja Shortland. 2023. Insurance and enterprise: Cyber insurance for ransomware. *The Geneva Papers on Risk and Insurance-Issues and Practice* 48, 2 (2023), 275–299.

[44] Rudra Prasad Baksi. 2022. Pay or not pay? A game-theoretical analysis of ransomware interactions considering a defender's deception architecture. In *52nd Annual IEEE/IFIP International Conference on Dependable Systems and Networks-Supplemental Volume (DSN-S'22)*. IEEE, 53–54.

[45] Chetan Bansal, Pantazis Deligiannis, Chandra Maddila, and Nikitha Rao. 2020. Studying ransomware attacks using web search logs. In *43rd International ACM SIGIR Conference on Research and Development in Information Retrieval*. 1517–1520.

[46] Manoj Basnet, Subash Poudyal, Mohd Hasan Ali, and Dipankar Dasgupta. 2021. Ransomware detection using deep learning in the SCADA system of electric vehicle charging station. In *IEEE PES Innovative Smart Grid Technologies Conference-Latin America (ISGT Latin America'21)*. IEEE, 1–5.

[47] Craig Beaman, Ashley Barkworth, Toluwalope David Akande, Saqib Hakak, and Muhammad Khurram Khan. 2021. Ransomware: Recent advances, analysis, challenges and future research directions. *Comput. Secur.* 111 (2021), 102490.

[48] Luuk Bekkers, Susanne van't Hoff-de Goede, Ellen Misana-ter Huurne, Ynze van Houten, Remco Spithoven, and Eric Rutger Leukfeldt. 2023. Protecting your business against ransomware attacks? Explaining the motivations of entrepreneurs to take future protective measures against cybercrimes using an extended protection motivation theory model. *Comput. Secur.* 127 (2023), 103099.

[49] Abubakar Bello and Alana Maurushat. 2020. Technical and behavioural training and awareness solutions for mitigating ransomware attacks. In *Computer Science On-line Conference*. Springer, 164–176.

[50] Ibrahim Bello, Haruna Chiroma, Usman A. Abdullahi, Abdulsalam Ya'u Gital, Fatsuma Jauro, Abdullah Khan, Julius O. Okesola, and M. Abdulhamid Shafi'i. 2020. Detecting ransomware attacks using intelligent algorithms: Recent development and next direction from deep learning and big data perspectives. *Journal of Ambient Intelligence and Humanized Computing* 12 (2020), 8699–8717.

[51] Eduardo Berrueta, Daniel Morato, Eduardo Magaña, and Mikel Izal. 2022. Crypto-ransomware detection using machine learning models in file-sharing network scenarios with encrypted traffic. *Expert Syst. Applic.* 209 (2022), 118299.

[52] C. V. Bijitha, Rohit Sukumaran, and Hiran V. Nath. 2020. A survey on ransomware detection techniques. In *8th International Conference on Secure Knowledge Management In Artificial Intelligence Era (SKM'19)*. Springer, 55–68.

[53] Paul Black, Ammar Sohail, Iqbal Gondal, Joarder Kamruzzaman, Peter Vamplew, and Paul Watters. 2020. API based discrimination of ransomware and benign cryptographic programs. In *27th International Conference on Neural Information Processing (ICONIP'20)*. Springer, 177–188.

[54] Robert Bold, Haider Al-Khateeb, and Nikolaos Ersotelos. 2022. Reducing false negatives in ransomware detection: A critical evaluation of machine learning algorithms. *Appl. Sci.* 12, 24 (2022), 12941.

[55] Parthajit Borah, Dhruba K. Bhattacharyya, and Jugal K. Kalita. 2021. Cost effective method for ransomware detection: An ensemble approach. In *17th International Conference on Distributed Computing and Internet Technology (ICDCIT'21)*. Springer, 203–219.

[56] Marcus Botacin, Fabricio Ceschin, Paulo De Geus, and André Grégio. 2020. We need to talk about antiviruses: Challenges & pitfalls of AV evaluations. *Comput. Secur.* 95 (2020), 101859.

[57] Marcus Botacin, Fabricio Ceschin, Ruimin Sun, Daniela Oliveira, and André Grégio. 2021. Challenges and pitfalls in malware research. *Comput. Secur.* 106 (2021), 102287.

[58] Marietjie Botes and Gabriele Lenzini. 2022. When cryptographic ransomware poses cyber threats: Ethical challenges and proposed safeguards for cybersecurity researchers. In *IEEE European Symposium on Security and Privacy Workshops (EuroS&PW'22)*. IEEE, 562–568.

[59] Calvin Brierley, Budi Arief, David Barnes, and Julio Hernandez-Castro. 2021. Industrialising blackmail: Privacy invasion based IoT ransomware. In *26th Nordic Conference on Secure IT Systems (NordSec'21)*. Springer, 72–92.

[60] Calvin Brierley, Jamie Pont, Budi Arief, David J. Barnes, and Julio Hernandez-Castro. 2020. PaperW8: An IoT bricking ransomware proof of concept. In *15th International Conference on Availability, Reliability and Security*. 1–10.

[61] Reeve Cabral, J. Todd McDonald, Lee M. Hively, and Ryan G. Benton. 2022. Profiling CPU behavior for detection of Android ransomware. In *SoutheastCon'22*. IEEE, 690–697.

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

[63] Emily Caroscio, Jack Paul, John Murray, and Suman Bhunia. 2022. Analyzing the ransomware attack on DC Metropolitan Police Department by Babuk. In *IEEE International Systems Conference (SysCon'22)*. IEEE, 1–8.

[64] Anna Cartwright and Edward Cartwright. 2023. The economics of ransomware attacks on integrated supply chain networks. *Digital Threats: Research and Practice* 4, 4 (2023), 1–14.

[65] Anna Cartwright, Edward Cartwright, Lian Xue, and Julio Hernandez-Castro. 2022. An investigation of individual willingness to pay ransomware. *Journal of Financial Crime* 30, 3 (2022), 728–741.

