IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 6 October 2023, accepted 17 October 2023, date of publication 30 October 2023, date of current version 3 November 2023.

Digital Object Identifier 10.1109/ACCESS.2023.3328351

SURVEY

A Review of State-of-the-Art Malware Attack Trends and Defense Mechanisms

JANNATUL FERDOUS[1], **RAFIQUL ISLAM**[2], **ARASH MAHBOUBI**[3], **AND MD. ZAHIDUL ISLAM**[4]

[1]School of Computing, Mathematics and Engineering, Charles Sturt University, Wagga Wagga, NSW 2650, Australia
[2]School of Computing, Mathematics and Engineering, Charles Sturt University, Albury, NSW 2640, Australia
[3]School of Computing, Mathematics and Engineering, Charles Sturt University, Port Macquarie, NSW 2444, Australia
[4]School of Computing, Mathematics and Engineering, Charles Sturt University, Bathurst, NSW 2795, Australia

Corresponding author: Jannatul Ferdous (jferdous@csu.edu.au)

This work was supported by the Charles Sturt University (CSU) Ph.D. Project Operating Fund.

ABSTRACT The increasing sophistication of malware threats has led to growing concerns in the anti-malware community, as malware poses a significant danger to online users despite the availability of numerous defense solutions. This study aims to comprehensively review malware evolution and current attack trends to identify effective defense mechanisms. It reviews the most recent journal articles, conference proceedings, reports, and online resources published during the last five years. We extensively review the malware landscape from 1970 to the present and analyze malware types, operational mechanisms, attack vectors, and vulnerabilities. Furthermore, we explore different defensive strategies developed in response to these evolving threats. Our findings highlight the increasing sophistication of malware attack trends, including a surge in cryptojacking, attacks on mobile devices, Internet of Things devices, ransomware, advanced persistent threats, supply chain attacks, fileless malware, cloud-based attacks, exploitation of remote employees, and attack trends on edge networks. Defense strategies have also evolved in parallel, emphasizing multilayered security measures to counter these dynamic threats. This study highlights the critical need for robust, multilayered security measures to combat dynamic malware. Despite these advancements, some open challenges and significant research gaps remain, which require further innovation. This review serves as a valuable guide for cybersecurity professionals by identifying the key trends, challenges, limitations, and future cybersecurity research opportunities.

INDEX TERMS Malware evolution, malware attack trends, defense mechanisms, malware detection, machine learning, deep learning.

I. INTRODUCTION

In the current digital era, malware attacks and defenses are becoming increasingly complex, creating an evolving cyberthreat landscape. Malware, which is characterized as deleterious software, infiltrates host systems, impairs operating systems or networks, and causes many complications, including data exfiltration. With the rapid progress in technology, malware threats have exhibited enhanced potency and intricacy, often exceeding the capabilities of traditional defense systems. This scholarly examination provides an exhaustive review of the emerging trends in malware assaults and their associated defensive structures.

Despite advances in technology and cybersecurity, malware attacks remain a challenge for netizens, as threat actors seek to make money or trade by stealing personal data, bank accounts, and credit statements. According to a report by DataProt, 560,000 new types of malware are detected daily, and the internet is currently flooded with over one billion malware programs [1]. PurpleSec found that the average data breach cost was $3.86 million, and cybercrime could cost $10.5 trillion by 2025, indicating increasing concerns about malware attacks [2]. According to Parachute in 2023, the financial sector suffered losses of over $49,207,908

The associate editor coordinating the review of this manuscript and approving it for publication was Chao Tong.

© 2023 The Authors. This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 License.
For more information, see https://creativecommons.org/licenses/by-nc-nd/4.0/

from ransomware in 2021, and phishing attacks against banks accounted for 23.2% of these losses [3]. In addition, SonicWall's latest report revealed that during the first half of 2023, malware volume peaked at 575 million in June, representing a 46% increase from the 395 million hits recorded in January, as shown in Figure 1 [4]. The recent statistical threat report mentioned above highlights that malware is causing increasing damage to the global economy in terms of quantity, complexity, and cost. To combat these threats, it is crucial to understand recent malware attack trends and the corresponding defense strategies.

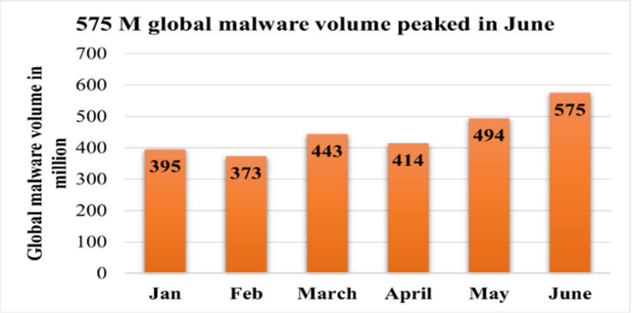


FIGURE 1. The increasing rate of global malware volume (Q1, 2023).

With the blessings of AI technology, cybercriminals can carry out targeted attacks quickly and on a larger scale, while bypassing traditional detection methods. Intelligent self-learning malware is an example of an AI-based cyberattack [5]. Polymorphic and metamorphic malware can fall into this category and reshape their appearance by altering their code with or without a different encryption key [6]. This evolution of malware has resulted in sophisticated threats, such as espionage, ransom, and sabotage, which pose considerable challenges to individuals, businesses, and governments. Several recent studies and threat reports have warned of various emerging trends in attacks, such as Emotet, which is dangerous malware. It began as a banking trojan, changed to polymorphic malware to steal data, and is now active again [4], [7]. Remote access trojans (RATs) and banking trojans have also been used in recent attacks [8]. Ransomware attacks have recently become increasingly sophisticated and frequent. For example, in 2021, ransomware was the top cyber threat, with attacks increasing by 140% in the third quarter [9]. Fileless attacks are another emerging trend in malware attacks that do not leave traces in the system; therefore, they are difficult to detect [10], [11], [12]. Advanced persistent threats (APTs) are highly complex, target-specific, persistent, and remain undetected until the target is compromised [13], [14]. In addition, cryptojacking [4], mobile malware [15], Internet of Things (IoT) [4], cloud attacks [16], and attack trends in edge networks [17] have become increasingly frequent and complex. Exploring these modern attack trends forms a primary focus of this review, as understanding the 'enemy' is the first step in building a robust defense.

In the last decade, most reviewed articles on malware discussed detection, approaches, and challenges. A common theme is the increasing importance of machine- and deep-learning techniques, as noted by Gibert et al. [18], Tayyab et al. [19], and Gopinath and Sethuraman [20]. However, these studies lacked a comparison with other techniques and temporal effectiveness analysis. Aslan and Samet [21] and Roseline and Geetha [22] surveyed detection and mitigation techniques but lacked a performance evaluation. Huang et al. [23] and Zhang et al. [24] explored malware detection through evasion tactics and memory forensics but did not address the evolution or practicality of defiance strategies. Shaukat et al. [25] proposed deep learning techniques without comparing them with existing methods. The authors of [26], [27], [28], [29], [30], and [31] only studied ransomware detection and defense solutions, and no other malware types. Similarly, [10], [11], [13], [32], [33], [34], [35], and [36] studied APT and fileless malware detection and prevention. In addition, Wang et al. and Liu et al. examined deep learning-based detection against Android malware [37], [38], offering a thorough analysis but they did not fully explore practical implementation and malware evolution. Several studies have investigated malware detection in IoT devices [39], [40], [41]. However, there is a lack of practicality and robustness in malware detection, and a failure to account for the ever-changing nature of IoT threats.

Following a thorough examination of the extant literature, it is noted that most research on malware detection uses machine and deep learning, not comprehensive defense solutions. It is critical to emphasize that malware detection alone does not provide a complete safeguard against modern malware; it is only one part of a multilayered defense mechanism. In addition, most survey studies have focused on certain malware types, such as ransomware or fileless malware, without considering others. Hence, comprehensive research is required to provide a complete picture of malware evolution, contemporary attack trends, and defense solutions. To our knowledge, no studies have been conducted on this topic. This is a significant research gap as technology advances and more devices are connected to global networks, thereby increasing the number of attack surfaces. However, an understanding of these threats is incomplete without a parallel study of the defense strategies designed to combat them.

This study aims to fill these gaps by comprehensively reviewing current malware attack trends and defense strategies. In this study, we explored malware evolution, ranging from the Creeper virus (1971) to widespread ransomware and other currently evolving attacks, to better understand the trends and tactics employed in such attacks, as illustrated in Figure 2. Our analysis revealed the latest sophisticated attack trends, including a dramatic increase in cryptojacking, ransomware attacks, APTs, supply chain attacks, fileless malware, and malware attacks on mobile devices, Internet of Things devices, and edge networks. We scrutinized threat vectors, vulnerabilities, attack targets, innovative tactics,

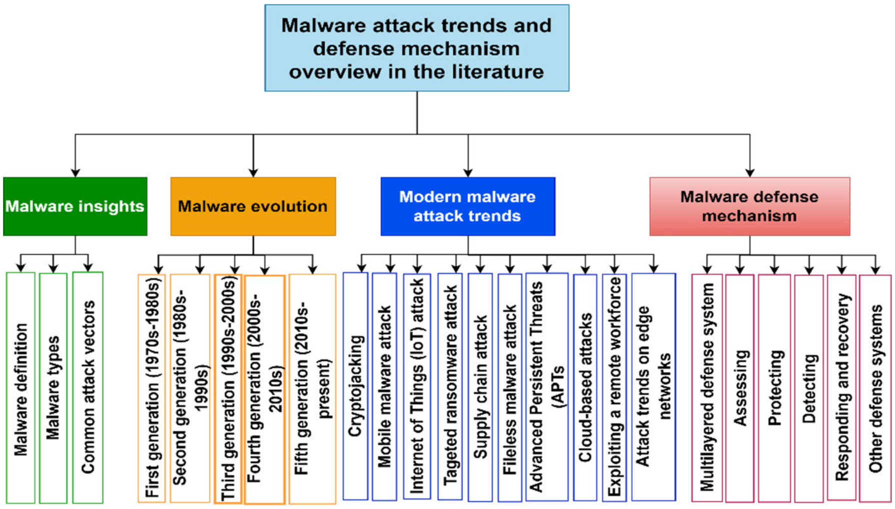

Malware attack trends and defense mechanism overview in the literature
Malware insights
Malware evolution
Modern malware attack trends
Malware defense mechanism
Malware definition
Malware types
Common attack vectors
First generation (1970s-1980s)
Second generation (1980s-1990s)
Third generation (1990s-2000s)
Fourth generation (2000s-2010s)
Fifth generation (2010s-present)
Cryptojacking
Mobile malware attack
Internet of Things (IoT) attack
Tageted ransomware attack
Supply chain attack
Fileless malware attack
Advanced Persistent Threats (APTs
Cloud-based attacks
Exploiting a remote workforce
Attack trends on edge networks
Multilayered defense system
Assessing
Protecting
Detecting
Responding and recovery
Other defense systems

FIGURE 2. Roadmap of this study. Upon analyzing malware evolution, we aim to identify the most current trends in malware attacks and suitable defense strategies by going through this outline.

TABLE 1. Classification of malware based on purpose and information-sharing system.

Malware type	Description	Use cases	Existing defense mechanisms
Virus [22]	Malware that copies itself and spreads when programs are shared.	Infecting executable files, boot sectors, email attachments, and macros.	Antivirus software, firewalls, awareness training, and limit file-sharing.
Trojan [43]	Malware masked as legitimate software to gain illegal access.	Data theft, download additional malware onto computer and then bypass security settings.	Intrusion detection system, antivirus program and system update regularly.
Worm [21]	Self-replicating malware that spreads to other systems through network vulnerabilities.	Targeting specific systems or networks, stealing data, and accelerating network traffic.	Network security tools, patch management, and user education.
Ransomware [44]	Malware that encrypts files and demands ransom for their release.	Encrypting files on a network or system, disrupting business operations.	Backup and recovery tools, endpoint detection, multiple security measures and antivirus solution.
Adware [22]	Malware that displays unwanted advertisements or pop-ups.	Attackers gain money and collect sensitive data through fake ads.	Antivirus software, ad-blocking software, user education, system updates.
Rootkit [22]	Rootkits modify operating system (OS) functions to conceal their presence.	Making detection harder by being persistent and stealthy.	Ongoing software updates and advanced antivirus solution.
Keyloggers [43]	Keyloggers steal passwords and credit card numbers by recording keyboard inputs.	Steal passwords and credit card numbers.	Manage passwords with password manager, implement multifactor authentication, etc.

and case studies on well-known malware attacks. Furthermore, this study explored multilayered and other defense strategies, ranging from traditional antiviral software to advanced artificial intelligence and machine learning-based solutions. Finally, this study identifies the major challenges and significant research gaps in malware detection and protection.

The key contributions of this paper are as follows:

- We survey malware evolution from 1970 to the present and discuss its history, features, and development to help understand current attack trends.
- We analyze the latest malware attack trends to gain insight and investigate effective countermeasures.
- This study highlights the need for multilayered security measures to defend against intelligent and dynamic malware.
- Finally, we identify the challenges and limitations of the current study and offer ideas and suggestions for future research.

The remainder of this paper is organized as follows. Section II presents insights into malware. Section III provides a taxonomy of malware evolution. Section IV explores modern malware attack trends and case studies on recent high-profile attacks. Section V reviews malware defense mechanisms and other protective strategies. Section VI presents the challenges, limitations and research gaps in the literature. Finally, Section VII concludes the paper.

II. AN INSIGHT INTO MALWARE

Knowing the fundamentals of malware is essential for effective cyberdefense against modern threats. This section covers malware basics.

A. MALWARE DEFINITION

Malware is malicious software designed to compromise system security and make illegal profits. Its criminal activities include data breaches and identity theft and it can be spread via various executable or software vectors [42].

B. MALWARE TYPES AND COMMON ATTACK VECTORS

1) CLASSIFICATION OF MALWARE

We categorized malware according to its aims and methods using information from the literature [18], [22], as outlined in Table 1.

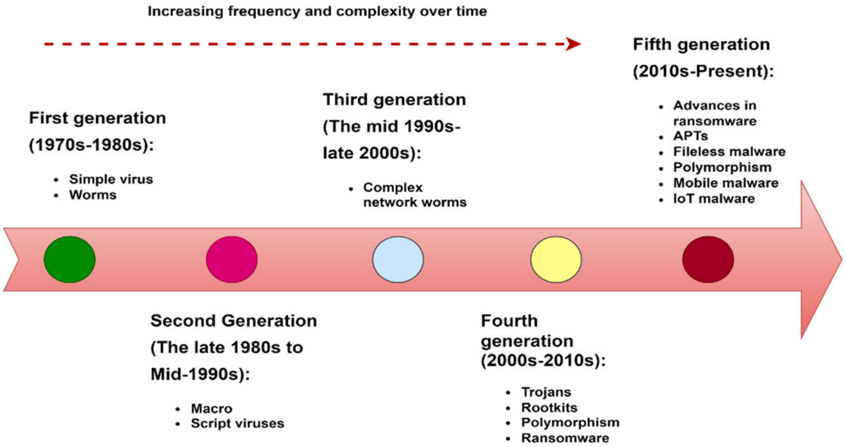


FIGURE 3. The ongoing evolution of malware reflects the persistent efforts of cybercriminals to bypass security measures and exploit new vulnerabilities.

2) COMMON ATTACK VECTORS

Cybercriminals constantly invent new ways to infiltrate the victim's system and steal sensitive data. Popular malware propagation sources are included in [41] and [45].

Drive-by Download: Attackers may infect secure webpages or ads with malware to exploit user data, causing accidental downloads.

Backdoors: Backdoors such as FinSpy allow unauthorized access to a computer, enabling remote malware installation and malicious script execution by the attackers.

Phishing: Typical malware attacks. Attackers trick trustworthy sources by manipulating users to trigger malware by using deceptive links or downloads.

Removable drives: Removable drives such as flash drives and hard disks are familiar sources of malware transfer, including viruses, worms, and ransomware.

Vulnerabilities: Malware authors often exploit operating systems, browsers, or other software flaws using tools, such as exploit kits, to leverage known or zero-day vulnerabilities.

III. THE EVOLUTIONARY LADDER OF MALWARE OVER TIME

We classified malware development into five generations based on their era of origin and features. Figure 3 shows the typical characteristics of each generation.