[66] Alberto Huertas Celdrán, Pedro M. Sánchez Sánchez, Eder J. Scheid, Timucin Besken, Geŕôme Bovet, Gregorio Martínez Pérez, and Burkhard Stiller. 2022. Policy-based and behavioral framework to detect ransomware affecting resource-constrained sensors. In *IEEE/IFIP Network Operations and Management Symposium (NOMS'22)*. IEEE, 1–7.

[67] S. Sibi Chakkaravarthy, D. Sangeetha, Meenalosini Vimal Cruz, V. Vaidehi, and Balasubramanian Raman. 2020. Design of intrusion detection honeypot using Social Leopard algorithm to detect IoT ransomware attacks. *IEEE Access* 8 (2020), 169944–169956.

[68] Niusen Chen, Josh Dafoe, and Bo Chen. 2022. Poster: Data recovery from ransomware attacks via file system forensics and flash translation layer data extraction. In *ACM SIGSAC Conference on Computer and Communications Security*. 3335–3337.

[69] Se-Beom Cheon, Geun-Yeong Choi, and DaeYoub Kim. 2023. A cheating attack on a whitelist-based anti-ransomware solution and its countermeasure. In *IEEE International Conference on Consumer Electronics (ICCE'23)*. IEEE, 01–04.

[70] Fabrizio Cicala and Elisa Bertino. 2020. Analysis of encryption key generation in modern crypto ransomware. *IEEE Trans. Depend. Sec. Comput.* 19, 2 (2020), 1239–1253.

[71] Alena Yuryna Connolly and Hervé Borrion. 2022. Reducing ransomware crime: Analysis of victims' payment decisions. *Comput. Secur.* 119 (2022), 102760.

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

[73] Andrea Continella, Alessandro Guagnelli, Giovanni Zingaro, Giulio De Pasquale, Alessandro Barenghi, Stefano Zanero, and Federico Maggi. 2016. ShieldFS: A self-healing, ransomware-aware filesystem. In *32nd Annual Conference on Computer Security Applications*. ACM, 336–347.

[74] Alfredo Cuzzocrea, Francesco Mercaldo, and Fabio Martinelli. 2021. A framework for supporting ransomware detection and prevention based on hybrid analysis. In *21st International Conference on Computational Science and Its Applications (ICCSA'21)*. Springer, 16–27.

[75] CyberCX. 2021. Ransomware and cyber extortion - how to protect your organization. *CyberCX Best Practice Guide* (2021). Retrieved from https://cybercx.com.au/ransomware/

[76] Cybersecurity and Infrastructure Security Agency (CISA). 2020. CISA-multi-state information sharing and analysis center (MS-ISAC) joint ransomware guide. (Sep. 2020). Retrieved from https://www.cisa.gov/resources-tools/resources/cisa-multi-state-information-sharing-and-analysis-center-ms-isac-joint-ransomware-guide

[77] Simon R. Davies, Richard Macfarlane, and William J. Buchanan. 2020. Evaluation of live forensic techniques in ransomware attack mitigation. *Forens. Sci. Int.: Digit. Investig.* 33 (2020), 300979.

[78] Simon R. Davies, Richard Macfarlane, and William J. Buchanan. 2021. Differential area analysis for ransomware attack detection within mixed file datasets. *Comput. Secur.* 108 (2021), 102377.

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

[80] Fabio De Gaspari, Dorjan Hitaj, Giulio Pagnotta, Lorenzo De Carli, and Luigi V. Mancini. 2022. Evading behavioral classifiers: A comprehensive analysis on evading ransomware detection techniques. *Neural Comput. Applic.* 34, 14 (2022), 12077–12096.

[81] Byron Denham and Dale R. Thompson. 2022. Ransomware and malware sandboxing. In *IEEE 13th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON'22)*. IEEE, 0173–0179.

[82] Jian Du, Sajid Hussain Raza, Mudassar Ahmad, Iqbal Alam, Saadat Hanif Dar, and Muhammad Asif Habib. 2022. Digital forensics as advanced ransomware pre-attack detection algorithm for endpoint data protection. *Secur. Commun. Netw.* 2022, 1 (2022), 1–16.

[83] Eliando Eliando and Yunianto Purnomo. 2022. LockBit 2.0 Ransomware: Analysis of infection, persistence, prevention mechanism. *CogITo Smart J.* 8, 1 (2022), 232–243.

[84] Abdulrahman Abu Elkhail, Nada Lachtar, Duha Ibdah, Rustam Aslam, Hamza Khan, Anys Bacha, and Hafiz Malik. 2023. Seamlessly safeguarding data against ransomware attacks. *IEEE Trans. Depend. Sec. Comput.* 20, 1 (2023), 1–16.

[85] Farnood Faghihi and Mohammad Zulkernine. 2021. RansomCare: Data-centric detection and mitigation against smartphone crypto-ransomware. *Comput. Netw.* 191 (2021), 108011.

[86] Rui Fang, Maochao Xu, and Peng Zhao. 2022. Determination of ransomware payment based on Bayesian game models. *Comput. Secur.* 116 (2022), 102685.

[87] Hossam Faris, Maria Habib, Iman Almomani, Mohammed Eshtay, and Ibrahim Aljarah. 2020. Optimizing extreme learning machines using chains of Salps for efficient Android Ransomware detection. *Appl. Sci.* 10, 11 (2020), 3706.

[88] Damien Warren Fernando and Nikos Komninos. 2022. FeSA: Feature selection architecture for ransomware detection under concept drift. *Comput. Secur.* 116 (2022), 102659.

[89] Damien Warren Fernando, Nikos Komninos, and Thomas Chen. 2020. A study on the evolution of ransomware detection using machine learning and deep learning techniques. *IoT* 1, 2 (2020), 551–604.

[90] Burak Filiz, Budi Arief, Orcun Cetin, and Julio Hernandez-Castro. 2021. On the effectiveness of ransomware decryption tools. *Comput. Secur.* 111 (2021), 102469.

[91] Kurt Friday, Elias Bou-Harb, and Jorge Crichigno. 2022. A learning methodology for line-rate Ransomware mitigation with P4 switches. In *16th International Conference on Network and System Security (NSS'22)*. Springer, 120–139.

[92] Gaddisa Olani Ganfure, Chun-Feng Wu, Yuan-Hao Chang, and Wei-Kuan Shih. 2020. DeepGuard: Deep generative user-behavior analytics for ransomware detection. In *IEEE International Conference on Intelligence and Security Informatics (ISI'20)*. IEEE, 1–6.

[93] Gaddisa Olani Ganfure, Chun-Feng Wu, Yuan-Hao Chang, and Wei-Kuan Shih. 2023. RTrap: Trapping and containing ransomware with machine learning. *IEEE Transactions on Information Forensics and Security* 18 (2023), 1433–1448.

[94] Chulan Gao, Hossain Shahriar, Dan Lo, Yong Shi, and Kai Qian. 2022. Improving the prediction accuracy with feature selection for ransomware detection. In *IEEE 46th Annual Computers, Software, and Applications Conference (COMPSAC'22)*. IEEE, 424–425.

[95] Tanya Gera, Jaiteg Singh, Abolfazl Mehbodniya, Julian L. Webber, Mohammad Shabaz, and Deepak Thakur. 2021. Dominant feature selection and machine learning-based hybrid approach to analyze Android ransomware. *Secur. Commun. Netw.* 2021, 1 (2021), 1–22.

[96] Michał Glet and Kamil Kaczyński. 2022. POSTER: Ransomware detection mechanism–Current state of the project. In *Applied Cryptography and Network Security Workshops: ACNS'22 Satellite Workshops, AIBlock, AIHWS, AIoTS, CIMSS, Cloud S&P, SCI, SecMT, SiMLA*. Springer, 616–620.

[97] José Antonio Gómez-Hernández, Raúl Sánchez-Fernández, and Pedro García-Teodoro. 2022. Inhibiting crypto-ransomware on windows platforms through a honeyfile-based approach with R-Locker. *IET Inf. Secur.* 16, 1 (2022), 64–74.

[98] John W. Goodell and Shaen Corbet. 2023. Commodity market exposure to energy-firm distress: Evidence from the Colonial Pipeline ransomware attack. *Finan. Res. Lett.* 51 (2023), 103329.

[99] Feike Hacquebord, Stephen Hilt, and David Sancho. 2022. The near and far future of ransomware business models. *Trend Micro Research* (Dec. 2022). Retrieved from https://documents.trendmicro.com/assets/white_papers/wp-the-near-and-far-future-of-ransomware.pdf

[100] Murat Haner, Melissa M. Sloan, Amanda Graham, Justin T. Pickett, and Francis T. Cullen. 2022. Ransomware and the Robin Hood effect?: Experimental evidence on Americans' willingness to support cyber-extortion. *Journal of Experimental Criminology* 19, 4 (2022), 943–970.

[101] Noor Hafizah Hassan, Zaireeda Mohd Fauzee, Noris Ismail, and Siti Sarah Maidin. 2022. Artificial intelligence of things (AIoT) ransomware detection conceptual framework. *Proc. Mechan. Eng. Res. Day* 2022, 1 (2022), 205–206.

[102] J. Hernandez-Castro, A. Cartwright, and Edward Cartwright. 2020. An economic analysis of ransomware and its welfare consequences. *R. Societ. Open Sci.* 7, 3 (2020), 190023.

[103] Juan A. Herrera-Silva and Myriam Hernández-Álvarez. 2023. Dynamic feature dataset for ransomware detection using machine learning algorithms. *Sensors* 23, 3 (2023), 1053.

[104] Manabu Hirano, Ryo Hodota, and Ryotaro Kobayashi. 2022. RanSAP: An open dataset of ransomware storage access patterns for training machine learning models. *Forens. Sci. Int.: Digit. Investig.* 40 (2022), 301314.

[105] Manabu Hirano and Ryotaro Kobayashi. 2022. Machine learning-based ransomware detection using low-level memory access patterns obtained from live-forensic hypervisor. In *IEEE International Conference on Cyber Security and Resilience (CSR'22)*. IEEE, 323–330.

[106] Jian Wei Hu, Yu Zhang, and Yan Peng Cui. 2020. Research on Android ransomware protection technology. In *Journal of Physics: Conference Series*, Vol. 1584. IOP Publishing, 012004.

[107] Jan Huck and Frank Breitinger. 2022. Wake up digital forensics' community and help combat ransomware. *IEEE Secur. Privac.* 20, 4 (2022), 61–70.

[108] William Hutton. 2022. Immunizing files against ransomware with koalafied immunity. In *Computing Conference on Intelligent Computing*. Springer, 735–741.

[109] Jinsoo Hwang, Jeankyung Kim, Seunghwan Lee, and Kichang Kim. 2020. Two-stage ransomware detection using dynamic analysis and machine learning techniques. *Wirel. Person. Communications* 112 (2020), 2597–2609.

[110] IBM. 2022. Definitive guide to ransomware 2022. *IBM Security* (May 2022). Retrieved from https://www.ibm.com/ransomware?utm_content=SRCWW

[111] IBM. 2023. X-force threat intelligence index 2023. *IBM Security* (Jan. 2023). Retrieved from https://www.ibm.com/reports/threat-intelligence

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

[113] Muhammad Junaid Iqbal, Sana Aurangzeb, Muhammad Aleem, Gautam Srivastava, and Jerry Chun-Wei Lin. 2022. RThreatDroid: A ransomware detection approach to secure IoT based healthcare systems. *IEEE Transactions on Network Science and Engineering* 10, 5 (2022), 2574–2583.

[114] M. Izham Jaya and Mohd Faizal Ab Razak. 2022. Dynamic ransomware detection for windows platform using machine learning classifiers. *Int. J. Inform. Visualiz.* 6, 2-2 (2022), 469–474.

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

[116] Yash Shashikant Joshi, Harsh Mahajan, Sumedh Nitin Joshi, Kshitij Pradeep Gupta, and Aarti Amod Agarkar. 2021. Signature-less ransomware detection and mitigation. *J. Comput. Virol. Hack. Techniq.* 17, 4 (2021), 299–306.