A. FIRST-GENERATION MALWARE (1970s–1980s): SIMPLE VIRUSES AND WORMS

Thomas Bob–were the first computer virus creepers to perform self-replicating tests in 1971. Elk Cloner hit Apple II in 1982, followed by the 'Brain' virus in 1986. Morris 1988 created the first computer worm, Morris Worm [46]. In 1989, Joseph Popp led the first ransomware, AIDS Trojan, demanding a ransom after infection [47].

B. SECOND-GENERATION MALWARE (THE LATE-1980s TO THE MID-1990s): MACRO AND SCRIPT VIRUSES

The mid-90s saw second-generation malware such as Microsoft Word macro language (WM Concept) and X97M/Laroux used macros and scripting [48]. In 1999, the Melissa virus disrupted the email system [49].

C. THIRD-GENERATION MALWARE (THE MID-1990s TO LATE-2000s)COMPLEX NETWORK WORMS

Third-generation malware, called network worms, exploit network vulnerabilities. Examples include the 'ILOVEYOU' worm [49], Code Red [50], and Nimda [51].

D. FOURTH-GENERATION MALWARE (2000s–2010s): THE EMERGENCE OF TROJANS, ROOTKITS, POLYMORPHISM, AND RANSOMWARE

Fourth-generation malware evolved into polymorphism, trojans, rootkits, and ransomware. The initially harmless trojans became a significant threat to cybersecurity with the emergence of sophisticated trojans, such as Beast in 2002 [52], Zeus in 2007 [53], and Tor-pig in 2008 [54]. A recent advancement is Taidoor, a RAT associated with the Chinese government [55]. In 1999, Sony Entertainment created the first Windows rootkit, SONY BMG, leading to CD recalls [56]. Over time, rootkits such as FuTo and Mebroot have advanced, demonstrating the need for boot-process security [57]. The Alureon/TDL-4 Rootkit in 2011 highlighted the complexity of data breaches [58]. Ransomware originated with the AIDS Trojan and evolved with programs such as Gpcoder, CryZip, Archives [59], [60], and Krotten [61]. Locker ransomware appeared in 2008, and the advent of cryptocurrencies in 2009 facilitated more attacks owing to secure and anonymous payments [62].

E. FIFTH-GENERATION MALWARE (2010s–PRESENT): ADVANCES IN RANSOMWARE, APTs, FILELESS MALWARE, POLYMORPHISM, MOBILE MALWARE, AND IoT MALWARE

Our review found that fifth-generation malware is the most damaging, elusive, and efficient and uses techniques such as polymorphism and metamorphism [63], [64], living-off-the-land strategies [35], [65], encryption [26], [28], exploiting vulnerabilities, and other innovative tactics.

Ransomware changed from CryptoLocker's RSA encryption and Bitcoin in 2013 [26] to NotePetya and WannaCry [66]. In 2019, corporate-focused ransomware, such as Ryuk [67], Ransomware-as-a-Service (RaaS), double extortion, and bug bounty tactics by Conti and Revil, improved the ransomware landscape [68].

Ransomware attacks surged in 2020 due to Covid-19 [69] and skyrocketed in 2021, with significant incidents, such as the Colonial Pipeline [70], JBS [71], and Kaseya [72]. Although attacks decreased in 2022 [73], threats remain with new techniques such as triple extortion and BlackCat's Rust language [74]. State actors developed malware such as Stuxnet and Flame, disrupting Iran's nuclear program and spying in the Middle East in 2010 and 2012 [49], [75]. APT attacks, such as Hydraq, Operation Aurora, and Carbanak [76] are notable. In 2020, the APT29 conducted SolarWinds supply chain attacks [77], [78]. Finally, long-standing snake malware was neutralized in 2023 by Perseus [79].

Cybercriminals have shifted their focus from file-based to fileless malware attacks and living-off-the-land (LotL) tactics to increase sophistication in cyber threats. This poses new challenges for detection. ToddyCat (2022) defines these threats using system tools or memory scripts [80]. This trend led to a 900% increase in the infiltration rate [81]. Zero-day exploits rose over 100% in 2021 compared to 2019, targeting Microsoft, Google, and Apple [82]. Twitter Zero-Day Exposed is a recent example [83]. Another current attack trend is the substantial spike in cryptojacking [4]. Furthermore, both Apple and Android phones are rising targets of cybercriminals. However, Android's open marketplace and third-party app stores may render it more vulnerable. FluBot [15] and Exodus Spyware [84] are the most recent and notorious examples of mobile malware. IoT devices are highly exposed to network attacks such as data theft, DDoS, ransomware, and data breaches, leading to recovery costs and downtime. Mirai botnet (2016), Verkada (2021), Jeep Hack (2015), and Stuxnet (2010) are examples of IoT cyber threats [85]. Recently, BlackMamba ChatGPT malware plans to use generative AI to create elusive variants by 2023 [86]. This growing threat complexity necessitates urgent and innovative countermeasures.

F. SUMMARY OF THE FINDINGS IN MALWARE EVOLUTION

Table 2 summarizes malware generation from 1970 to the present in terms of the emergence period, target platforms, initial access methods, key characteristics, and destruction. The key findings of each generation are as follows:

- Table 2 shows that the first generation of malware marked the birth of self-replicating codes, which were typically spread via floppy disks or MS-Word documents, with harmless payloads. The primary purpose of this study was to demonstrate technical skills such as the Creeper virus.
- Second-generation malware targeting Windows software emerged from the late 1980s to the mid-1990s. The malware in this generation accessed systems by exploiting software vulnerabilities through email attachments, particularly Word, Excel, and Melissa. Although less harmful, this paved the way for more destructive malware attacks.
- Third-generation malware, from the mid-1990s to the late-2000s, included complex network worms that primarily targeted Windows and other systems. For example, the 'ILOVEYOU' worm exploited network vulnerabilities and used social engineering to spread and infect millions of computers. Code Red and Nimda used multiple propagation methods and caused billions of dollars in damages.
- The fourth malware generation (2000s–2010s) used advanced techniques for stealth and evasion, mainly targeting Windows. It resulted in boosting cyber security. This period saw the emergence of ransomware, which poses a significant risk to encrypting user data.
- Table 2 shows that the fifth or current generation of malware has evolved into highly sophisticated forms since 2010, targeting a more comprehensive range of platforms, including Windows, Linux, Mobile, IoT, and network systems. According to the literature, some of these factors are unknown. Some malware types have become powerful weapons because they cause severe damage without affecting human life. For example, APTs can remain in a system to launch sophisticated attacks. We also found that modern malware leverages cutting-edge strategies, such as the RasS model, double and triple extortion, and high-level programming languages to maximize financial gains, scale, and evade detection.

Based on the information in Table 2, we further categorized the chronological evolution of malware trends, focusing on the most recurring attack vector, the initial access approach, and the primary purpose of the attack, as shown in Figure 4.

- Considering the target platforms summarized in Table 2, Windows is the most popular target for notable malware strains because most end users, organizations, and enterprises use this popular and user-friendly operating system. Figure 4(a) shows that only 21.2% of the malware author's attacks targeted other platforms.
- Regarding the initial access method illustrated in Figure 4 (b), phishing and exploiting vulnerabilities are the two most popular infection methods used in modern malware. Spam emails, floppy disks, drive-by downloads, Smishing, and MS-Word documents are infection methods that follow phishing and vulnerability.
- Figure 4 (c) shows that the primary purpose of malware, particularly in the modern age, is to perform malicious activities and earn financial profit.

Our review of malware evolution reveals that prior studies have mainly focused on technical aspects, such as defining and types of malware and not on their consequences for defense strategies. To address this issue, we studied the behaviors of malware, targets, and damaging actions

TABLE 2. Summary of significant malware evolution of five generations.

Malware strains	First seen	Platform	Infection method	Target/characteristics	Destruction
First-generation malware (the 1970s–1980s)					
Creeper virus	1971	Windows	ARPANET network.	To check if a code can duplicate itself.	No intention to be malicious.
Elk Cloner virus	1982	Apple II	Floppy disks.	The first boot sector virus observed "in the wild."	It was created as a prank with no malicious intention.
Morris's worm	1988	Windows	Send mail/SMTP.	Rise network activities to crash the internet.	Around 10% of the 60,000 computers were affected.
AIDS Trojan	1989	Windows	Floppy disks.	The distributor masked floppy disks as AIDS surveys to spread viruses.	He demanded a ransom of $189/year or $385/lifetime from the attendees of the WHO AIDS conference.
Second-generation malware (the late-1980s to mid-1990s)					
W.M. Concept	1995	Windows	MS-Word documents.	MS-Word.	It duplicates itself harmlessly.
X97M/Laroux	1996	Windows	Infected MS-Word files.	MS-Excel.	The infected file replaces the original file.
Melissa	1999	Windows	Email attachment.	Use features of both macros and worms.	It caused $80 million in damages.
Third-generation malware (the mid-1990s to late-2000s)					
'ILOVEYOU' worm	2000	Windows and others	Social engineering.	Microsoft Outlook users.	Compromised millions of computers worldwide.
Code Red	2001	Windows	Vulnerability in web server.	A first large-scale attack on enterprise networks.	Infected more than 3.59K computers and caused billions in damages.
Nimda	2001	Windows	Email attachments, modified websites.	They targeted both servers and client machines using multiple attack vectors.	The estimated damages amount to $2.6 billion.
Fourth-generation malware (the 2000s–2010s)					
Trojan (Beast)	2002	Windows	Email attachments.	Can bypass firewall restrictions and remote administration.	They allow the attacker complete control over the compromised computer.
Trojan Zeus	2007	Windows	Drive-by downloads and phishing.	Zeus employed stealth tactics to make it hard to be detected.	Steal data from the U.S. Department of Transportation.
Sony BMG Rootkit	2005	Windows	Music CDs.	To stop illegal copying of Sony's publications.	It affected their reputation.
Mebroot Rootkit	2007	Windows	Drive-by downloads.	Difficult to detect because it lacked executable files, registry keys, etc.	It infected computers by gaining control of the boot process.
Gpcoder	2005	Windows	Spear-phishing.	The first usage of symmetric encryption.	Encrypted files and asked for ransom.
CryZip, Archievus, and Krotten	2006	Windows	Spam email, drive-by downloading.	The first use of asymmetric encryption.	Delete, overwrite, and ask for ransom using a prepaid voucher.
Randsom.C	2008	Windows	Spam.	Appeared as the first locker ransomware.	Demanded ransom through SMS.
Fifth-generation malware (2010s–present)					
Stuxnet	2010	Windows	USB Stick.	To disrupt Iran's nuclear program.	Caused damage to over 1000 machines.
CryptoLocker	2013	Windows	Phishing.	Applied asymmetric encryption method.	The first use of Bitcoin as extortion.
Emotet	2014	Windows and network	Email Phishing.	Cybercriminals hire Emotet to install additional types of malware.	Financial gain.
WannaCry	2017	Windows	Vulnerability.	This attack used the hard-coded I.P. address for C&C communication.	Encrypted with AES & RSA and deleted files. Damage was around $100 million.
Snake malware	2018	Windows	Vulnerabilities.	It stole sensitive information from Industrial Control Systems.	Data stolen from over 50 countries and 100 computer systems.
Conti and REvil	2019	Windows, Linux	Vulnerability.	Used RaaS model, stole information and threat for double extortion.	Cost $45 million and $6 million.
SolarWinds	2020	Windows	Phishing.	Infiltrated the SolarWinds software supply chain.	Affected 18,000 users of Orion products in the U.S.
Corona	2020	Windows	Phishing.	Targeted health organizations.	Encryption (AES & RSA) and overwrite.
FluBot	2020	Mobile	Smishing.	Worm-like spreading to infect address books.	Steal login info from banks and other sites.
Colonial Pipeline	2021	Windows	Vulnerability.	System operation was closed for seven days.	The cost of the data breach was USD 4.4 million.
Verkada	2021	Cloud-based IoT devices	Legitimate admin account credentials.	Cameras in factories, hospitals, schools, prisons, etc.	Infected over 150,000 customer cameras.
LockBit	2022	Unknown	Compromised systems.	It used the RaaS model, double extortion tactics, and the bug bounty concept.	192 attacks affecting 41 countries.
ToddyCat	2022	Windows	Spear-phishing emails.	Backdoor facilitated stealthy network infiltration and persistent covert presence.	Identity theft, financial loss, and emotional distress.
Twitter Zero-Day attack	2022	Windows	Unknown vulnerabilities.	This attack undermined the integrity of Twitter's platform and user trust.	The attackers stole the personal information of 5.4 million accounts.
BlackCat	2023	Unknown	Initial Access Brokers (IABs).	Critically designed using rust programming to avoid detection.	Infected more than 350 victims as of May 2023.

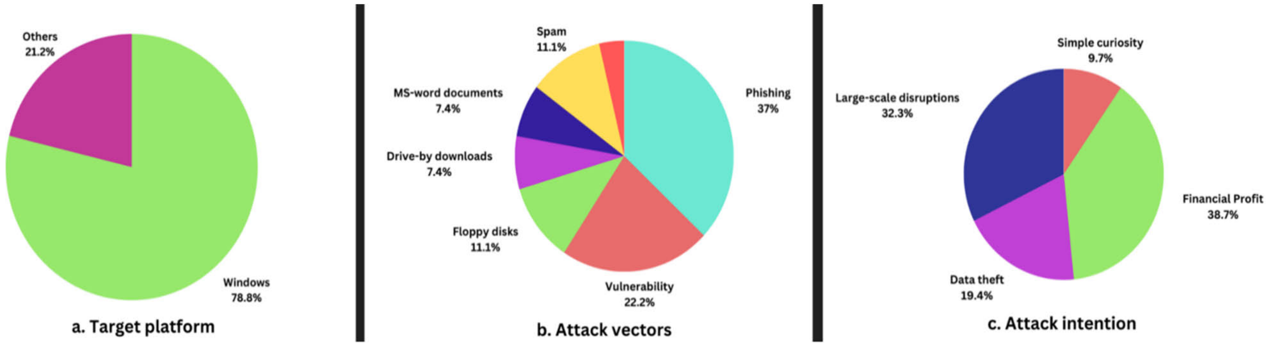


FIGURE 4. Dispersion of (a) target platform, (b) attack strategies, and (c) attack goals of notable malware families from 1970 to the present.

to provide clear insights into sophisticated attack trends. Our findings indicate that recent malware has attempted to bypass AV/AM techniques, which is a primary concern for the research community. Therefore, finding a robust solution for malware detection remains a challenge.

IV. CURRENT MALWARE ATTACK TRENDS

Recently, the frequency and complexity of malware attacks have increased significantly, posing extensive threats to individuals and organizations. By studying the evolution of malware, including our previous research [87], we identified the most current attack trends encompassing attack methods, case studies, and their impacts, which are detailed in this study, to facilitate the formulation of effective defense strategies.

A. RECORD RISE IN CRYPTOJACKING ATTACKS

Cryptojacking is the unauthorized use of a victim's computer resources to mine a cryptocurrency. SonicWall's latest report reveals that cybercriminals are shifting from ransomware to covertly mine digital currencies for financial gain. In the first half of 2023, the number of cryptojacking attacks surpassed 332 million, compared to 66.7 million in the corresponding period of 2022. Cybercriminals adjust tools, tactics, and procedures to improve their success. For instance, they moved from attacking endpoints to cloud services, such as using Kubernetes clusters to mine Dero.

Key Characteristics We found some specific characteristics of cryptojacking attacks in the literature, including:

- Cryptojacking attacks use a victim's device to mine cryptocurrency, resulting in high CPU usage [88].
- Graphics processing units (GPUs) are now accessible to computers, making them attractive for cryptojacking [88].
- Vulnerable routers are lucrative attack vectors for cryptojacking attacks [89].
- Cryptojacking uses malicious scripts to mine cryptocurrencies, which can be found in the victim's browser cache or a hacked website's source code [90], [91].

These specific characteristics, such as increased CPU usage, compromised graphics processing units (GPU), vulnerable routers, and malicious scripts of cryptojacking attacks, can be used as indicators for detection using advanced machine-learning techniques.

For example, in late March 2023, cybercriminals included a new variant of Async RAT malware designed to steal cryptocurrencies [4]. The new variant has extra command support, clippers, crypto stealers, and keylogger modules, and stops system sleep. SonicWall RTDMI identifies a JavaScript file that downloads and runs fileless AsyncRAT.