[117] Adhirath Kapoor, Ankur Gupta, Rajesh Gupta, Sudeep Tanwar, Gulshan Sharma, and Innocent E. Davidson. 2021. Ransomware detection, avoidance, and mitigation scheme: A review and future directions. *Sustainability* 14, 1 (2021), 8.

[118] Ilker Kara and Murat Aydos. 2022. The rise of ransomware: Forensic analysis for Windows based ransomware attacks. *Expert Syst. Applic.* 190 (2022), 116198.

[119] Chee Keong Ng, Sutharshan Rajasegarar, Lei Pan, Frank Jiang, and Leo Yu Zhang. 2020. VoterChoice: A ransomware detection honeypot with multiple voting framework. *Concurr. Comput.: Pract. Exper.* 32, 14 (2020), e5726.

[120] Quintin Kerns, Bryson Payne, and Tamirat Abegaz. 2022. Double-extortion ransomware: A technical analysis of Maze ransomware. In *Future Technologies Conference (FTC'21)*. Springer, 82–94.

[121] Ban Mohammed Khammas. 2020. Ransomware detection using random forest technique. *ICT Express* 6, 4 (2020), 325–331.

[122] Firoz Khan, Cornelius Ncube, Lakshmana Kumar Ramasamy, Seifedine Kadry, and Yunyoung Nam. 2020. A digital DNA sequencing engine for ransomware detection using machine learning. *IEEE Access* 8 (2020), 119710–119719.

[123] Muhammad Mubashir Khan, Muhammad Faraz Hyder, Shariq Mahmood Khan, Junaid Arshad, and Muhammad M. Khan. 2023. Ransomware prevention using moving target defense based approach. *Concurrency and Computation: Practice and Experience* 35, 7 (2023), e7592.

[124] Rana Abdul Sami Khan and Dr Mohd Nordin Abdul Rahman. 2023. Efficiency of surveillance of TCP packet in IoT in reducing the risk of ransomware attacks. *J. Theor. Appl. Inf. Technol.* 101, 3 (2023).

[125] Amin Kharraz, William Robertson, Davide Balzarotti, Leyla Bilge, and Engin Kirda. 2015. Cutting the Gordian knot: A look under the hood of ransomware attacks. In *International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment*. Springer, 3–24.

[126] Karl Kiesel, Tom Deep, Austin Flaherty, and Suman Bhunia. 2022. Analyzing multi-vector ransomware attack on Accellion file transfer appliance server. In *7th International Conference on Smart and Sustainable Technologies (SpliTech'22)*. IEEE, 1–6.

[127] Giyoon Kim, Soram Kim, Soojin Kang, and Jongsung Kim. 2022. A method for decrypting data infected with hive ransomware. *J. Inf. Secur. Applic.* 71 (2022), 103387.

[128] Geun Yong Kim, Joon-Young Paik, Yeongcheol Kim, and Eun-Sun Cho. 2022. Byte frequency based indicators for crypto-ransomware detection from empirical analysis. *J. Comput. Sci. Technol.* 37, 2 (2022), 423–442.

[129] S. H. Kok, Azween Abdullah, and N. Z. Jhanjhi. 2022. Early detection of crypto-ransomware using pre-encryption detection algorithm. *J. King Saud Univ.-Comput. Inf. Sci.* 34, 5 (2022), 1984–1999.

[130] S. H. Kok, A. Azween, and N. Z. Jhanjhi. 2020. Evaluation metric for crypto-ransomware detection using machine learning. *J. Inf. Secur. Applic.* 55 (2020), 102646.

[131] Boyan Kostadinov, Joseph Liu, and Julio Rayme. 2022. Using data science tools for investigating chat logs from the Conti ransomware group. In *IEEE 13th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON'22)*. IEEE, 0095–0101.

[132] Vladimir Kropotov, Bakuei Matsukawa, Robert McArdle, Fyodor Yarochkin, Shingo Matsugaya, Erin Burns, Eireann Leverett, and Waratah Analytics. 2023. What decision-makers need to know about ransomware risk. *Trend Micro Research* (Feb. 2023). Retrieved from https://documents.trendmicro.com/assets/white_papers/wp-what-decision-makers-need-to-know-about-ransomware-risk-1.pdf

[133] Sumit Kumar. 2022. An effective ransomware detection approach in a cloud environment using volatile memory features. *J. Comput. Virol. Hack. Techniq.* 18, 4 (2022), 407–424.

[134] Anthony Cheuk Tung Lai, Ping Fan Ke, Kelvin Chan, Siu Ming Yiu, Dongsun Kim, Wai Kin Wong, Shuai Wang, Joseph Muppala, and Alan Ho. 2022. RansomSOC: A more effective security operations center to detect and respond to ransomware attacks. *J. Internet Serv. Inf. Secur.* 12, 3 (2022), 63–75.

[135] Michael Lang, Lena Yuryna Connolly, Paul Taylor, and Phillip J. Corner. 2022. The evolving menace of ransomware: A comparative analysis of pre-pandemic and mid-pandemic attacks. *Digital Threats: Research and Practice* 4, 4 (2022), 1–22.

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

[137] Sanggu Lee, Yoona Kim, Dusol Lee, Inhyuk Choi, and Jihong Kim. 2022. Alohomora: Protecting files from ransomware attacks using fine-grained I/O whitelisting. In *14th ACM Workshop on Hot Topics in Storage and File Systems*. 113–118.

[138] Yassine Lemmou, Jean-Louis Lanet, and El Mamoun Souidi. 2021. A behavioural in-depth analysis of ransomware infection. *IET Inf. Secur.* 15, 1 (2021), 38–58.

[139] Zhen Li and Qi Liao. 2020. Ransomware 2.0: To sell, or not to sell a game-theoretical model of data-selling ransomware. In *15th International Conference on Availability, Reliability and Security*. 1–9.

[140] Zhen Li and Qi Liao. 2022. Preventive portfolio against data-selling ransomware—A game theory of encryption and deception. *Comput. Secur.* 116 (2022), 102644.

[141] Zhida Li, Ana Laura Gonzalez Rios, and Ljiljana Trajković. 2020. Detecting internet worms, ransomware, and blackouts using recurrent neural networks. In *IEEE International Conference on Systems, Man, and Cybernetics (SMC'20)*. IEEE, 2165–2172.

[142] Zhida Li, Ana Laura Gonzalez Rios, and Ljiljana Trajkovic. 2022. Machine learning for detecting the WestRock ransomware attack using BGP routing records. *IEEE Communications Magazine* 61, 3 (2022), 20–26.

[143] Asad Waqar Malik, Zahid Anwar, and Anis U. Rahman. 2022. A novel framework for studying the business impact of ransomware on connected vehicles. *IEEE Internet of Things Journal* 10, 10 (2022), 8348–8356.

[144] Farnoush Manavi and Ali Hamzeh. 2020. 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)*. IEEE, 82–87.

[145] Carlos Manzano, Claudio Meneses, and Paul Leger. 2020. An empirical comparison of supervised algorithms for ransomware identification on network traffic. In *39th International Conference of the Chilean Computer Science Society (SCCC'20)*. IEEE, 1–7.

[146] Benjamin Marais, Tony Quertier, and Stéphane Morucci. 2022. AI-based malware and ransomware detection models. In *Conference on Artificial Intelligence for Defense*.

[147] Mohammad Masum, Md Jobair Hossain Faruk, Hossain Shahriar, Kai Qian, Dan Lo, and Muhaiminul Islam Adnan. 2022. Ransomware classification and detection with machine learning algorithms. In *IEEE 12th Annual Computing and Communication Workshop and Conference (CCWC'22)*. IEEE, 0316–0322.

[148] Víctor Mayoral-Vilches, Unai Ayucar Carbajo, and Endika Gil-Uriarte. 2020. Industrial robot ransomware: Akerbeltz. In *4th IEEE International Conference on Robotic Computing (IRC'20)*. IEEE, 432–435.

[149] Grant McDonald, Pavlos Papadopoulos, Nikolaos Pitropakis, Jawad Ahmad, and William J. Buchanan. 2022. Ransomware: Analysing the impact on Windows active directory domain services. *Sensors* 22, 3 (2022), 953.

[150] Timothy McIntosh, Julian Jang-Jaccard, Paul Watters, and Teo Susnjak. 2019. The inadequacy of entropy-based ransomware detection. In *International Conference on Neural Information Processing*. Springer, 181–189.

[151] Timothy McIntosh, A. S. M. Kayes, Yi-Ping Phoebe Chen, Alex Ng, and Paul Watters. 2021. Dynamic user-centric access control for detection of ransomware attacks. *Comput. Secur.* 111 (2021), 102461.

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

[153] Timothy McIntosh, A. S. M. Kayes, Yi-Ping Phoebe Chen, Alex Ng, and Paul Watters. 2023. Applying staged event-driven access control to combat ransomware. *Computers & Security* 128 (2023), 103160.

[154] Timothy McIntosh, Tong Liu, Teo Susnjak, Hooman Alavizadeh, Alex Ng, Raza Nowrozy, and Paul Watters. 2023. Harnessing GPT-4 for generation of cybersecurity GRC policies: A focus on ransomware attack mitigation. *Comput. Secur.* 134 (2023), 103424.

[155] Timothy R. McIntosh, Julian Jang-Jaccard, and Paul A. Watters. 2018. Large scale behavioral analysis of ransomware attacks. In *International Conference on Neural Information Processing*. Springer, 217–229.

[156] Timothy R. McIntosh, Teo Susnjak, Tong Liu, Paul Watters, Dan Xu, Dongwei Liu, Raza Nowrozy, and Malka N. Halgamuge. 2024. From COBIT to ISO 42001: Evaluating cybersecurity frameworks for opportunities, risks, and regulatory compliance in commercializing large language models. *Computers & Security* 144 (2024), 103964.

[157] Rui Mei, Han-Bing Yan, and Zhi-Hui Han. 2021. RansomLens: Understanding ransomware via causality analysis on system provenance graph. In *3rd International Conference on Science of Cyber Security (SciSec'21)*. Springer, 252–267.

[158] Per Håkon Meland, Yara Fareed Fahmy Bayoumy, and Guttorm Sindre. 2020. The ransomware-as-a-service economy within the darknet. *Computers & Security* 92 (2020), 101762.

[159] Anthony Melaragno and William Casey. 2022. Change point detection with machine learning for rapid ransomware detection. In *IEEE International Conference on Dependable, Autonomic and Secure Computing, International Conference on Pervasive Intelligence and Computing, International Conference on Cloud and Big Data Computing, International Conference on Cyber Science and Technology Congress (DASC/PiCom/CBDCom/CyberSciTech'22)*. IEEE, 1–9.

[160] Tom Meurs, Marianne Junger, Erik Tews, and Abhishta Abhishta. 2022. Ransomware: How attacker's effort, victim characteristics and context influence ransom requested, payment and financial loss. In *Symposium on Electronic Crime Research (eCrime'22)*.

[161] Trend Micro. 2022. Defending the expanding attack surface. *Trend Micro Research* (Aug. 2022). Retrieved from https://documents.trendmicro.com/assets/rpt/rpt-defending-the-expanding-attack-surface-trend-micro-2022-midyear-cybersecurity-report.pdf

[162] Trend Micro. 2022. Future/Tense—Trend micro security predictions for 2023. *Trend Micro Research* (Dec. 2022). Retrieved from https://documents.trendmicro.com/assets/rpt/rpt-future-tense-trend-micro-security-predictions-for-2023.pdf

[163] Microsoft. 2022. Microsoft digital defense report 2022. *Microsoft Research* (2022). Retrieved from https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE5bUvv?culture=en-us&country=us

[164] Donghyun Min, Yungwoo Ko, Ryan Walker, Junghee Lee, and Youngjae Kim. 2021. A content-based ransomware detection and backup solid-state drive for ransomware defense. *IEEE Trans. Comput.-aid. Des. Integ. Circ. Syst.* 41, 7 (2021), 2038–2051.