B. MOBILE MALWARE ATTACKS

Among the recent malware attack trends, mobile malware has grown significantly in sophistication and frequency. The surge in mobile device usage and dependency offers a golden opportunity for cybercriminals to target naïve users. Researchers observed a 500% surge in mobile malware attacks in early 2022, with two peaks in February [15].

Key characteristics: Mobile malware attacks share certain characteristics as follows:

- Mobile malware drains battery power and communicates with command-and-control servers, thereby leading to higher data usage. A sudden battery drain without a change in the usage pattern may indicate malware [92].
- If new apps appear on a device that the user has not downloaded, it may indicate malware [93].
- Malware can cause applications or devices to crash frequently.
- Certain malware may make unauthorized payments via SMS or even online [94].

Mobile malware attacks can be identified early using AI tools by analyzing unexpected characteristics, such as battery drain, increased data usage, unfamiliar apps, frequent crashes, and unauthorized payments.

Case study of Exodus Spyware as a mobile malware attack (2019): One notable example of mobile malware is Exodus Spyware targeting iPhones and Android phones, which caused an alarm after being discovered in 2019. Once installed on a device, it can obtain root permissions, giving attackers complete control of the device and access to all data, thereby raising substantial privacy concerns [84]. Based on the analysis of the attack traits, it became apparent that command-and-control server security measures were inadequate.

C. INTERNET OF THINGS (IoT) ATTACKS

SonicWall shows 7.9 million IoT malware attacks in the first half of 2023, a 37% increase from the same period in 2022. This attack level surpasses the full-year total for 2020 and 2021 and the combined totals for 2018 and 2019 [4]. With the growing number of IoT devices, such as smart gadgets and sensors, common security weaknesses and valuable data make them prime targets for cybercriminals. Cybercriminals exploit these devices for multiple destructive purposes, such as prompting DDoS attacks, espionage, stealing data, and sabotage.

Key characteristics: IoT malware has distinct features and attack behaviors, as follows:

- Malware-infected IoT devices have large abnormal traffic patterns that can be detected by analyzing packet headers, size, and distribution [95].
- Stealth is an IoT malware feature that hides files, boot sectors, and partitions [40].
- Some IoT malware converts infected devices from the worm category into networks, honeypots, and proxy servers such as Moose, TheMoon, and OMG [40].
- Malware often modifies the configuration of IoT devices; this can be detected by comparison with a known good configuration [95].
- IoT malware often prevents rebooting to avoid deletions; however, rebooting usually removes malware [40].

Monitoring these characteristics can enable early identification of IoT attacks and possible remedies.

Case study of Mirai botnet as a malware attack on IoT devices: This attack was first identified in 2016 and has attacked many IoT devices to create a network of compromised units that are then used to launch DDoS assaults. This attack shuts down popular websites like Twitter, Netflix, and GitHub. This real-life scenario illustrates the impact of malware attacks on devices and highlights the importance of safeguarding these devices against widely recognized vulnerabilities [96].

D. INCREASED NUMBER OF TARGETED RANSOMWARE ATTACKS

Recent malware trends have highlighted increased targeted ransomware attacks, in which hackers access a network or system, encrypt data, and demand a ransom to restore access. This increase in ransomware attacks is driven by several factors, including potential financial gains, easy operation, the rise of ransomware-as-a-service platforms, and the popularity of cryptocurrencies like Bitcoin [97]. Ransomware attacks are wide-ranging, targeting everything from desktops and mobile devices and increasingly involving IoT devices.

Key characteristics: Ransomware attacks exhibit the following specific characteristics:

- Ransomware often exhibits abnormal file behavior, such as encrypting files at a rapid rate or modifying file extensions [30].
- This may generate unusual network traffic patterns, such as a sudden increase in outbound connections or communication with suspicious IP addresses [31].
- Often, they propagate through spam emails and phishing attacks [30].
- It often exploits the vulnerabilities of a system [26].
- Ransomware targets an array of devices, including desktops, mobile devices, and IoT devices [26].

Therefore, network traffic spikes, encrypted files, system modifications, and malicious emails with attachments or links are signs of ransomware attacks. AI tools such as machine learning and deep learning can detect and address these indicators early.

Case study of the Colonial Pipeline as a ransomware attack: We chose the Colonial Pipeline ransomware attack for our case study in which the U.S. oil transportation entity fell victim to a sophisticated ransomware attack in May 2021 by DarkSide through a compromised Virtual Private Network (VPN) account [98]. Attackers carried out this operation in several stages: initial system breach via a dormant VPN account, network surveillance, loading of the ransomware, and, ultimately, the ransom demand. The attack caused a 45% energy supply disruption, fuel shortages, and price hikes [99]. An analysis of the attack characteristics indicates the presence of outdated VPNs and vulnerable network security measures. This scenario highlights the significance of understanding the attack characteristics and vulnerabilities for timely detection and response.

E. SUPPLY CHAIN ATTACKS

Supply chain attacks have recently emerged as a significant and growing threat to cybersecurity. These attacks have extensive implications for both organizations and customers [100].

Key characteristics: The main characteristics of supply chain attacks are as follows [101].

- Supply chain attacks are well-planned, sophisticated, and tend to be legitimate software updates to avoid suspicion.
- Large scale and highly damaging.
- The attacker infiltrates a trusted vendor or supplier and introduces malicious code or backdoors into software or system components early in the supply chain.
- A large amount of data can be transferred to or from third-party vendors.
- Sometimes, it generates fake websites and sends phishing emails to access a victim's system.

An analysis of the above characteristics reveals some early indicators of supply chain attacks that can be detected using AI tools, including unusual network activity, unknown software, poor system performance, and unusual communication. These signs may not confirm an attack but together increase the likelihood of an ongoing attack.

Case study of SolarWinds as a supply chain attack: The SolarWinds attack in early 2021 demonstrated the sophistication of supply chain attacks. Hackers infiltrated SolarWinds' software development and planted malicious code into legitimate software updates, which were then sent to customers, including government agencies and Fortune 500. This attack remained undetected for months, enabling hackers to steal sensitive data, spy, and potentially threaten national security [77], [78]. The case study revealed that the SolarWinds attack exploited specific vulnerabilities, including weak user credentials and poor network monitoring, indicating a growing threat of complex network attacks.

F. FILELESS MALWARE ATTACKS

Recent studies have demonstrated a sharp increase in fileless malware attacks. Hence, the early detection of vulnerabilities and potential solutions is vital for minimizing their effects.

Key characteristics: Some indicators of fileless malware attacks that aid early detection are as follows.

- Fileless malware uses social engineering, email attachments, exploit kits, and advertisements to deceive users into clicking malicious links to download [10].
- It exploits legitimate tools such as PowerShell, Java script, and WMI to evade traditional security [35].
- Fileless malware attacks computer memory or registries, leaving no files and making detection difficult [11].
- These attacks use software or operating system flaws to inject malicious code into the memory.
- Fileless malware uses persistence to remain active after rebooting [35].

Therefore, unusual system calls or network traffic can reveal fileless malware attacks that reside in memory or registries. In addition, because fileless malware resides in memory or registries, analyzing memory dumps, registries, commands, security logs, processes, email attachments, and links in conjunction with advanced state-of-the-art machine-learning algorithms can effectively detect fileless malware.

Case study of ToddyCat attacks as fileless malware attacks: A recent example of fileless malware attacks is the ToddyCat attacks in Southeast Asia for data espionage in 2022 [102]. The attackers used social engineering tactics to entice users to open malicious URLs that installed backdoor malware into the computer' memory. This attack used advanced cyber-espionage tools, like Samurai Backdoor and Ninja Trojan, to infiltrate the targeted networks. Malware bypasses traditional security by exploiting innocent user behavior and deceptive emails and remains undetected [80]. ToddyCat attacks weaken societal trust in technology and cybersecurity and highlight improved security measures, advanced threat detection, and increased anti-phishing training.

G. ADVANCED PERSISTENT THREATS (APTs)

APTs have become a growing concern in recent malware trends, exhibiting steady increases in sophistication and persistence. These are long-term targeted attacks and combinations of different methods are used to achieve their goals. These threats are often associated with nation-state actors, who aim to steal sensitive information or disrupt critical infrastructure [13], [34], [103].

Key characteristics: Some primary characteristics of APT attacks are as follows.

- APT malware often runs processes to hide detection during an attack. Collecting this data is essential for detecting abnormal behaviors [104].
- APT malware camouflages during C&C server interactions. Behavioral analysis cannot detect APT at this stage. APT detection requires the analysis of initial Domain Name System (DNS) requests and host communications with remote C2 servers [103].
- This type of attack often exploits software vulnerabilities.
- APTs are multistage, low, and slow attacks throughout the attack lifecycle. During lateral movements, attackers search for vulnerable hosts, gain knowledge about targets, and escalate privileges. Exfiltration involves copying sensitive data to an external server. Hence, APT activities can be detected by tracking network communications for signs such as changes in the vertex degree (number of connections to the network). For example, APTs have a lower vertex degree during lateral movement but a higher vertex degree variation during exfiltration (more connections to external servers) [103].

To find solutions for timely remedies, AI tools can be trained to detect and classify APT activity based on different stages of attack characteristics, such as different processes (registry events, network events, etc.), initial DNS requests, number of connections with the network, and other parameters involved in communication between the host and remote C2 servers.

Case study of NotPetya as an APT attack: In 2017, NotPetya was responsible for one of the most destructive APT attacks in the world. Initially, NotPetya appeared to be ransomware, but it was a destructive APT attack that targeted Ukrainian organizations and quickly spread globally, affecting numerous multinational companies. The attack leveraged a compromised Ukrainian accounting software update to spread the malware. NotPetya caused billions of dollars in damage by disrupting shipping ports, banks, and government systems [105]. This case study indicates that attackers can exploit software flaws, emphasizing the importance of recognizing attack traits and vulnerabilities for prompt detection and response.

H. CLOUD-BASED ATTACKS

In 2022, cloud-based cyberattacks experienced a 48% surge, with Asia documenting the most significant increase, followed by Europe and North America. These increasing trends underscore the need for robust security measures at individual and organizational levels [16].

Key characteristics: Cloud-based attacks target cloud-based platforms such as computing, storage, or hosted applications. Such attacks can lead to data breaches, data loss, unauthorized access to sensitive data, and service disruptions.

The following are some common techniques used in cloud-based attacks [106].

- Attackers steal login credentials to access a user's cloud account.
- Attackers use DoS attacks to crash cloud services by flooding them with traffic.
- Cloud-based attacks often involve unusual network traffic, such as a sudden data transfer spike or communication with dubious IPs.
- Attackers may inject malicious code to gain control or exploit cloud app/infrastructure vulnerabilities.

Knowing these common characteristics can help organizations defend themselves against cloud-based attacks.

I. EXPLOITING A REMOTE WORKFORCE

Working from home has revealed various vulnerabilities in accessing corporate networks. By taking advantage of the pandemic, attackers have targeted a remote workforce. Reports show a surge in malware attacks exploiting remote-work vulnerabilities to infiltrate networks. For example, in March 2022, Alliance Virtual Offices reported a 238% increase in cyberattacks owing to remote working during the pandemic. These incidents highlight business risks in telecommuting environments [107]. Remote access trojans (RATs) also target remote workers; RATs are often disguised as legitimate software. Additionally, the use of the videoconferencing service Zoom skyrocketed in 2020, with people working from home and connecting with loved ones. In April, a cyberattack called zoombombing enabled hackers to join private meetings, access conversations, and share offensive content [108].

Key characteristics: Malware attacks that exploit a remote workforce exhibit certain traits, as outlined below.

- Cybercriminals use weak password security and VPN flaws to breach corporate networks and steal data [109].
- Attackers can exploit a Remote Desktop Protocol (RDP) to access the internal system of a network. Malware such as Ryuk, WannaCry, and NotPeya uses exploits to spread and infect systems through known vulnerabilities [110].
- The misuse of both work and personal devices leads to increased vulnerability when working remotely [107].

Organizations should protect against malware attacks on remote workers by using secure passwords, remote access tools, and phishing awareness training.

J. ATTACK TRENDS ON EDGE NETWORKS

Edge networks are computer networks that process data near their sources. Unlike traditional networks, which send data to a centralized location for processing, edge networks process data at the edge of the network, either on a device or in a nearby router or switch. This approach speeds up data processing and reduces latency, making it ideal for the IoT, self-driving cars, and smart cities [17], [111]. Like other computer networks, edge networks are susceptible to malware. Because edge networks are designed to process data quickly and at the edge of the network, they often rely on lightweight hardware and software that may not be as secure as the more robust traditional network architectures. This leaves them open to attacks that exploit vulnerabilities in networks, devices, or software. Attackers have recognized the growing importance of edge networks and have devised various strategies to exploit their vulnerabilities. Common attack trends in edge networks include Distributed Denial of Service (DDoS) attacks, data breaches, and man-in-the-middle attacks. These attacks aim to disrupt network operations, compromise sensitive data, or intercept communication between users and edge devices [17].

K. SUMMARY OF FINDINGS IN MODERN MALWARE ATTACK TRENDS

In the subsequent discussion, we have summarized and compared the leading attack trends in Table 3.

- The table shows that cryptojacking attacks can hijack devices and use them to mine cryptocurrencies that are unrecognized by the owner.
- Mobile malware is also increasing, exploiting system and app weaknesses to steal sensitive data using mainly SMS phishing and mobile botnet attack vectors, as shown in the 2019 Exodus spyware attack.
- Ransomware threats are escalating and usually target healthcare, financial, and governmental entities, leveraging phishing emails and brute-force attacks. RaaS and multiple extortion methods increase the threat complexity and adaptability, as highlighted by the Colonial Pipeline attack.
- The number of supply chain attacks, primarily for financial and espionage purposes, is rising. Attackers employ phishing and fake websites to exploit software developers and suppliers via software hijacking and counterfeit components. The 2020 SolarWinds attack has highlighted this trend.
- APTs and fileless malware attacks exemplify stealth and persistence. Both attacks target long-term data theft while hiding in the system. This represents a shift from direct attacks to covert operations, highlighting the growing importance of data. The 2017 NotPetya attack used innovative tactics, such as living-off-the-land and zero-day vulnerabilities, whereas scripting languages were used in the 2022 ToddyCat attack. Infrastructure, energy, and technology are common targets.

Our analysis of modern malware attack trends reveals several similarities and divergences. The landscape of malware threats is evolving, with each attack pattern presenting unique challenges. Understanding these trends, their effects and attackers' tactics is essential for creating successful defense strategies.

V. DEFENSE MECHANISMS

Based on a previous study on malware evolution and current attack trends, it is evident that malware is persistently advancing with novel threats and vulnerabilities, leading to

TABLE 3. Summary of the characteristics of modern malware attack trends.

Attack trend	Primary motive	Typical delivery technique	Exploited vulnerability	Potential target sectors	Innovative tactics	Increasing rates	Notable example/case study
Cryptojacking	Financial gain	Web-based and file-based cryptojacking	Unpatched software, insecure websites, cloud environment vulnerability	Targeting any systems with adequate resources for crypto mining	Advanced fileless techniques, social engineering, malicious mobile apps, etc.	Very high	AsyncRAT malware
Mobile malware attack	Financial gain by stealing credit card, banking, and personal data	Smishing, app impersonation, advertising, etc.	Operating system and app vulnerabilities	Industries with sensitive data and mobile tech	Code obfuscation, exploit kits, SMS phishing, mobile botnets	High	Exodus spyware (2019)
Internet of Things (IoT) Attacks	Financial gain, espionage, and disruption	Weak credentials, device misconfigurations, insecure network, etc.	Outdated firmware or software on IoT devices	Industries and sectors where IoT devices are used	Botnets and DDoS attack, Man-in-the-Middle attacks, device spoofing, etc.	High	Mirai botnet (2016)
Ransomware attack	Data encryption and extortion	Email phishing, brute-force attacks	Software vulnerabilities and OS design flaws	Healthcare, financial, and government organizations	RaaS, double extortion, triple extortion, rust language	Very high	Colonial Pipeline attack (2021)
Supply chain attacks	Financial gain, espionage	Phishing emails or creating fake websites, brute-force attacks	Software or hardware supply chain of an organization	Software developers and trusted suppliers	Software hijacking, fake components, and software vulnerabilities	High	SolarWinds attack (2020)
Fileless malware	Evasion of traditional security measures	Malicious emails, web exploits	Misuse of legitimate system tools	Financial, healthcare, etc.	Scripting languages	High	ToddyCat attack (2022)
APTs	Long-term data theft	Social engineering, spear-phishing	System and software vulnerabilities	Infrastructure, energy, and technology	Living-off-the-land tactics, zero-day flaws, etc.	Moderate	NotPetya (2017)
Cloud-based attack	Data breaches	Stealing login credentials	Computing and storage system vulnerability	Cloud services	Flooded cloud services with unusual traffic	High	-
Exploiting Remote Workforce	Financial gain and disrupt business operations	Social engineering, outdated VPNs, vulnerable networks, etc.	Exploiting vulnerabilities in third-party software	Remote workers	Phishing scams, brute-force attacks, webcam hacking, etc.	Moderate	Remote access trojans (RATs)

increased intelligence and a shift from single-phase defense to comprehensive, multilayered defense systems. We classified the defense mechanisms into two categories.