[165] Ricardo Misael Ayala Molina, Sadegh Torabi, Khaled Sarieddine, Elias Bou-Harb, Nizar Bouguila, and Chadi Assi. 2021. On ransomware family attribution using pre-attack paranoia activities. *IEEE Trans. Netw. Serv. Manag.* 19, 1 (2021), 19–36.

[166] Caio Carvalho Moreira, Claudomiro de Souza de Sales Jr, and Davi Carvalho Moreira. 2022. Understanding ransomware actions through behavioral feature analysis. *J. Commun. Inf. Syst.* 37, 1 (2022), 61–76.

[167] Matthew A. Mos and Md Minhaz Chowdhury. 2020. The growing influence of ransomware. In *IEEE International Conference on Electro Information Technology (EIT'20)*. IEEE, 643–647.

[168] Gareth Mott, Sarah Turner, Jason R. C. Nurse, Jamie MacColl, James Sullivan, Anna Cartwright, and Edward Cartwright. 2023. Between a rock and a hard (ening) place: Cyber insurance in the ransomware era. *Computers & Security* 128 (2023), 103162.

[169] Routa Moussaileb, Nora Cuppens, Jean-Louis Lanet, and Hélène Le Bouder. 2021. A survey on windows-based ransomware taxonomy and detection mechanisms. *ACM Comput. Surv.* 54, 6 (2021), 1–36.

[170] Routa Moussaileb, Nora Cuppens, Jean-Louis Lanet, and Hélène Le Bouder. 2020. Ransomware network traffic analysis for pre-encryption alert. In *12th International Symposium on Foundations and Practice of Security (FPS'19)*. Springer, 20–38.

[171] Michael Mundt and Harald Baier. 2022. Threat-based simulation of data exfiltration towards mitigating multiple ransomware extortions. *Digital Threats: Research and Practice* 4, 4 (2022), 1–23.

[172] Ganapathi Nalinipriya, Maram Balajee, Chittibabu Priya, and Cristin Rajan. 2022. Ransomware recognition in blockchain network using water moth flame optimization-aware DRNN. *Concurr. Comput.: Pract. Exper.* 34, 19 (2022), e7047.

[173] Hannah T. Neprash, Claire C. McGlave, Dori A. Cross, Beth A. Virnig, Michael A. Puskarich, Jared D. Huling, Alan Z. Rozenshtein, and Sayeh S. Nikpay. 2022. Trends in ransomware attacks on US hospitals, clinics, and other health care delivery organizations, 2016-2021. In *JAMA Health Forum*, Vol. 3. American Medical Association, e224873–e224873.

[174] Fakhroddin Noorbehbahani and Mohammad Saberi. 2020. Ransomware detection with semi-supervised learning. In *10th International Conference on Computer and Knowledge Engineering (ICCKE'20)*. IEEE, 024–029.

[175] Commonwealth Government of Australia. 2021. Australian government—Ransomware action plan. (Oct. 2021). Retrieved from https://www.homeaffairs.gov.au/cyber-security-subsite/files/ransomware-action-plan.pdf

[176] National Cyber Security Centre of the Netherlands. 2022. Ransomware incident response plan. (Aug. 2022). Retrieved from https://english.ncsc.nl/binaries/ncsc-en/documenten/publications/2022/augustus/2/incident-response-plan-ransomware/Opmaak+Incident+response+plan_WEB2.pdf

[177] Mohammad N. Olaimat, Mohd Aizaini Maarof, and Bander Ali S. Al-rimy. 2021. Ransomware anti-analysis and evasion techniques: A survey and research directions. In *3rd International Cyber Resilience Conference (CRC'21).* IEEE, 1–6.

[178] Gaddisa Olani, Chun-Feng Wu, Yuan-Hao Chang, and Wei-Kuan Shih. 2022. DeepWare: Imaging performance counters with deep learning to detect ransomware. *IEEE Transactions on Computers* 72, 3 (2022), 600–613.

[179] Otasowie Owolafe and Aderonke F. Thompson. 2022. Analysis of crypto-ransomware using network traffic. *J. Inf. Secur. Cybercr. Res.* 5, 1 (2022), 76–83.

[180] Harun Oz, Ahmet Aris, Albert Levi, and A. Selcuk Uluagac. 2022. A survey on ransomware: Evolution, taxonomy, and defense solutions. *ACM Comput. Surv.* 54, 11s (2022), 1–37.

[181] Jamie Pont, Budi Arief, and Julio Hernandez-Castro. 2020. Why current statistical approaches to ransomware detection fail. In *International Conference on Information Security.* Springer, 199–216.

[182] Subash Poudyal and Dipankar Dasgupta. 2020. Ai-powered ransomware detection framework. In *IEEE Symposium Series on Computational Intelligence (SSCI'20).* IEEE, 1154–1161.

[183] Subash Poudyal and Dipankar Dasgupta. 2021. Analysis of crypto-ransomware using ML-based multi-level profiling. *IEEE Access* 9 (2021), 122532–122547.

[184] James H. Price and Judy Murnan. 2004. Research limitations and the necessity of reporting them. *Am. J. Health Educ.* 35, 2, 66.

[185] Bin Qin, Yalong Wang, and Changchun Ma. 2020. API call based ransomware dynamic detection approach using textCNN. In *International Conference on Big Data, Artificial Intelligence and Internet of Things Engineering (ICBAIE'20).* IEEE, 162–166.

[186] Gowtham Ramesh and Anjali Menen. 2020. Automated dynamic approach for detecting ransomware using finite-state machine. *Decis. Supp. Syst.* 138 (2020), 113400.

[187] Rahul Rastogi, Gaurav Agarwal, and R. K. Shukla. Interactive security of ransomware with heuristic random bit generator. In *International Conference on Communications and Cyber-physical Engineering (ICCCE'20).* Springer, 965–973.

[188] T. R. Reshmi. 2021. Information security breaches due to ransomware attacks-a systematic literature review. *Int. J. Inf. Manag. Data Insights* 1, 2 (2021), 100013.