- Multilayered defense mechanisms.
- Other defense mechanisms.

A. MULTILAYERED DEFENSE MECHANISMS

We mainly focus on a multilayered defense strategy to protect against potential malware threats; this approach has gained significant attention in the recent cybersecurity literature. This approach ensures that, if an attacker breaches one layer of defense, the other layers remain opposed, making it challenging for attackers to evade detection. This method involves implementing multiple layers of protection: assessing, protecting, detecting, responding, and recovering [112], [113], which are interdependent and mutually supportive. Each area has distinct objectives that can be categorized further. The subsequent subsections provide detailed explanations for each category.

1) ASSESSING

The layered defense approach starts with a thorough assessment of an organization's security posture, including its resources and potential vulnerabilities, which guides future risk management practices and contributes to minimizing the threat exposure [113], [114].

2) PROTECTING

The protection layer plays a significant role by using multiple security checks at different levels and prevents modern malware attacks by controlling access, as illustrated in Table 4.

3) DETECTING

Several malware detection methods have been proposed in the literature. Figure 5 illustrates the various malware detection methods [20], [22], [120]. This section provides a concise overview of each technique and focuses on AI-based detection methods.

a: ARTIFICIAL INTELLIGENCE-BASED MALWARE DETECTION

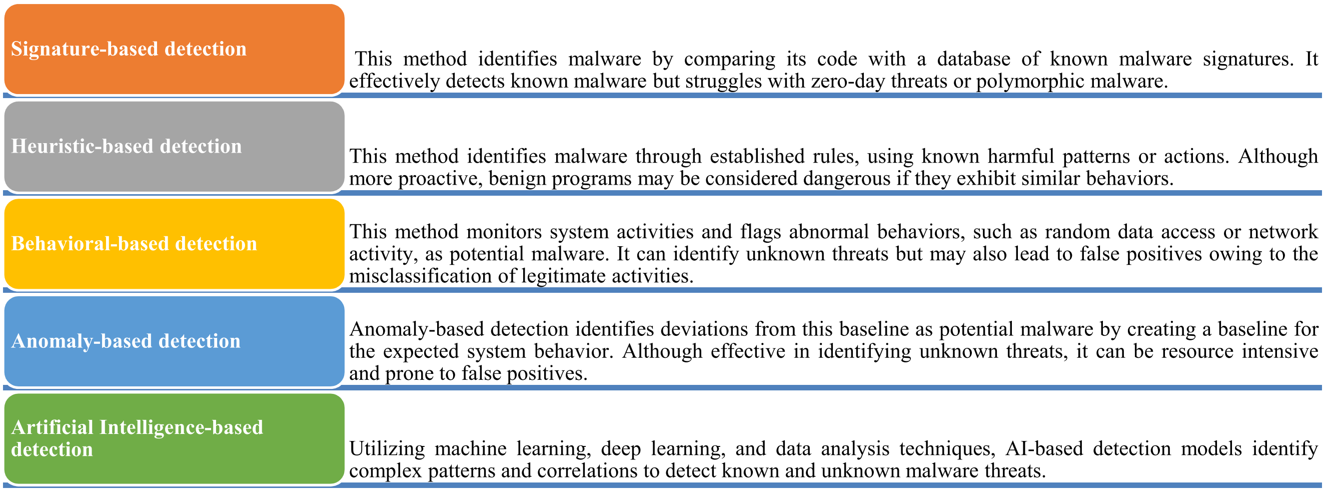
This section explores advanced AI techniques, such as machine learning and deep learning, for superior malware detection, owing to their adaptability, scalability, and real-time response. This method effectively manages obfuscated malware, reduces false positives, and outperforms traditional methods in addressing unknown threats. Table 5 summarizes the datasets that are widely used for training and evaluating deep learning and machine learning models for malware detection. This section reviews the most recent literature on detecting different malware attack trends, including ransomware, APT, fileless, Android, and IoT malware attacks, using different datasets and AI techniques.

b: RANSOMWARE DETECTION APPROACHES

This review examines recent studies employing different machine learning and deep learning techniques for ransomware detection, focusing on how these methods adapt to the evolution of ransomware. For example, [121] proposed a hierarchical neural network approach called SwiftR for cross-platform ransomware detection. The authors extracted features from process-trace files and employed deep learning techniques, such as file encryption and process injection, to identify ransomware behavior. Experiments demonstrate

TABLE 4. Various security points at the protection layer.

Security checks	Description
Physical security	Several studies have emphasized the significance of physical security in safeguarding hardware infrastructure from unauthorized intrusion and theft. This security is critical to an organization's defense, allowing only authorized personnel to access server rooms or data centers [115][116].
Endpoint security	This layer protects individual devices (e.g., desktop computers, laptops, and smartphones) connected to the network by implementing antivirus or anti-malware software, personal firewalls, regular patch management, and ensuring secure configurations for operating systems and applications [117].
Application and data security	This layer aims to protect software applications and sensitive data by implementing secure coding practices, encryption technologies, application firewalls, penetration testing, backup, and regular vulnerability assessments.
Network security	Network security, a vital part of a defense system, offers enhanced visibility of network activities in real-time. After reviewing the literature, we found that this phase employs various automated tools for security, such as firewalls, IDPSs, VPNs, EDRs, and SIEM systems [13][118][119], and aids in quick detection and response to potential breaches.
Data backup security	Regular data backup is a vital security measure that aids rapid recovery from significant attacks or data loss.
Security awareness training	Training staff on secure methods, such as password protection, multifactor authentication, and regular exercise, helps mitigate human errors, social engineering attacks, and insider threats [114].



Signature-based detection

This method identifies malware by comparing its code with a database of known malware signatures. It effectively detects known malware but struggles with zero-day threats or polymorphic malware.

Heuristic-based detection

This method identifies malware through established rules, using known harmful patterns or actions. Although more proactive, benign programs may be considered dangerous if they exhibit similar behaviors.

Behavioral-based detection

This method monitors system activities and flags abnormal behaviors, such as random data access or network activity, as potential malware. It can identify unknown threats but may also lead to false positives owing to the misclassification of legitimate activities.

Anomaly-based detection

Anomaly-based detection identifies deviations from this baseline as potential malware by creating a baseline for the expected system behavior. Although effective in identifying unknown threats, it can be resource intensive and prone to false positives.

Artificial Intelligence-based detection

Utilizing machine learning, deep learning, and data analysis techniques, AI-based detection models identify complex patterns and correlations to detect known and unknown malware threats.

FIGURE 5. Typical malware detection approaches.

that SwiftR (98%) accurately distinguishes legitimate processes from ransomware but cannot handle non-executed ransomware. Singh et al. [138] introduced a unique machine learning approach, SINN-RD, which uses spline interpolation and neural networks for efficient ransomware detection. This study demonstrates its superior performance over traditional detection methods, reinforcing its potential as a significant advancement in combating ransomware threats. Homayoun et al. [123] proposed a deep ransomware threat hunting and intelligence system for the fog layers. Fernando and Komninos [124] introduced a feature selection architecture for ransomware detection under concept drift. Davies et al. [138] utilized a differential area analysis for ransomware attack detection within mixed-file datasets. For early stage detection, Al-rimy et al. [139] presented a crypto-ransomware early detection model using advanced machine learning models, such as incremental bagging and enhanced semi-random subspace selection. Rhode et al. [140] explored early stage malware prediction using Recurrent Neural Networks (RNNs). Zhang et al. [109] employed patch-based Convolutional Neural Networks (CNN) and self-attention networks for ransomware classification by leveraging embedded n-grams of opcodes. Herrera-Silva and Hernández-Álvarez [141] developed a dynamic feature dataset for ransomware detection using ML algorithms, whereas Zhang et al. [142] adopted a similar approach but used n-grams of opcodes. In the context of encrypted traffic, Berrueta et al. [143] applied ML models to crypto-ransomware detection in file-sharing network scenarios. Abbasi et al. [144] developed behavior-based ransomware classification using a Particle Swarm Optimization (PSO) wrapper-based approach for feature selection. Almashhadani et al. [145] created a multifeatured metaclassifier-network-based system for ransomware detection. Hsu et al. [146] enhanced file entropy analysis to improve the machine learning detection rate of ransomware.

TABLE 5. Datasets for malware detection.

Reference	Dataset name	Brief description	Source and link	Performance of AI models on these dataset	Accuracy (%)
Datasets for detecting ransomware attack					
[121]	SwiftR dataset	This paper used multiple datasets for evaluation. The first evaluation scenario included 40.3 k samples and in the final evaluation scenario, the authors used a very large, challenging production dataset with 183 k samples.	https://dataset.karbab.net/swiftr.	Hierarchical Neural Network (HNN) LSTM	98
[122]	IEEE Dataport	This repository holds the results of testing over 70 ransomware samples from various families since 2015. It includes the malware's network traffic (DNS and TCP) and I/O operations while encrypting a shared network directory.	http://dx.doi.org/10.21227/qnyn-q136.	Artificial Neural Network (ANN)	99.83
[123]	DRTHIS dataset	This dataset includes 220 Cerber, 220 Locky, 220 TeslaCrypt ransomware samples, and 219 goodware samples obtained from the source link expanded by 99 CryptoWall, 28 TorrentLocker, and 77 Sage samples.	https://ieeexplore.ieee.org/document/8051108	Convolution Neural Network (CNN) and Long Short-Term Memory (LSTM)	99.6
[124]	Elderan dataset	The Elderan dataset contains a list of hashes for each ransomware sample used. These samples were collected from 2013 to 2015.	https://arxiv.org/pdf/1609.03020.pdf	Random Forest (RF)	96
[125]	Kaggle dataset	Kaggle supports various dataset formats, with CSV being the simplest and most popular for tabular data. This paper collected datasets from six Kaggle sources.	https://www.kaggle.com/docs/datasets#resources-for-starting-a-data-project	RF, GB, DT, AdaBoost, NN, Stochastic Gradient Descent (SGD), NB, ANN, and LSTM	99.8
Datasets used for detecting APT attack					
[126]	Malware Capture CTU-13 dataset	This dataset includes 29 network traffic and 6 APT attack malicious codes: Andromeda, Cobalt, Cridex, Dridex, Emotet, and Gh0stRAT.	https://www.stratosphereips.org/datasets-malware	Combined CNN-MLP and CNN-LSTM	99 for CNN-LSTM
[127]	Contagio malware database	Contagio is a comprehensive archive of historical malware samples, threats, observations, and analyses. This paper collected 107 types of traffic data from this public repository and one type of normal traffic data from Alexa top.	https://contagiodump.blogspot.com/	RESNET_LSTM and PARALLEL_LSTM	99.9
[104]	Interactive Malware analysis	This malware hunting repository offers live incident access, examining networks, files, modules, and registry activities directly via a web browser. This paper gathered APT malware data from this Online Sandbox Any Run and other resources, along with normal data.	Interactive Online Malware Sandbox. https://app.any.run/	RF, CNN, Multi-Layer Perceptron (MLP), and Long Short-Term Memory (LSTM)	93
Datasets used for detecting fileless malware attack					
[10]	Non-obfuscated malicious PowerShell commands dataset Obfuscated malicious PSCmds dataset	This dataset contains 3,057 non-obfuscated PSCmds with 23 behavioral labels and collected from various sources. The dataset was generated by applying 12 obfuscation methods to 3,057 non-obfuscated PSCmds and obtained 36,684 obfuscated samples. The dataset is used for obfuscation multi-label classification.	https://github.com/pan-unit42/iocs/tree/master/psencmds https://any.run/malware-reports/ https://www.filescan.io/reports/ https://virusshare.com/	Support Vector Machine (SVM), Random Forest (RF), Decision Tree (DT), KNN and Deep Neural Network (DNN)	99.82 with DNN
[11]	Fileless malware dataset (memory dump)	This dataset was mainly collected from TalTech Library, which was an unbalanced dataset. Hence this dataset was augmented by adding five new fileless malware from three other reputable repositories – VirusShare, PolySwarm and AnyRun.	https://digikogu.taltech.ee/en/Item/87cb2a3a-7ef5-43f0-89a5-ef4cb588b0d5 https://virusshare.com/ https://polyswarm.network/ https://app.any.run/	RF, DT, SVM, Logistic Regression (LR), KNN, XGB, and Gradient Boosting (GB)	Maximum 93.3 for RF
[128]	Dumpware10 dataset	The Dumpware10 dataset encompasses 4,294 executables (3,686 malicious, 608 benign) across 11 categories and is publicly accessible for non-commercial use.	https://web.cs.hacettepe.edu.tr/~selman/dumpware10/	RF, Extreme Gradient Boosting (XGBoost), Linear SVM, (SMO), and J48.	96.39 with SMO
Datasets used for detecting IoT malware					
[129]	R client VirusTotal dataset	R client for Virustotal Public API scans files and URLs for viruses, worms, trojans, etc. It also categorizes content hosted by a domain from multiple services.	https://github.com/soodoku/virustotal/	Federated learning (KNN, RF, DNN, MLP)	96
[95]	N-BaIoT dataset IoT network intrusion dataset	The N-BaIoT dataset contains 245 million traffic flows from IoT and IT devices, representing 50 malware families and 20 benign activities, as discussed in the paper. The IoT network dataset contains traffic from attack scenarios, including simulated Mirai traffic.	N-BaIoT https://ieeexplore.ieee.org/document/8490192 IEEE Dataport (2019) http://dx.doi.org/10.21227/q70p-q449	Federated learning (MLP and Autoencoder)	99.98
[130]	A normal dataset An attack dataset	Normal dataset, which includes traces of the normal behavior of the network devices. Attack dataset, which includes traces of normal and attacking behavior of the network devices during a specified time.	Both datasets are extracted from a testbed network consisting of 78 IoT/IIoT devices located in a city.	Autoencoder	99.9
[131]	The Microsoft Malware dataset (MMD) IoT Malware Dataset (IMD)	The MMD dataset has 43,572 files, including 10,868 labeled malware. This study uses only labeled datasets. IMD dataset comprises byte and assembly files (11,150) and obtained from reputable repositories such as VirusShare, VirusTotal, and MalwareBazaar.	Microsoft Malware classification challenge https://arxiv.org/abs/1802.10135 VirusShare https://virusshare.com/ MalwareBazaar https://bazaar.abuse.ch/	Convolution Neural Network (CNN) and bidirectional Long Short-Term Memory (LSTM)	99.91 and 99.83
[132]	MQTTset Dataset	This new dataset was created using IoT devices' MQTT communication and simulating a smart room scenario. The dataset contains 33 features to detect six attack types: legitimate, DoS, slowite, brute-force, malformed, and flood.	https://doi.org/10.3390/s20226578	KNN and Multi-Layer Perceptron Classifier (MLPC)	91 and 93

TABLE 5. ***(Continued.)*** **Datasets for malware detection.**

Datasets used for detecting Android malware					
[133]	Drebin dataset Android Malware Dataset (AMD) RmvDroid dataset	The Drebin dataset contains 5,560 maligned Android apps from 179 families, collected from August 2010 to October 2012, labeled by the Drebin authors. The dataset comprises 24,650 malware samples from 71 families, spanning 135 unique variants identified between 2010 and 2016. RmvDroid (2019) offers a dataset of 9,133 app samples from 56 malware families in the official Android market.	Drebin dataset https://www.sec.cs.tu-bs.de/~danarp/drebin/ AMD https://www.cs.bgsu.edu/sanroy/Files/papers/amd2017.pdf RmvDroid dataset https://dl.acm.org/doi/abs/10.1109/MSR.2019.00067	K-Nearest Neighbors (KNN), Decision Tree (DT), Support Vector Machines (SVM), and Random Forest (RF).	-
[134]	M0Droid dataset AMD dataset Kaggle benign and malicious dataset	It contains 200 benign and 200 malicious applications as well as 76 native permissions extracted as attributes. This dataset contains 1000 malicious and 1000 benign applications. Data was collected from verified benign and malicious URLs using a low interactive client honeypot to capture network traffic.	M0Droid https://doi.org/10.1080/15536548.2015.1073510 AMD http://amd.arguslab.org/ Kaggle https://www.kaggle.com/datasets/xwolf12/malicious-and-benign-websites	Decision Tree (DT), Support Vector Machines (SVM), Naive Bayes (NB) and K-Nearest Neighbors (KNN).	96.95 for AMD
[135]	VirusShare dataset Google Play App Store	20,000 malware samples from VirusShare were downloaded. 20,000 benign samples were obtained from the Google Play App Store.	VirusShare https://virusshare.com/ Google Play App Store https://play.google.com/store	SVM, RF and Multimodal Neural Network (MNN)	98
[136]	CCCS-CIC-AndMal-2020 dataset	This paper uses the 2020 CCCS-CIC-AndMal-2020 dataset, with 400K Android apps and 141 features. It has 53,439 samples of 14 malware types, split evenly between benign and malicious.	https://www.unb.ca/cic/datasets/index.html	Ensemble of RF, KNN, MLP, SVM and LR	95
[137]	Android apps image dataset	3000 malicious and 3000 benign apps were used to test the method.	Obtained from Drebin and Malgenome Android malware datasets	ANN, CNN, and VGG19-based autoencoder	98.56

Limitations: We found that most techniques proposed in the literature require large datasets, have the risk of producing false positives, and struggle to identify unfamiliar or novel ransomware.

c: ADVANCED PERSISTENT THREAT (APT) DETECTION APPROACHES

The landscape of machine learning and deep learning applications for advanced persistent threat (APT) detection spans various techniques and features. For example, Ghafir et al. used machine-learning correlation analysis [147] and Hidden Markov Models [148] for APT detection using multiple features. The first utilized features include network and system events, process execution patterns, and log data. The second approach provides time- and frequency-based attributes focusing on network measures. Do Xuan et al. proposed a deep learning-based Flow Network Analysis [149] and a combined deep learning model [126]. The authors used network flow data and graph-based features to train the detection model. Niu et al. [127] proposed a method that combines deep learning, time-sequence analysis, and association analysis to detect APT malware traffic. They used features such as network flow, traffic statistics, and temporal patterns. Other methods include semi-supervised learning with complex network characteristics [103], real-time provenance tracking [32], real-time APT detection using an ensemble learning approach [150], decepticon techniques [151], and deep graph networks [104] to detect APTs by leveraging packet- and network-level attributes, network flow data, traffic analyses, and graph-based features. Yang et al. [33] developed a data backup and recovery strategy for the APTs. Several studies have focused on improving the defensive capabilities of a game theory approach against APTs [152], [153], [154]. Whereas Moothedath et al. [152] employed dynamic information flow tracking to detect multistage APTs, Yang et al. [153] proposed an effective repair strategy using a differential-game approach. Rass et al. [154] primarily focused on defense strategies using game theory. Notably, these studies largely underscore the efficacy of game theory in APT defense; however, they also share some common limitations. For example, it is a complex task that requires deep knowledge of both game theory and APTs, which mainly targets APT detection and prevention but can also consider aspects such as vulnerability, risks, awareness, and preventive actions.

Limitations: Many of these studies face challenges such as the need for real-world data for validation [32], [104], [127], [147], [148], [151], computational complexity [104], [126], scalability [149], [150], false positives [32], [127], [149], [151], and feature selection issues [104], [126].

d: FILELESS MALWARE ATTACK DETECTION APPROACHES

Several studies have provided valuable insights into fileless malware detection using machine learning and deep learning methods. Sanjay et al. [155] proposed a technique that uses memory forensics-based analysis to detect fileless malware based on opcode sequences, whereas Tsai et al. [10] utilized multi-label classifiers for de-obfuscating and profiling malicious PowerShell commands. Khalid et al. [11] presented an overview of ML techniques for fileless malware detection, suggesting that combining deep-learning methods with large datasets can provide an effective solution. Borana et al. [156]

proposed an assistive tool for detecting fileless malware, whereas Bozkir et al. [128] combined memory forensics, manifold learning, and computer vision to detect malware.

Limitations: Detecting fileless malware presents issues, including ineffective signature-based detection, challenges in securing samples from inactive controls and common servers, and their ability to resist virtual environment analysis.

e: MALWARE DETECTION APPROACHES IN IoT DEVICES

The literature presents various ML and DL techniques for IoT malware detection. Several studies have focused on the use of federated learning [95], [129], [130] to ensure privacy and lower communication costs despite potential data bias and resource challenges. For example, Shukla et al. [129] proposed a federated learning approach that uses heterogeneous models for on-device malware detection in IoT networks. It outperformed traditional federated learning in terms of accuracy by 13% and reduced the number of false positives by 63.99%. However, this requires homogeneous on-device models, which may be difficult to implement in networked IoT systems. Other studies have explored the use of deep-learning models for malware detection in IoT devices [132], [157], [158], [159]. For instance, Chaganti et al. [157] used deep-learning models to achieve high accuracy but only for certain types of malware. Abdullah et al. [158] and Khan and Ullah [159] employed hybrid learning models with a high detection rate but with complexity and limited training datasets. Smmarwar et al. [160] developed AI for detecting malware in industrial IoT, emphasizing dynamic feature selection and continuous model updates. Ali et al. [161] proposed a flexible multitask deep-learning method that addresses the issue of imbalanced datasets. Golmaryami et al. [162] demonstrated high detection rates using self-supervised adversarial machine-learning models.

Limitations: Overall, deep-learning-based methods, such as CNNs and LSTM networks, are promising for IoT malware detection. However, challenges such as heterogeneous models, scalability, diverse datasets, and computational demands remain.

f: MALWARE DETECTION APPROACHES IN ANDROID

Several studies have explored various machine learning (ML) methods for detecting Android malware. Zhao et al. [133] discussed the effect of sample duplication on machine learning but did not examine different types of repetitions. Sahin et al. [134] presented LinRegDroid, a detection system that uses multiple linear regression models. However, their effectiveness against complex malware remains unclear. Kim et al. [135] explored a multimodal deep-learning approach using various features and achieved notable results, whereas Tang et al. [163] proposed an obfuscation variant detection method using multi-granularity opcode features. Zhu et al. [164] proposed an end-to-end detection system; however, its real-time efficiency was unclear. Bakır and Bakır [137] developed an autoencoder-based malware detector, but its resistance to advanced evasion remains unknown. Islam et al. [136] optimized the feature selection and ensemble machine learning to classify malware. Finally, Bhat et al. [165] focused on system-call-based detection by leveraging homogeneous and heterogeneous machine-learning ensembles.

Limitations: Although these studies point to an ongoing trend in ML and ensemble methods for malware detection, gaps are apparent in terms of addressing complex, obfuscated, or zero-day malware.

g: STATE-OF-THE-ART TOOLS AND TECHNIQUES FOR TACKLING MODERN MALWARE

In this section, we describe AI-powered anti-malware tools designed to detect modern malware attacks and enhance scanning engines. We divided AI-enabled modern malware detection tools and techniques into two categories: traditional machine-learning techniques and deep-learning techniques to detect, analyze, and prevent various types of malware threats. Security analysts may use traditional machine learning tools and techniques to automate different types of malware analysis, such as behavior or dynamic analysis, network traffic analysis, memory forensic analysis, system log and event analysis, and static analysis. These approaches use manual features based on domain expertise. Deep learning solutions have replaced feature engineering in the traditional ML workflow with a trainable system that can automatically extract features from the raw input to the final output. These sophisticated tools respond much faster and are more accurate than traditional systems. Table 6 summarizes the best AI-powered tools and techniques to combat today's sophisticated and intelligent malware.

4) RESPONDING AND RECOVERING

The response layer focuses on rapidly mitigating the detected threats and protecting the organization from further damage. Incident response teams can achieve this goal by following a pre-set plan. Subsequently, in the recovery layer, measures are executed to recover system functionality following an attack. Combining these security controls across disciplines provides a robust defense against modern malware.

Numerous methods have been identified for recovering data compromised by malware attacks, including key recovery [166], hardware-based recovery, cloud backups [167] [168], and the use of 'out-of-place update' features of SSD [169], although their effectiveness varies. Recently, a deep-learning-powered framework called PowerDP [10] was developed, which offers innovative recovery approaches by de-obfuscating PowerShell scripts and identifying behavior patterns to help recover from malware attacks.

A review of cybersecurity recovery strategies revealed gaps and potential areas for future research.

B. OTHER DEFENSE MECHANISMS

Various other defense strategies, including moving-target techniques, access control mechanisms, and holistic defense

TABLE 6. Summary of state-of-the-art tools and techniques for combating modern malware.

Tool: In the context of malware detection, tools are software programs or hardware devices that help detect, analyze, eliminate, or prevent malware threats. They help to implement the techniques.
Technique: In the context of malware detection, techniques are the approaches used to identify, classify, and eliminate malware threats.

Tool/Technique	Description	Source link	Reference
Traditional machine learning based tools/techniques			
Dynamic or behavior analysis tools (Cuckoo Sandbox, VMWare, VirusTotal and ANY.run)	These tools execute suspicious files in a separate virtual or controlled environment to monitor for malware activity and effects.	https://cuckoosandbox.org/ https://www.vmware.com/au.html https://app.any.run/	[170]
Network security tools (IDS/IPS, firewalls, WAFs)	These network traffic analysis tools are used to monitor network traffic and detect and prevent malware attacks at the gateway level.	https://geekflare.com/best-ids-and-ips-tools/ https://www.cisco.com/c/en/us/products/security/firewalls/what-is-a-firewall.html	[171]
CICFlowMeter	It captures packet data in real-time and uses statistical algorithms to extract features for network traffic classification.	https://www.internetworldstats.com/emarketing.htm	[126]
Memory forensics tool (Volatility Framework)	A popular open-source tool that analyzes memory dumps to extract information on running processes, network connections, and system activity.	https://github.com/volatilityfoundation/volatility	[11]
System monitoring tool (Sysmon, ProcMon)	Sysmon is developed by Microsoft and collects and analyzes malicious processes or event IDs from the Windows operating system kernel. ProcMon is designed to continuously monitor changes in the registry, file system, network, and process activities, and to log them.	https://learn.microsoft.com/en-us/sysinternals/downloads/sysmon https://learn.microsoft.com/en-us/sysinternals/downloads/procmon	[104] [22]
Static analysis tool (Yara IDA Pro, PeView, etc.)	YARA is a pattern matching tool that is specifically designed for identifying and classifying malware based on textual or binary patterns. IDA Pro disassembles code and provides a detailed review of its structure and function to identify elements of malware. PeView provides header information for PE files.	https://virustotal.github.io/yara/ https://www.linkedin.com/advice/3/how-do-you-use-ida-pro-analyze-malware-samples https://eyehatemalwares.com/malware-analysis/static-analysis/ma-peview/	[87]
Deep learning and artificial intelligences-based tools/techniques			
Cylance Protect	Cylance utilizes AI to predict, identify, and block threats like malware and ransomware before they can affect the system, offering a proactive approach to threat management.	https://docs.blackberry.com/en/unified-endpoint-security/blackberry-ues/overview/What-is-BlackBerry-Protect-Desktop/Architecture-BlackBerry-Protect-Desktop	[172]
DarkTrace	An AI-powered autonomous response solution that detects cyber threats and responds accordingly to neutralize attacks in progress.	https://darktrace.com/	[173]
CrowdStrike Falcon	This cloud-based, AI-infused tool provides next-generation antivirus protection. It incorporates machine learning algorithms to detect new threats and take remedial action in real-time.	https://www.crowdstrike.com/falcon-platform/	[174]
DeepArmor	DeepArmor uses machine learning and natural language processing to detect and block malware, viruses, worms, trojans, and ransomware.	https://www.getapp.com/security-software/a/deeparmor/	[172]
Deep Instinct	Deep Instinct's software uses artificial neural networks to protect against ransomware and other malware attacks in real-time.	https://www.deepinstinct.com/	[172]
Deep Feature Extractor (DFE)	This is an AI-powered tool which uses deep learning-based malware detection that leverages Convolutional Neural Networks (CNNs) and Recurrent Neural Networks (RNNs) to extract features from malicious files.	https://elib.dlr.de/106352/2/CNN.pdf	[123]
SentinelOne	An AI-powered endpoint security solution, SentinelOne offers prevention, detection, and response capabilities against various types of threats, including malware.	https://www.sentinelone.com/	[174]
Symantec Enterprise Cloud	Symantec Enterprise Cloud provides hybrid security for large, complex organizations on devices, in data centers, and the cloud.	https://www.symantec.com/	[174]
Sophos Intercept X	Sophos Intercept X utilizes machine learning models to detect and respond to malware for end-point security.	https://www.sophos.com/en-us/products/endpoint-antivirus	[174]

systems, have been studied to combat specific threats. Lee et al. [175] devised a strategy that randomly alters the file extensions for ransomware protection by introducing an element of unpredictability. On a broad scale, Keong et al.'s VoterChoice [176] and Shaukat et al.'s honey file-based systems [177] utilize intrusion detection and ML-based layers, respectively. In addition, Chowdhary et al.'s [178] SDN-based system for cloud network systems demonstrated advanced measures against sophisticated threats. Moreover, Krishnan, Duttagupta, and Achuthan [179] proposed a SDNFV-based security framework for edge-computing infrastructure, emphasizing threat monitoring. Similarly, Myneni et al. [180] introduced Smart-Defense, a distributed, deep-learning-aided solution for combating DDoS attacks within edge-computing realms. Both studies underline the relevance of cutting-edge technologies in enhancing edge network security. Hence, to improve the security of edge networks, organizations should implement customized defense plans, including implementing network segmentation to minimize exposure to threats, deploying intrusion detection and prevention systems (IDPS), leveraging behavioral analytics and machine learning for anomaly detection, and maintaining up-to-date firmware and patch management practices to address vulnerabilities and ensure the integrity of edge devices.

Despite these various approaches, they highlight the necessity of multifaceted and evolving defense against complex malware threats.

1) SUMMARY OF THE FINDINGS ON DEFENSE MECHANISMS

This section presents a comparative analysis of multilayered defensive methods and other systems, highlighting the core function of each layer against modern malware and their relative effectiveness. For instance,

- The assessment part identifies and studies risks, helping obtain a system that is ready for possible attacks. It differs from the protecting domain, which keeps things safe by using special tools. Instead of using direct safety measures, an assessment area reacts to potential threats.
- A protection mechanism can protect against specific types of attack. However, its effectiveness is compromised if an attacker can circumvent this safeguard and remain undetected. Moreover, the organization's risks remain high even if potential dangers are detected early without appropriate response and recovery tactics. Therefore, it is imperative to implement robust prevention measures coupled with practical strategies for incident management to match emerging threats within an organizational context.
- The protection and detection domains are then combined. The protection layer attempts to maintain the safety of the system while detecting security problems. Both are important but offer different benefits. The protection phase stops many attacks but may not work on new threats. The detection stage identifies issues that may result from past protection efforts, mainly unknown or advanced threats.
- Recent studies have shown a trend of using AI, specifically DL and ML, to detect malware such as ransomware, APTs, fileless, mobile, and IoT malware using various techniques. One notable trend is the integration of deep learning networks, such as CNNs and RNNs, for ransomware and other complex attack detection. These networks are good at processing large and complex data, such as opcode sequences and file entropy, to enhance detection accuracy. Memory forensics and metaclassifiers are recent approaches to detecting fileless malware, which is typically difficult because of the lack of disk footprints. Autoencoders, which can learn patterns from limited data, are also gaining popularity because of their self-learning capabilities. Moreover, recent studies on IoT malware detection have highlighted the use of federated learning owing to its ability to reduce communication costs and ensure privacy. Genetic algorithms and transfer learning have also attracted attention for the detection of the latest malware attack trends.
- Table 5 summarizes the datasets available for malware detection. For each dataset, we provide a brief description of its characteristics, such as the number of samples, types of malware, and features provided. We also provide the sources and links of these datasets, which is an essential aspect of research. In addition, we evaluated the performance of several deep learning and machine learning architectures on these datasets. New researchers can save time by using existing datasets instead of spending time and resources to create their dataset from scratch. These datasets are useful for creating and testing malware detection methods and assessing malware detection tools.
- Table 6 summarizes the state-of-the-art tools and techniques for modern malware analysis, helping new researchers become familiar with them. These tools and techniques can be effective in hunting modern malware based on specific needs, capabilities, and budgets.
- Finally, the response and recovery layers help fix problems after detecting a computer attack. They are essential because they allow things to return to normal and work well when earlier steps do their job correctly.
- By contrast, other defense strategies may rely on a more singular focus, such as signature-based detection, behavior analysis, or isolated security controls. Although these methods can prevent specific types of malware, their overall efficacy is limited by the increasingly sophisticated threats that exploit new vulnerabilities. The narrow scope of such strategies may result in potential security gaps and weaker defense mechanisms. Simultaneously, multilayered defenses holistically combat malware threats through several layers of security, with unique roles. Their combined efforts have yielded adaptable and robust defenses against the continuously evolving malware landscapes.