[189] Elpida Rouka, Celyn Birkinshaw, and Vassilios G. Vassilakis. 2020. SDN-based malware detection and mitigation: The case of ExPetr ransomware. In *IEEE International Conference on Informatics, IoT, and Enabling Technologies (ICIoT'20).* IEEE, 150–155.

[190] Krishna Chandra Roy and Qian Chen. 2021. DeepRan: Attention-based BiLSTM and CRF for ransomware early detection and classification. *Information Systems Frontiers* 23 (2021), 299–315.

[191] Pierce Ryan, John Fokker, Sorcha Healy, and Andreas Amann. 2022. Dynamics of targeted ransomware negotiation. *IEEE Access* 10 (2022), 32836–32844.

[192] Soobia Saeed, N. Z. Jhanjhi, Mehmood Naqvi, Mamoona Humayun, and Shakeel Ahmed. 2020. Ransomware: A framework for security challenges in internet of things. In *2nd International Conference on Computer and Information Sciences (ICCIS'20).* IEEE, 1–6.

[193] Davide Sanvito, Giuseppe Siracusano, Roberto Gonzalez, and Roberto Bifulco. 2022. Poster: MUSTARD-adaptive behavioral analysis for ransomware detection. In *ACM SIGSAC Conference on Computer and Communications Security.* 3455–3457.

[194] Michele Scalas, Konrad Rieck, and Giorgio Giacinto. 2021. Explanation-driven characterization of Android ransomware. In *ICPR International Workshops and Challenges: Pattern Recognition.* Springer, 228–242.

[195] Christoph Sendner, Lukas Iffländer, Sebastian Schindler, Michael Jobst, Alexandra Dmitrienko, and Samuel Kounev. 2022. Ransomware detection in databases through dynamic analysis of query sequences. In *IEEE Conference on Communications and Network Security (CNS'22).* IEEE, 326–334.

[196] Nikhil Sharma and Ravi Shanker. 2022. Analysis of ransomware attack and their countermeasures: A review. In *International Conference on Electronics and Renewable Systems (ICEARS'22).* IEEE, 1877–1883.

[197] Purushottam Sharma, Shaurya Kapoor, and Richa Sharma. 2023. Ransomware detection, prevention and protection in IoT devices using ML techniques based on dynamic analysis approach. *Journal of System Assurance Engineering and Management* 14, 1 (2023), 287–296.

[198] Shweta Sharma, C. Rama Krishna, and Rakesh Kumar. 2021. RansomDroid: Forensic analysis and detection of Android ransomware using unsupervised machine learning technique. *Forens. Sci. Int.: Digit. Investig.* 37 (2021), 301168.

[199] Shaila Sharmeen, Yahye Abukar Ahmed, Shamsul Huda, Bari Ş Koçer, and Mohammad Mehedi Hassan. 2020. Avoiding future digital extortion through robust protection against ransomware threats using deep learning based adaptive approaches. *IEEE Access* 8 (2020), 24522–24534.

[200] Shina Sheen, K. A. Asmitha, and Sridhar Venkatesan. 2022. R-Sentry: Deception based ransomware detection using file access patterns. *Comput. Electric. Eng.* 103 (2022), 108346.

[201] Shina Sheen and S. Gayathri. 2022. Early detection of Android locker ransomware through foreground activity analysis. In *3rd International Conference on Communication, Computing and Electronics Systems (ICCCES'21)*. Springer, 921–932.

[202] Anamika Singh, Md Akkas Ali, B. Balamurugan, and Vandana Sharma. 2022. Blockchain: Tool for controlling ransomware through pre-encryption and post-encryption behavior. In *5th International Conference on Computational Intelligence and Communication Technologies (CCICT'22)*. IEEE, 584–589.

[203] Jaskaran Singh, Keshav Sharma, Mohammad Wazid, and Ashok Kumar Das. 2023. SINN-RD: Spline interpolation-envisioned neural network-based ransomware detection scheme. *Comput. Electric. Eng.* 106 (2023), 108601.

[204] Daryle Smith, Sajad Khorsandroo, and Kaushik Roy. 2022. Machine learning algorithms and frameworks in ransomware detection. *IEEE Access* 10 (2022), 117597–117610.

[205] N. K. Sreelaja. 2021. Ant colony optimization based light weight binary search for efficient signature matching to filter ransomware. *Appl. Soft Comput.* 111 (2021), 107635.

[206] M. Sukul, S. Aswin Lakshmanan, and R. Gowtham. 2022. Automated dynamic detection of ransomware using augmented bootstrapping. In *6th International Conference on Trends in Electronics and Informatics (ICOEI'22)*. IEEE, 787–794.

[207] Veronika Szücs, Gábor Arányi, and Ákos Dávid. 2021. Introduction of the ARDS—Anti-Ransomware Defense System model—based on the systematic review of worldwide ransomware attacks. *Appl. Sci.* 11, 13 (2021), 6070.

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

[209] Usman Tariq, Imdad Ullah, Mohammed Yousuf Uddin, and Se Jin Kwon. 2022. An effective self-configurable ransomware prevention technique for IoMT. *Sensors* 22, 21 (2022), 8516.

[210] Shivani Tripathy, Debiprasanna Sahoo, Manoranjan Satpathy, and Madhu Mutyam. 2022. Formal modeling and verification of security properties of a ransomware-resistant SSD. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems* 42, 8 (2022), 2766–2770.

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

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

[213] Umara Urooj, Bander Ali Saleh Al-rimy, Anazida Zainal, Fuad A. Ghaleb, and Murad A. Rassam. 2022. Ransomware detection using the dynamic analysis and machine learning: A survey and research directions. *Appl. Sci.* 12, 1 (2022), 172.

[214] Chloe VonderLinden, Joseph Walton, Anthony Melaragno, and William Casey. 2022. The visualization of ransomware infection. In *IEEE International Conference on Dependable, Autonomic and Secure Computing, International Conference on Pervasive Intelligence and Computing, International Conference on Cloud and Big Data Computing, International Conference on Cyber Science and Technology Congress (DASC/PiCom/CBDCom/CyberSciTech'22)*. IEEE, 1–7.

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

[216] Senmiao Wang, Hua Zhang, Sujuan Qin, Wenmin Li, Tengfei Tu, Ana Shen, and Wentao Liu. 2022. KRProtector: Detection and files protection for IoT devices on Android without ROOT against ransomware based on decoys. *IEEE Internet Things J.* 9, 19 (2022), 18251–18266.

[217] Azka Wani and S. Revathi. 2020. Ransomware protection in loT using software defined networking. *Int. J. Electric. Comput. Eng. (2088-8708)* 10 (2020).

[218] Mohammad Wazid, Ashok Kumar Das, and Sachin Shetty. 2022. BSFR-SH: Blockchain-enabled security framework against ransomware attacks for smart healthcare. *IEEE Transactions on Consumer Electronics* 69, 1 (2022), 18–28.

[219] Wenqi Wei, Mu Qiao, Eric Butler, and Divyesh Jadav. 2022. Graph representation learning based vulnerable target identification in ransomware attacks. In *IEEE International Conference on Big Data (Big Data'22)*. IEEE, 2423–2430.

[220] Jarunee Wonglimpiyarat and Napaporn Yuberk. 2005. In support of innovation management and Roger's Innovation Diffusion theory. *Govern. Inf. Quart.* 22, 3 (2005), 411–422.

[221] Chutitep Woralert, Chen Liu, and Zander Blasingame. 2022. HARD-Lite: A lightweight hardware anomaly real-time detection framework targeting ransomware. In *Asian Hardware Oriented Security and Trust Symposium (AsianHOST'22)*. IEEE, 1–6.

[222] Bahaa Yamany, Marianne A. Azer, and Nashwa Abdelbaki. 2022. Ransomware clustering and classification using similarity matrix. In *2nd International Mobile, Intelligent, and Ubiquitous Computing Conference (MIUCC'22)*. IEEE, 41–46.

[223] Bahaa Yamany, Mahmoud Said Elsayed, Anca D. Jurcut, Nashwa Abdelbaki, and Marianne A. Azer. 2022. A new scheme for ransomware classification and clustering using static features. *Electronics* 11, 20 (2022), 3307.

[224] Yagiz Yilmaz, Orcun Cetin, Budi Arief, and Julio Hernandez-Castro. 2021. Investigating the impact of ransomware splash screens. *J. Inf. Secur. Applic.* 61 (2021), 102934.

[225] Yagiz Yilmaz, Orcun Cetin, Claudia Grigore, Budi Arief, and Julio Hernandez-Castro. 2023. Personality types and ransomware victimisation. *Digital Threats: Research and Practice* 4, 4 (2023), 1–25.

[226] Tongxin Yin, Armin Sarabi, and Mingyan Liu. 2023. Deterrence, backup, or insurance: Game-theoretic modeling of ransomware. *Games* 14, 2 (2023), 20.

[227] Adam Young and Moti Yung. 1996. Cryptovirology: Extortion-based security threats and countermeasures. In *IEEE Symposium on Security and Privacy*. IEEE, 129–140.

[228] Lena Yuryna Connolly, David S. Wall, Michael Lang, and Bruce Oddson. 2020. An empirical study of ransomware attacks on organizations: An assessment of severity and salient factors affecting vulnerability. *J. Cybersecur.* 6, 1 (2020), tyaa023.

[229] Javier Yuste and Sergio Pastrana. 2021. Avaddon ransomware: An in-depth analysis and decryption of infected systems. *Comput. Secur.* 109 (2021), 102388.

[230] Umme Zahoora, Asifullah Khan, Muttukrishnan Rajarajan, Saddam Hussain Khan, Muhammad Asam, and Tauseef Jamal. 2022. Ransomware detection using deep learning based unsupervised feature extraction and a cost sensitive Pareto ensemble classifier. *Scient. Rep.* 12, 1 (2022), 15647.

[231] Temechu Girma Zewdie, Anteneh Girma, and Paul Cotae. 2022. Ransomware attack detection on the Internet of Things using machine learning algorithm. In *HCI International 2022–Late Breaking Papers: Interacting with eXtended Reality and Artificial Intelligence: 24th International Conference on Human-Computer Interaction, HCII 2022, Virtual Event, June 26–July 1, 2022, Proceedings*. Springer, 598–613.

[232] Chunming Zhang, Fengji Luo, and Gianluca Ranzi. 2022. Multistage game theoretical approach for ransomware attack and defense. *IEEE Transactions on Services Computing* 16, 4 (2022), 2800–2811.

[233] Xueqin Zhang, Jiyuan Wang, and Shinan Zhu. 2021. Dual generative adversarial networks based unknown encryption ransomware attack detection. *IEEE Access* 10 (2021), 900–913.

[234] Xiang Zhang, Ziyue Zhang, Ruyi Ding, Cheng Gongye, Aidong Adam Ding, and Yunsi Fei. 2022. Ran $ Net: An anti-ransomware methodology based on cache monitoring and deep learning. In *Great Lakes Symposium on VLSI*. 487–492.

[235] Yipeng Zhang, Min Li, Xiaoming Zhang, Yueying He, and Zhoujun Li. 2022. Defeat magic with magic: A novel ransomware attack method to dynamically generate malicious payloads based on PLC control logic. *Appl. Sci.* 12, 17 (2022), 8408.

[236] Jinting Zhu, Julian Jang-Jaccard, Amardeep Singh, Ian Welch, A. I.-Sahaf Harith, and Seyit Camtepe. 2022. A few-shot meta-learning based siamese neural network using entropy features for ransomware classification. *Comput. Secur.* 117 (2022), 102691.

[237] Danyil Zhuravchak, Taras Ustyianovych, Valery Dudykevych, Bogdan Venny, and Khrystyna Ruda. 2021. Ransomware prevention system design based on file symbolic linking honeypots. In *11th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS'21)*. IEEE, 284–287.

[238] Hiba Zuhair, Ali Selamat, and Ondrej Krejcar. 2020. A multi-tier streaming analytics model of 0-Day ransomware detection using machine learning. *Appl. Sci.* 10, 9 (2020), 3210.

Received 13 March 2023; revised 15 July 2024; accepted 27 August 2024