In summary, although a multilayered defense strategy offers a more comprehensive and resilient approach to modern malware threats, it also presents challenges, including its complexity, cost, and potential for defensive gaps, necessitating careful planning and continuous evaluation to ensure optimal protection in an organization's cybersecurity landscape.

VI. CHALLENGES, LIMITATIONS AND FUTURE RESEARCH DIRECTIONS

Studies on existing malware detection methods indicate that researchers in this field are exploring multiple ways to address security vulnerabilities across different platforms. However, several challenges and limitations remain in the realm of malware detection techniques that should be considered when devising new approaches in the future, as follows.

Evasion techniques: Attackers use complex obfuscation, code morphing, and encryption methods to bypass detection and require constant model updates to remain relevant.

Dynamic and evolving threats: The dynamic nature of malware is another challenge as malware authors constantly adapt their strategies and develop new techniques. Hence, timely updates in defense strategies are required to identify malicious activities accurately.

Scalability of detection methods: With the increasing volume and complexity of modern malware, traditional detection methods face scalability and real-time response challenges.

Lack of signatures: An increase in fileless malware that does not leave detectable traces on a disk renders signature-based detection methods ineffective.

In addition to these open issues, the current literature lacks comprehensive defense solutions, accurate model validation, diverse and large datasets, cross-platform detection methods, and computational complexity.

A. THE CRITICAL RESEARCH GAPS IN THE LITERATURE ARE AS FOLLOWS

1) DEVELOPMENT OF MULTILAYERED DEFENSE MECHANISMS

This study discusses the limitations of single-layer defense mechanisms and the need for more comprehensive approaches. Future research could explore multilayered defense mechanisms by including more security layers to protect against different phases, such as analyzing network traffic, monitoring system activities, and integrating contextual information (e.g., user behavior) for accurate multistage attack detection and false positive reduction. In addition, this review reveals some potential areas for the future exploration of multilayered defense mechanisms, such as their inherent complexity, resource allocation, and associated costs.

2) DEVELOPMENT OF A CROSS-DEVICE CRYPTOJACKING DETECTION AND PROTECTION MECHANISM

Most existing studies focus on a particular type of architecture that does not address group device security. As cryptojacking attacks can affect a wide range of devices, including desktops, mobile phones, and IoT devices, it could be useful to develop a solution that can comprehensively detect and prevent these attacks. This solution could involve machine-learning algorithms and deep neural networks that can detect patterns and anomalies in device behavior without needing specific signatures. Potential suspicious activities to be flagged include high CPU usage, increased power consumption, suspicious network activities, and other system activity logs. For example, a potential solution may include browser extensions to detect and block cryptojacking scripts, standardized testbeds to evaluate anti-cryptojacking tools, and containerization to isolate sensitive resources from malicious processes.

3) NOVEL ADAPTIVE RANSOMWARE DEFENSE FRAMEWORK

The existing literature still needs to focus on the practicality, robustness, and constantly evolving nature of ransomware threats. This study highlights the challenges posed by the dynamic nature of modern ransomware attacks that can bypass traditional antivirus and firewall systems. Future researchers could focus on developing an adaptive model that uses machine learning and adaptive learning techniques, such as transfer learning, reinforcement learning, and incremental learning, to respond to these new and evolving threats. Using these advanced techniques, an anti-ransomware system can identify patterns of behavior associated with previous ransomware attacks, learn from them, and adapt its defense measures accordingly.

4) CREATING MORE COMPREHENSIVE DATASETS AND OPTIMIZING THE DETECTION MODEL EFFICIENCY

Although the proposed adaptive ransomware defense framework is promising for addressing ransomware threats, the effectiveness of machine learning and adaptive learning techniques requires further research. Additional evaluations are required to assess the scalability, reliability, and efficiency of these techniques to mitigate and prevent ransomware attacks effectively. A major limitation of the literature is the scope of the dataset used for training and testing the adaptive model. Although the dataset covers a broad range of ransomware behaviors, it may not capture all possible ransomware strains or attack scenarios. Additionally, the dataset may be limited by sample size, which could affect the accuracy and generalizability of the adaptive model. Another limitation is the computational complexity of implementing the adaptive models. The use of machine learning and adaptive learning techniques such as transfer learning, reinforcement learning, and incremental learning requires significant computational resources, which may not be feasible for all organizations or systems. In addition, the complexity of the model may hinder its ability to respond quickly to new and evolving ransomware threats. To address these limitations, future researchers could focus on developing more comprehensive and diverse datasets for training and testing adaptive ransomware defense frameworks. Moreover, new research can explore techniques for optimizing the computational efficiency of machine learning and adaptive learning models for real-time ransomware detection and defense.

5) ADAPTIVE DEFENSE STRATEGY AGAINST APTS THROUGH GAME THEORY–MACHINE LEARNING HYBRID APPROACH

Detecting advanced persistent threats (APTs) is challenging because of their complex and targeted nature. Although game-theoretic approaches have shown promising results, they have limitations, and there is room for continued research to further enhance their detection efficiency, scalability, and applicability. They may need to be combined with other approaches to fit into a security strategy. For instance, adaptive defense strategies incorporating game theory and machine learning could be an innovative research gap. This would explore how deep reinforcement learning models can learn from dynamic APTs using neural networks, and game theory would be used to identify the optimal defense against an attack at any stage. This solution allocates resources for detecting and preventing APTs.

6) REAL-TIME DETECTION AND MITIGATION OF IOT MALWARE ATTACKS THROUGH EDGE COMPUTING

Edge computing can be combined with AI-based techniques to detect and mitigate IoT malware attacks in real-time, while reducing the overhead of centralized cloud-based analysis. This method can provide faster response times and prevent the propagation of malware. A well-known example of real-time detection and mitigation through edge computing includes fog computing, which uses a lower-layer edge device and fog layer to enable real-time data analysis and decision-making [181]. Hence, implementing AI-based techniques such as deep learning and machine learning to enhance IoT malware detection and mitigation, combined with novel architectural solutions, such as edge-computing-based systems to counter potential threats, represents an exciting research direction with significant potential for further exploration.

7) APPLICATION OF TRANSFER LEARNING TO IMPROVE DETECTION ACCURACY

The combination of transfer learning and machine learning, as evidenced by successful applications in the literature [182], [183], [184], [185], appears to be a promising technique for defending devices against tricky and sophisticated malware and leveraging pre-trained models to improve accuracy and reduce reliance on heavily labeled data. However, additional research is necessary to fully understand their role in combating modern malware threats, including zero days, and to deliver robust adaptive models.

VII. CONCLUSION

This study explores how malware threats have become more complicated and why we need a more robust defense against them. Based on the analysis in this review, this study highlights the developing nature of malware, explores prevalent attack patterns, and emphasizes the need for a more comprehensive approach to defense solutions rather than a narrow focus on detection strategies. Maintaining pace through continuous innovation and knowledge enhancement is paramount as the malware landscape evolves. We studied various defense systems and highlighted a layered security system that maintains resilience even when a single layer fails, thereby forming an effective counter to diverse malware threats. This study also identifies gaps in current research, particularly the lack of comprehensive studies that cover the complete picture of malware evolution, contemporary attack trends, and their defense solutions. The practical implications of multilayered defense systems include their enhanced resilience against modern complex malware threats. Ultimately, an improved security stance for an organization is achieved through a multilayered defense system, adding complexity to the compromise of the attacker's system. This review suggests that further research is required to improve the efficiency of multilayered defense systems, which are currently challenged by their complexity, cost, and potential security gaps. In addition, we aim to address the issues outlined in Section VI, and develop a comprehensive and generalized model for malware detection. This study concludes with a call for an ongoing emphasis on research and innovation in cybersecurity to match the pace of fast-changing malware threats, thus ensuring a secure digital space.

REFERENCES

[1] B. Jovanovic. *A Not-So-Common Cold: Malware Statistics in 2023*. DataPort. Accessed: May 17, 2023. [Online]. Available: https://dataprot.net/statistics/malware-statistics/

[2] PURPLESEC. *Cyber Security Statistics The Ultimate List Of Stats Data, & Trends for 2023*. Accessed: May 17, 2023. [Online]. Available: https://purplesec.us/resources/cyber-security-statistics/

[3] K. Kizzee. *Cyber Attack Statistics to Know in 2023*. Parachute. Accessed: Apr. 18, 2023. [Online]. Available: https://parachute.cloud/cyber-attack-statistics-data-and-trends/

[4] C. Threat, "Sonicwall cyber threat report," SonicWall, USA, Tech. Rep., 2023.

[5] B. Guembe, A. Azeta, S. Misra, V. C. Osamor, L. Fernandez-Sanz, and V. Pospelova, *The Emerging Threat of AI-Driven Cyber Attacks: A Review*, vol. 36, no. 1. New York, NY, USA: Taylor & Francis, 2022.

[6] Z. Mumtaz, M. Afzal, W. Iqbal, W. Aman, and N. Iltaf, "Enhanced metamorphic techniques—A case study against havex malware," *IEEE Access*, vol. 9, pp. 112069–112080, 2021, doi: 10.1109/ACCESS.2021.3102073.

[7] EUROPOL. (2021). *World's Most Dangerous Malware EMOTET Disrupted Through Global Action*. Accessed: May 18, 2023. [Online]. Available: https://www.europol.europa.eu/media-press/newsroom/news/world's-most-dangerous-malware-emotet-disrupted-through-global-action

[8] A. Gezer, G. Warner, C. Wilson, and P. Shrestha, "A flow-based approach for trickbot banking trojan detection," *Comput. Secur.*, vol. 84, pp. 179–192, Jul. 2019, doi: 10.1016/j.cose.2019.03.013.

[9] PSecurity. *73 Ransomware Statistics Vital for Security in 2023*. Accessed: Jul. 15, 2023. [Online]. Available: https://www.pandasecurity.com/en/mediacenter/security/ransomware-statistics/

[10] M.-H. Tsai, C.-C. Lin, Z.-G. He, W.-C. Yang, and C.-L. Lei, "PowerDP: De-obfuscating and profiling malicious PowerShell commands with multi-label classifiers," *IEEE Access*, vol. 11, pp. 256–270, 2023, doi: 10.1109/ACCESS.2022.3232505.

[11] O. Khalid, "An insight into the machine-learning-based fileless malware detection," *Sensors*, vol. 23, no. 2, pp. 1–20, 2023, doi: 10.3390/s23020612.

[12] A. Afianian, S. Niksefat, B. Sadeghiyan, and D. Baptiste, ''Malware dynamic analysis evasion techniques: A survey,'' *ACM Comput. Surveys*, vol. 52, no. 6, pp. 1–28, Nov. 2020, doi: 10.1145/3365001.

[13] A. Alshamrani, S. Myneni, A. Chowdhary, and D. Huang, ''A survey on advanced persistent threats: Techniques, solutions, challenges, and research opportunities,'' *IEEE Commun. Surveys Tuts.*, vol. 21, no. 2, pp. 1851–1877, 2nd Quart., 2019, doi: 10.1109/COMST.2019.2891891.

[14] S. S. Chakkaravarthy, D. Sangeetha, and V. Vaidehi, ''A survey on malware analysis and mitigation techniques,'' *Comput. Sci. Rev.*, vol. 32, pp. 1–23, May 2019, doi: 10.1016/j.cosrev.2019.01.002.

[15] D. Palmer. (2022). *Smartphone Malware is on the Rise, Here'S What to Watch Out for*. ZDNET. Accessed: Jun. 17, 2023. [Online]. Available: https://www.zdnet.com/article/smartphone-malware-is-on-the-rise-heres-what-to-watch-out-for

[16] G. Turner. *Cloud-Based Cyber-Attacks Increased by 48% in 2022*. Accessed: Jun. 25, 2023. [Online]. Available: https://www.digit.fyi/cloud-based-cyber-attacks-increased-by-48-in-2022/

[17] I. Gulatas, H. H. Kilinc, A. H. Zaim, and M. A. Aydin, ''Malware threat on edge/fog computing environments from Internet of Things devices perspective,'' *IEEE Access*, vol. 11, pp. 33584–33606, 2023, doi: 10.1109/ACCESS.2023.3262614.

[18] D. Gibert, C. Mateu, and J. Planes, ''The rise of machine learning for detection and classification of malware: Research developments, trends and challenges,'' *J. Netw. Comput. Appl.*, vol. 153, Mar. 2020, Art. no. 102526, doi: 10.1016/j.jnca.2019.102526.

[19] U.-E.-H. Tayyab, F. B. Khan, M. H. Durad, A. Khan, and Y. S. Lee, ''A survey of the recent trends in deep learning based malware detection,'' *J. Cybersecurity Privacy*, vol. 2, no. 4, pp. 800–829, Sep. 2022, doi: 10.3390/jcp2040041.

[20] G. M. and S. C. Sethuraman, ''A comprehensive survey on deep learning based malware detection techniques,'' *Comput. Sci. Rev.*, vol. 47, Feb. 2023, Art. no. 100529, doi: 10.1016/j.cosrev.2022.100529.

[21] Ö. A. Aslan and R. Samet, ''A comprehensive review on malware detection approaches,'' *IEEE Access*, vol. 8, pp. 6249–6271, 2020, doi: 10.1109/ACCESS.2019.2963724.

[22] S. A. Roseline and S. Geetha, ''A comprehensive survey of tools and techniques mitigating computer and mobile malware attacks,'' *Comput. Electr. Eng.*, vol. 92, Jun. 2021, Art. no. 107143, doi: 10.1016/j.compeleceng.2021.107143.

[23] Y. Huang, U. Verma, C. Fralick, G. Infantec-Lopez, B. Kumar, and C. Woodward, ''Malware evasion attack and defense,'' in *Proc. 49th Annu. IEEE/IFIP Int. Conf. Dependable Syst. Netw. Workshops (DSN-W)*, Jun. 2019, pp. 34–38, doi: 10.1109/DSN-W.2019.00014.

[24] S. Zhang, C. Hu, L. Wang, M. J. Mihaljevic, S. Xu, and T. Lan, ''A malware detection approach based on deep learning and memory forensics,'' *Symmetry*, vol. 15, p. 758, Dec. 2023. [Online]. Available: https://www.mdpi.com/2073-8994/15/3/758?utm_source=researcher_app&utm_medium=referral&utm_campaign=RESR_MRKT_Researcher_inbound

[25] K. Shaukat, S. Luo, and V. Varadharajan, ''A novel deep learning-based approach for malware detection,'' *Eng. Appl. Artif. Intell.*, vol. 122, Jun. 2023, Art. no. 106030, doi: 10.1016/j.engappai.2023.106030.

[26] H. Oz, A. Aris, A. Levi, and A. S. Uluagac, ''A survey on ransomware: Evolution, taxonomy, and defense solutions,'' *ACM Comput. Surveys*, vol. 54, no. 11s, pp. 1–37, Jan. 2022, doi: 10.1145/3514229.

[27] R. Moussaileb, N. Cuppens, J. L. Lanet, and H. Le Bouder, ''A survey on windows-based ransomware taxonomy and detection mechanisms: Case closed?'' *ACM Comput. Surv.*, vol. 54, no. 6, pp. 1–36, Jul. 2021, doi: 10.1145/3453153.

[28] T. McIntosh, A. S. M. Kayes, Y.-P.-P. Chen, A. Ng, and P. Watters, ''Ransomware mitigation in the modern era: A comprehensive review, research challenges, and future directions,'' *ACM Comput. Surveys*, vol. 54, no. 9, pp. 1–36, Dec. 2022, doi: 10.1145/3479393.

[29] F. Aldauiji, O. Batarfi, and M. Bayousef, ''Utilizing cyber threat hunting techniques to find ransomware attacks: A survey of the state of the art,'' *IEEE Access*, vol. 10, pp. 61695–61706, 2022, doi: 10.1109/ACCESS.2022.3181278.

[30] I. Kara and M. Aydos, ''The rise of ransomware: Forensic analysis for windows based ransomware attacks,'' *Exp. Syst. Appl.*, vol. 190, Mar. 2022, Art. no. 116198, doi: 10.1016/J.ESWA.2021.116198.

[31] S. Razaulla, C. Fachkha, C. Markarian, A. Gawanmeh, W. Mansoor, B. C. M. Fung, and C. Assi, ''The age of ransomware: A survey on the evolution, taxonomy, and research directions,'' *IEEE Access*, vol. 11, pp. 40698–40723, 2023, doi: 10.1109/ACCESS.2023.3268535.

[32] H. Irshad, G. Ciocarlie, A. Gehani, V. Yegneswaran, K. H. Lee, J. Patel, S. Jha, Y. Kwon, D. Xu, and X. Zhang, ''TRACE: Enterprise-wide provenance tracking for real-time APT detection,'' *IEEE Trans. Inf. Forensics Security*, vol. 16, pp. 4363–4376, 2021, doi: 10.1109/TIFS.2021.3098977.

[33] L.-X. Yang, K. Huang, X. Yang, Y. Zhang, Y. Xiang, and Y. Y. Tang, ''Defense against advanced persistent threat through data backup and recovery,'' *IEEE Trans. Netw. Sci. Eng.*, vol. 8, no. 3, pp. 2001–2013, Jul. 2021, doi: 10.1109/TNSE.2020.3040247.

[34] A. Sharma, B. B. Gupta, A. K. Singh, and V. K. Saraswat, ''Advanced persistent threats (APT): Evolution, anatomy, attribution and countermeasures,'' *J. Ambient Intell. Humanized Comput.*, vol. 14, no. 7, pp. 9355–9381, Jul. 2023, doi: 10.1007/s12652-023-04603-y.

[35] I. Kara, ''Fileless malware threats: Recent advances, analysis approach through memory forensics and research challenges,'' *Exp. Syst. Appl.*, vol. 214, Mar. 2023, Art. no. 119133, doi: 10.1016/j.eswa.2022.119133.

[36] S. Kumar, ''An emerging threat fileless malware: A survey and research challenges,'' *Cybersecurity*, vol. 3, no. 1, p. 1, Dec. 2020, doi: 10.1186/s42400-019-0043-x.

[37] Z. Wang, Q. Liu, and Y. Chi, ''Review of Android malware detection based on deep learning,'' *IEEE Access*, vol. 8, pp. 181102–181126, 2020, doi: 10.1109/ACCESS.2020.3028370.

[38] Y. Liu, C. Tantithamthavorn, L. Li, and Y. Liu, ''Deep learning for Android malware defenses: A systematic literature review,'' *ACM Comput. Surveys*, vol. 55, no. 8, pp. 1–36, Aug. 2023, doi: 10.1145/3544968.

[39] A. Gaurav, B. B. Gupta, and P. K. Panigrahi, ''A comprehensive survey on machine learning approaches for malware detection in IoT-based enterprise information system,'' *Enterprise Inf. Syst.*, vol. 17, no. 3, Mar. 2023, Art. no. 2023764, doi: 10.1080/17517575.2021.2023764.

[40] P. Victor, A. Habibi, L. Rongxing, L. Tinshu, S. Pulei, and X. Shahrear, *IoT Malware: An Attribute-Based Taxonomy, Detection Mechanisms and Challenges*. Cham, Switzerland: Springer, 2023.

[41] C. Alex, G. Creado, W. Almobaideen, O. A. Alghanam, and M. Saadeh, ''A comprehensive survey for IoT security datasets taxonomy, classification and machine learning mechanisms,'' *Comput. Secur.*, vol. 132, Sep. 2023, Art. no. 103283, doi: 10.1016/j.cose.2023.103283.

[42] Y. Ye, T. Li, D. Adjeroh, and S. S. Iyengar, ''A survey on malware detection using data mining techniques,'' *ACM Comput. Surveys*, vol. 50, no. 3, pp. 1–40, May 2018, doi: 10.1145/3073559.

[43] A. Abusitta, M. Q. Li, and B. C. M. Fung, ''Malware classification and composition analysis: A survey of recent developments,'' *J. Inf. Secur. Appl.*, vol. 59, Jun. 2021, Art. no. 102828, doi: 10.1016/j.jisa.2021.102828.

[44] C. Beaman, A. Barkworth, T. D. Akande, S. Hakak, and M. K. Khan, ''Ransomware: Recent advances, analysis, challenges and future research directions,'' *Comput. Secur.*, vol. 111, Dec. 2021, Art. no. 102490, doi: 10.1016/J.COSE.2021.102490.

[45] L. Caviglione, M. Choras, I. Corona, A. Janicki, W. Mazurczyk, M. Pawlicki, and K. Wasielewska, ''Tight arms race: Overview of current malware threats and trends in their detection,'' *IEEE Access*, vol. 9, pp. 5371–5396, 2021, doi: 10.1109/ACCESS.2020.3048319.

[46] H. Orman, ''The Morris worm: A fifteen-year perspective,'' *IEEE Secur. Privacy*, vol. 1, no. 5, pp. 35–43, Sep. 2003, doi: 10.1109/MSECP.2003.1236233.

[47] J. Bates, E. Wilding, and F. Skulason, ''Trojan horse: AIDS information introductory diskette version 2.0,'' *Virus Bull.*, pp. 1–20, Jan. 1990. [Online]. Available: https://www.virusbulletin.com/uploads/pdf/magazine/1990/199001.pdf

[48] P. Szor, *The art of Computer Virus Research and Defense: Art Comp Virus Res Defense*. London, U.K.: Pearson Education, 2005, p. 1.

[49] M. N. Alenezi, H. K. Alabdulrazzaq, A. A. Alshaher, and M. M. Alkharang, ''Evolution of malware threats and techniques: A review,'' *Int. J. Commun. Netw. Inf. Secur.*, vol. 12, no. 3, pp. 326–337, Apr. 2022, doi: 10.17762/ijcnis.v12i3.4723.

[50] D. Moore, C. Shannon, and K. Claffy, ''Code-red: A case study on the spread and victims of an internet worm,'' *Proc. 2nd Internet Meas. Work. (IMW)*, 2002, pp. 273–284.

[51] A. Mackie, J. Roculan, R. Russel, and M. Van Velzen, "Nimda worm analysis," *Secur. Focus. Incid. Anal. Rep. Version*, vol. 2, pp. 1–21, Sep. 2002. [Online]. Available: http://dpnm.postech.ac.kr/research/04/nsri/papers/010919-Analysis-Nimda.pdf.

[52] Wikipedia. (2022). *Beast (Trojan Horse)*. Accessed: Jun. 4, 2023. [Online]. Available: https://en.wikipedia.org/wiki/Beast_(Trojan_horse)

[53] Wikipedia. *Zeus (Malware)*. Accessed: Jun. 4, 2023. [Online]. Available: https://en.wikipedia.org/wiki/Zeus_(malware)

[54] Wikipedia. (2022). *Torpig*. Accessed: Jun. 4, 2023. [Online]. Available: https://en.wikipedia.org/wiki/Torpig

[55] K. Howard. *How Trojan Malware is Evolving to Survive and Evade Cybersecurity in 2021*. Accessed: Jan. 26, 2021. [Online]. Available: https://umbrella.cisco.com/blog/how-trojan-malware-is-evolving-to-survive-and-evade-cybersecurity-in-2021

[56] I Digital Guide. *What is a Rootkit?*. Accessed: May 30, 2023. [Online]. Available: https://www.ionos.com/digitalguide/server/security/what-is-a-rootkit/

[57] Wikipedia. (2021). *Mebroot*. Accessed: Jun. 4, 2023. [Online]. Available: https://en.wikipedia.org/wiki/Mebroot

[58] T. Moes. *Rootkit Examples (2023): The 10 Worst Attacks of All Time*. Accessed: May 30, 2023. [Online]. Available: https://softwarelab.org/blog/rootkit-examples/

[59] V. Drake. (2022). *The History and Evolution of Ransomware Attacks*. Accessed: Apr. 29, 2023. [Online]. Available: https://flashpoint.io/blog/the-history-and-evolution-of-ransomware-attacks/

[60] K. Savage, P. Coogan, and H. Lau. (2015). *Symantec Security Response The Evolution of Ransomware*. p. 57. [Online]. Available: http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/the-evolution-of-ransomware.pdf

[61] A. Gostev. *Krotten Source Traced–for the Moment*. Kaspersky. Accessed May 30, 2023. [Online]. Available: https://securelist.com/krotten-source-traced-for-the-moment/30086/

[62] D. Y. Huang, M. M. Aliapoulios, V. G. Li, L. Invernizzi, E. Bursztein, K. McRoberts, J. Levin, K. Levchenko, A. C. Snoeren, and D. McCoy, "Tracking ransomware end-to-end," in *Proc. IEEE Symp. Secur. Privacy (SP)*, May 2018, pp. 618–631, doi: 10.1109/SP.2018.00047.

[63] C. Catalano, A. Chezzi, M. Angelelli, and F. Tommasi, "Deceiving AI-based malware detection through polymorphic attacks," *Comput. Ind.*, vol. 143, Dec. 2022, Art. no. 103751, doi: 10.1016/j.compind.2022.103751.

[64] D. Javaheri, P. Lalbakhsh, and M. Hosseinzadeh, "A novel method for detecting future generations of targeted and metamorphic malware based on genetic algorithm," *IEEE Access*, vol. 9, pp. 69951–69970, 2021, doi: 10.1109/ACCESS.2021.3077295.

[65] F. Barr-Smith, X. Ugarte-Pedrero, M. Graziano, R. Spolaor, and I. Martinovic, "Survivalism: Systematic analysis of windows malware living-off-the-land," in *Proc. IEEE Symp. Secur. Privacy (SP)*, May 2021, pp. 1557–1574, doi: 10.1109/SP40001.2021.00047.

[66] D.-Y. KAO, S.-C. HSIAO, and R. TSO, "Analyzing WannaCry ransomware considering the weapons and exploits," in *Proc. 21st Int. Conf. Adv. Commun. Technol. (ICACT)*, Feb. 2019, pp. 1098–1107, doi: 10.23919/ICACT.2019.8702049.

[67] S. Primer. (2020). *Ryuk*. Accessed: May 7, 2023. [Online]. Available: https://www.cisecurity.org/wp-content/uploads/2020/01/Security-Primer-Ryuk-2.pdf

[68] K. June. (2020). *The New Generation of Ransomware—An in Depth Study of Ransomware-as-a-Service*. [Online]. Available: http://essay.utwente.nl/81595/1/Keijzer_MA_EEMCS.pdf

[69] C. Wuest. (2020). *Digital CoronaVirus: Yet Another Ransomware Combined With Infostealer*. Accessed: May 10, 2023. [Online]. Available: https://www.acronis.com/en-us/blog/posts/digital-coronavirus-yet-another-ransomware-combined-infostealer/

[70] C. D. Jen Easterly. *The Attack on Colonial Pipeline: What We've Learned & What We've Done Over the Past Two Years*. Accessed: May 15, 2023. [Online]. Available: https://www.cisa.gov/news-events/news/attack-colonial-pipeline-what-weve-learned-what-weve-done-over-past-two-years

[71] Wikipedia. *JBS S.A. Ransomware Attack*. Accessed: May 2, 2023. [Online]. Available: https://en.wikipedia.org/wiki/JBS_S.A._ransomware_attack

[72] CISA. (2021). *Kaseya Ransomware Attack: Guidance for Affected MSPs and Their Customers*. Accessed: Mar. 6, 2023. [Online]. Available: https://www.cisa.gov/news-events/news/kaseya-ransomware-attack-guidance-affected-msps-and-their-customers

[73] S Staff. (2022). *Ransomware Attacks Decreased 61% in 2022*. Accessed: Feb. 12, 2023. [Online]. Available: https://www.securitymagazine.com/articles/98772-ransomware-attacks-decreased-61-in-2022

[74] R. Lakshmanan. *Improved BlackCat Ransomware Strikes with Lightning Speed and Stealthy Tactics*. Accessed: Jun. 4, 2023. [Online]. Available: https://thehackernews.com/2023/06/improved-blackcat-ransomware-strikes.html?m=1

[75] K. Oleinichenko. (2022). *How Malware Has Evolved Over Time*. Accessed: Mar. 30, 2023. [Online]. Available: https://riskxchange.co/1006358/how-malware-has-evolved-over-time/

[76] B. Stojanović, K. Hofer-Schmitz, and U. Kleb, "APT datasets and attack modeling for automated detection methods: A review," *Comput. Secur.*, vol. 92, May 2020, Art. no. 101734, doi: 10.1016/j.cose.2020.101734.

[77] Securin. (2021). *SolarWinds-Attackers at It Again in Back-to-Back Campaigns*. Accessed: May 30, 2023. [Online]. Available: https://www.securin.io/solarwinds-attackers-at-it-again-in-back-to-back-campaigns/

[78] T. Thompson. (2021). *The Colonial Pipeline Ransomware Attack and the SolarWinds Hack Were all but Inevitable—Why National Cyber Defense is a 'Wicked' Problem*. Accessed: May 30, 2023. [Online]. Available: https://theconversation.com/the-colonial-pipeline-ransomware-attack-and-the-solarwinds-hack-were-all-but-inevitable-why-national-cyber-defense-is-a-wicked-problem-160661

[79] P. Id. (2023). *Hunting Russian Intelligence 'Snake' Malware*. [Online]. Available: https://www.cisa.gov/sites/default/files/2023-05/aa23-129a_snake_malware_2.pdf

[80] Kaspersky Research. (2022). *ToddyCat: An Advanced Threat Actor Targets High-Profile Entities With New Malware*. Accessed: Jun. 9, 2023. [Online]. Available: https://www.kaspersky.com/about/press-releases/2022_toddycat-an-advanced-threat-actor-targets-high-profile-entities-with-new-malware

[81] WatchGuard Technologies. (2021). *New Research: Fileless Malware Attacks Surge by 900% and Cryptominers Make a Comeback, While Ransomware Attacks Decline*. Accessed: Feb. 25, 2023. [Online]. Available: https://www.globenewswire.com/en/news-release/2021/03/30/2201173/0/en/New-Research-Fileless-Malware-Attacks-Surge-by-900-and-Cryptominers-Make-a-Comeback-While-Ransomware-Attacks-Decline.html

[82] J. Sadowski and C. Charrier. *Move, Patch, Get Out the Way: 2022 Zero-Day Exploitation Continues at an Elevated Pace*. Accessed: May 15, 2023. [Online]. Available: https://www.mandiant.com/resources/blog/zero-days-exploited-2022

[83] D. Winder. (2022). *This Zero-Day Twitter Hack Has Already Impacted 5.5 Million Users: Report*. Accessed: May 10, 2023. [Online]. Available: https://www.forbes.com/sites/daveywinder/2022/11/29/zero-day-twitter-hack-confirmed-impact-could-exceed-20-million-users-report/?sh=3a1f876d56c5

[84] E. Harper. (2019). *Exodus Spyware Targets iPhones & Android Phones to Collect All of Your Personal Data*. Accessed: Jul. 18, 2023. [Online]. Available: https://www.techlicious.com/blog/exodus-spyware-android-iphone/#google_vignette

[85] A. Husar. (2022). *IoT Security: 5 Cyber-Attacks Caused by IoT Security Vulnerabilities*. Accessed: Jul. 7, 2023. [Online]. Available: https://www.cm-alliance.com/cybersecurity-blog/iot-security-5-cyber-attacks-caused-by-iot-security-vulnerabilities

[86] A. Mascellino. *ChatGPT Creates Polymorphic Malware*. Accessed: Jun. 11, 2023. [Online]. Available: https://www.infosecurity-magazine.com/news/chatgpt-creates-polymorphic-malware/

[87] J. Ferdous, R. Islam, M. Bhattacharya, and M. Z. Islam, "Malware resistant data protection in hyper-connected networks: A survey," 2023, *arXiv:2307.13164*.

[88] C. Pott, B. Gulmezoglu, and T. Eisenbarth, "Overcoming the pitfalls of HPC-based cryptojacking detection in presence of GPUs," in *Proc. 13th ACM Conf. Data Appl. Secur. Priv.*, 2023, pp. 177–188, doi: 10.1145/3577923.3583655.

[89] H. L. J. Bijmans, T. M. Booij, and C. Doerr, "Just the tip of the iceberg: Internet-scale exploitation of routers for cryptojacking," Proc. ACM Conf. Comput. Commun. Secur., pp. 449–464, 2019, doi: 10.1145/3319535.3354230.

[90] F. A. Aponte-Novoa, D. P. Álvarez, R. Villanueva-Polanco, A. L. S. Orozco, and L. J. G. Villalba, "On detecting cryptojacking on websites: Revisiting the use of classifiers," *Sensors*, vol. 22, no. 23, pp. 1–15, 2022, doi: 10.3390/s22239219.

[91] A. Hernandez-Suarez, G. Sanchez-Perez, L. K. Toscano-Medina, J. Olivares-Mercado, J. Portillo-Portilo, J.-G. Avalos, and L. J. G. Villalba, "Detecting cryptojacking web threats: An approach with autoencoders and deep dense neural networks," *Appl. Sci.*, vol. 12, no. 7, p. 3234, Mar. 2022, doi: 10.3390/app12073234.

[92] H.-J. Zhu, Z.-H. You, Z.-X. Zhu, W.-L. Shi, X. Chen, and L. Cheng, "DroidDet: Effective and robust detection of Android malware using static analysis along with rotation forest model," *Neurocomputing*, vol. 272, pp. 638–646, Jan. 2018, doi: 10.1016/j.neucom.2017.07.030.

[93] P. Faruki, A. Bharmal, V. Laxmi, V. Ganmoor, M. S. Gaur, M. Conti, and M. Rajarajan, "Android security: A survey of issues, malware penetration, and defenses," *IEEE Commun. Surveys Tuts.*, vol. 17, no. 2, pp. 998–1022, 2nd Quart., 2015, doi: 10.1109/COMST.2014.2386139.

[94] Y. Zhou and X. Jiang, "Dissecting Android malware: Characterization and evolution," in *Proc. IEEE Symp. Secur. Priv.*, no. 4 Jul. 2012, pp. 95–109, doi: 10.1109/SP.2012.16.

[95] V. Rey, P. M. S. Sánchez, A. H. Celdrán, and G. Bovet, "Federated learning for malware detection in IoT devices," *Comput. Netw.*, vol. 204, Feb. 2022, Art. no. 108693, doi: 10.1016/j.comnet.2021.108693.

[96] *Mirai Botnet: How IoT Devices Almost Brought Down The Internet*. Accessed: Jun. 18, 2023. [Online]. Available: https://www.secureblink.com/threat-research/mirai

[97] S. H. Kok, A. Abdullah, N. Z. Jhanjhi, and M. Supramaniam, "Ransomware, threat and detection techniques: A review," *Int. J. Comput. Sci. Netw. Secur.*, vol. 19, no. 2, pp. 136–146, Feb. 2019.

[98] R. Lakshmanan. (2021). *Hackers Breached Colonial Pipeline Using Compromised VPN Password*. Accessed: Jun. 7, 2023. [Online]. Available: https://thehackernews.com/2021/06/hackers-breached-colonial-pipeline.html

[99] Wikipedia. *Colonial Pipeline*. Accessed: Jun. 7, 2023. [Online]. Available: https://en.wikipedia.org/wiki/Colonial_Pipeline

[100] CrowdStrike. (2021). *What is a Supply Chain AttacK?* Accessed: Jun. 17, 2023. [Online]. Available: https://www.crowdstrike.com/cybersecurity-101/cyberattacks/supply-chain-attacks/

[101] A. Andreoli, A. Lounis, M. Debbabi, and A. Hanna, "On the prevalence of software supply chain attacks: Empirical study and investigative framework," *Forensic Sci. Int., Digit. Invest.*, vol. 44, Mar. 2023, Art. no. 301508, doi: 10.1016/j.fsidi.2023.301508.

[102] G. Dedola. (2022). *APT ToddyCat*. Kaspersky. Accessed: Jun. 9, 2023. [Online]. Available: https://securelist.com/toddycat/106799/

[103] A. Zimba, H. Chen, Z. Wang, and M. Chishimba, "Modeling and detection of the multi-stages of advanced persistent threats attacks based on semi-supervised learning and complex networks characteristics," *Future Gener. Comput. Syst.*, vol. 106, pp. 501–517, May 2020, doi: 10.1016/j.future.2020.01.032.

[104] C. Do Xuan and D. Huong, "A new approach for APT malware detection based on deep graph network for endpoint systems," *Appl. Intell.*, vol. 52, pp. 14005–14024, Mar. 2022, doi: 10.1007/s10489-021-03138-z.

[105] A. Greenberg. (2018). *The Untold Story of NotPetya, the Most Devastating Cyberattack in History*. Wired. Accessed: Jun. 17, 2023. [Online]. Available: https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/

[106] Ö. Aslan, M. Ozkan-Okay, and D. Gupta, "Intelligent behavior-based malware detection system on cloud computing environment," *IEEE Access*, vol. 9, pp. 83252–83271, 2021, doi: 10.1109/ACCESS.2021.3087316.

[107] M. K. Pratt. (2022). *Remote Work Cybersecurity: 12 Risks and how to Prevent Them*. Accessed: Jun. 20, 2023. [Online]. Available: https://www.techtarget.com/searchsecurity/tip/Remote-work-cybersecurity-12-risks-and-how-to-prevent-them

[108] *Recent Cyberattacks*. Accessed: Sep. 15, 2023. [Online]. Available: https://www.fortinet.com/resources/cyberglossary/ransomware

[109] B. Zhang, W. Xiao, X. Xiao, A. K. Sangaiah, W. Zhang, and J. Zhang, "Ransomware classification using patch-based CNN and self-attention network on embedded N-grams of opcodes," *Future Gener. Comput. Syst.*, vol. 110, pp. 708–720, Sep. 2020, doi: 10.1016/j.future.2019.09.025.

[110] T. Pósa and J. Grossklags, "Work experience as a factor in cyber-security risk awareness: A survey study with university students," *J. Cybersecurity Privacy*, vol. 2, no. 3, pp. 490–515, Jun. 2022, doi: 10.3390/jcp2030025.

[111] Q. Vu Khanh, V.-H. Nguyen, Q. N. Minh, A. D. Van, N. Le Anh, and A. Chehri, "An efficient edge computing management mechanism for sustainable smart cities," *Sustain. Comput., Informat. Syst.*, vol. 38, Apr. 2023, Art. no. 100867, doi: 10.1016/j.suscom.2023.100867.

[112] L. A. Gordon, M. P. Loeb, and L. Zhou, "Integrating cost–benefit analysis into the NIST cybersecurity framework via the Gordon–Loeb model," *J. Cybersecurity*, vol. 6, no. 1, pp. 1–8, Jan. 2020, doi: 10.1093/CYBSEC/TYAA005.

[113] F. R. Moreira, D. A. Da Silva Filho, G. D. A. Nze, R. T. de Sousa Júnior, and R. R. Nunes, "Evaluating the performance of NIST's framework cybersecurity controls through a constructivist multicriteria methodology," *IEEE Access*, vol. 9, pp. 129605–129618, 2021, doi: 10.1109/ACCESS.2021.3113178.

[114] N. Sun, C.-T. Li, H. Chan, M. Z. Islam, M. R. Islam, and W. Armstrong, "How do organizations seek cyber assurance? Investigations on the adoption of the common criteria and beyond," *IEEE Access*, vol. 10, pp. 71749–71763, 2022, doi: 10.1109/ACCESS.2022.3187211.

[115] S. Nifakos, "Influence of human factors on cyber security within healthcare organisations: A systematic review," *Sensors*, vol. 21, no. 15, pp. 1–25, 2021, doi: 10.3390/s21155119.

[116] J. Wang, P. Gong, H. Wang, W. Zhang, C. Sun, and B. Zhao, "A right transfer access control model of Internet of Things based on smart contract," *Secur. Commun. Netw.*, vol. 2022, pp. 1–11, May 2022, doi: 10.1155/2022/3682952.

[117] A. Omran Almagrabi, "An efficient security solution for industrial Internet of Things applications," *Comput., Mater. Continua*, vol. 72, no. 2, pp. 3961–3983, 2022, doi: 10.32604/cmc.2022.026513.

[118] N. Moukafih, G. Orhanou, and S. El Hajji, "Neural network-based voting system with high capacity and low computation for intrusion detection in SIEM/IDS systems," *Secur. Commun. Netw.*, vol. 2020, pp. 1–15, Jul. 2020, doi: 10.1155/2020/3512737.

[119] J. Yang and H. Lim, "Deep learning approach for detecting malicious activities over encrypted secure channels," *IEEE Access*, vol. 9, pp. 39229–39244, 2021, doi: 10.1109/ACCESS.2021.3064561.

[120] F. A. Aboaoja, A. Zainal, F. A. Ghaleb, B. A. S. Al-rimy, T. A. E. Eisa, and A. A. H. Elnour, "Malware detection issues, challenges, and future directions: A survey," *Appl. Sci.*, vol. 12, no. 17, p. 8482, Aug. 2022, doi: 10.3390/app12178482.

[121] E. B. Karbab, M. Debbabi, and A. Derhab, "SwiftR: Cross-platform ransomware fingerprinting using hierarchical neural networks on hybrid features," *Exp. Syst. Appl.*, vol. 225, Sep. 2023, Art. no. 120017, doi: 10.1016/j.eswa.2023.120017.

[122] J. Singh, K. Sharma, M. Wazid, and A. K. Das, "SINN-RD: Spline interpolation-envisioned neural network-based ransomware detection scheme," *Comput. Electr. Eng.*, vol. 106, Mar. 2023, Art. no. 108601, doi: 10.1016/j.compeleceng.2023.108601.

[123] S. Homayoun, A. Dehghantanha, M. Ahmadzadeh, S. Hashemi, R. Khayami, K.-K.-R. Choo, and D. E. Newton, "DRTHIS: Deep ransomware threat hunting and intelligence system at the fog layer," *Future Gener. Comput. Syst.*, vol. 90, pp. 94–104, Jan. 2019, doi: 10.1016/j.future.2018.07.045.

[124] D. W. Fernando and N. Komninos, "FeSA: Feature selection architecture for ransomware detection under concept drift," *Comput. Secur.*, vol. 116, May 2022, Art. no. 102659, doi: 10.1016/j.cose.2022.102659.

[125] R. A. M. Alsaidi, W. M. S. Yafooz, H. Alolofi, G. A.-M. Taufiq-Hail, A.-H.-M. Emara, and A. Abdel-Wahab, "Ransomware detection using machine and deep learning approaches," *Int. J. Adv. Comput. Sci. Appl.*, vol. 13, no. 11, pp. 112–119, 2022, doi: 10.14569/IJACSA.2022.0131112.

[126] C. Do Xuan and M. H. Dao, "A novel approach for APT attack detection based on combined deep learning model," *Neural Comput. Appl.*, vol. 33, no. 20, pp. 13251–13264, Oct. 2021, doi: 10.1007/s00521-021-05952-5.

[127] W. Niu, J. Zhou, Y. Zhao, X. Zhang, Y. Peng, and C. Huang, "Uncovering APT malware traffic using deep learning combined with time sequence and association analysis," *Comput. Secur.*, vol. 120, Sep. 2022, Art. no. 102809, doi: 10.1016/j.cose.2022.102809.

[128] A. S. Bozkir, E. Tahillioglu, M. Aydos, and I. Kara, "Catch them alive: A malware detection approach through memory forensics, manifold learning and computer vision," *Comput. Secur.*, vol. 103, Apr. 2021, Art. no. 102166, doi: 10.1016/j.cose.2020.102166.

[129] S. Shukla, S. Rafatirad, H. Homayoun, and S. M. P. Dinakarrao, "Federated learning with heterogeneous models for on-device malware detection in IoT networks," in *Proc. Design, Autom. Test Eur. (DATE)*, Apr. 2023, pp. 1–6, doi: 10.23919/DATE56975.2023.10137288.

[130] X. Sáez-de-Cámara, J. L. Flores, C. Arellano, A. Urbieta, and U. Zurutuza, "Clustered federated learning architecture for network anomaly detection in large scale heterogeneous IoT networks," *Comput. Secur.*, vol. 131, Aug. 2023, Art. no. 103299, doi: 10.1016/j.cose.2023.103299.

[131] A. De Paola, S. Gaglio, G. L. Re, and M. Morana, "A hybrid system for malware detection on big data," in *Proc. IEEE Conf. Comput. Commun. Workshops (INFOCOM WKSHPS)*, Apr. 2018, pp. 45–50, doi: 10.1109/INFCOMW.2018.8406963.

[132] U. Garg, S. Kumar, and M. Kumar, "A hybrid approach for the detection and classification of MQTT-based IoT-malware," in *Proc. Int. Conf. Sustain. Comput. Data Commun. Syst. (ICSCDS)*, Mar. 2023, pp. 1154–1159, doi: 10.1109/ICSCDS56580.2023.10104820.

[133] Y. Zhao, L. Li, H. Wang, H. Cai, T. F. Bissyandé, J. Klein, and J. Grundy, "On the impact of sample duplication in machine-learning-based Android malware detection," *ACM Trans. Softw. Eng. Methodol.*, vol. 30, no. 3, pp. 1–38, Jul. 2021, doi: 10.1145/3446905.

[134] D. Ö. Sahin, S. Akleylek, and E. Kiliç, "LinRegDroid: Detection of Android malware using multiple linear regression models-based classifiers," *IEEE Access*, vol. 10, pp. 14246–14259, 2022, doi: 10.1109/ACCESS.2022.3146363.

[135] T. Kim, B. Kang, M. Rho, S. Sezer, and E. G. Im, "A multimodal deep learning method for Android malware detection using various features," *IEEE Trans. Inf. Forensics Security*, vol. 14, no. 3, pp. 773–788, Mar. 2019, doi: 10.1109/TIFS.2018.2866319.

[136] R. Islam, M. I. Sayed, S. Saha, M. J. Hossain, and M. A. Masud, "Android malware classification using optimum feature selection and ensemble machine learning," *Internet Things Cyber-Phys. Syst.*, vol. 3, pp. 100–111, Jan. 2023, doi: 10.1016/j.iotcps.2023.03.001.

[137] H. Bakır and R. Bakır, "DroidEncoder: Malware detection using auto-encoder based feature extractor and machine learning algorithms," *Comput. Electr. Eng.*, vol. 110, Sep. 2023, Art. no. 108804, doi: 10.1016/j.compeleceng.2023.108804.

[138] S. R. Davies, R. Macfarlane, and W. J. Buchanan, "Differential area analysis for ransomware attack detection within mixed file datasets," *Comput. Secur.*, vol. 108, Sep. 2021, Art. no. 102377, doi: 10.1016/J.COSE.2021.102377.

[139] B. A. S. Al-Rimy, M. A. Maarof, and S. Z. M. Shaid, "Crypto-ransomware early detection model using novel incremental bagging with enhanced semi-random subspace selection," *Future Gener. Comput. Syst.*, vol. 101, pp. 476–491, Dec. 2019, doi: 10.1016/j.future.2019.06.005.

[140] M. Rhode, P. Burnap, and A. Wedgbury, "Real-time malware process detection and automated process killing," *Secur. Commun. Netw.*, vol. 2021, pp. 1–23, Dec. 2021, doi: 10.1155/2021/8933681.

[141] J. A. Herrera-Silva and M. Hernández-Álvarez, "Dynamic feature dataset for ransomware detection using machine learning algorithms," *Sensors*, vol. 23, no. 3, p. 1053, Jan. 2023, doi: 10.3390/s23031053.

[142] H. Zhang, X. Xiao, F. Mercaldo, S. Ni, F. Martinelli, and A. K. Sangaiah, "Classification of ransomware families with machine learning based on N-gram of opcodes," *Future Gener. Comput. Syst.*, vol. 90, pp. 211–221, Jan. 2019, doi: 10.1016/j.future.2018.07.052.

[143] E. Berrueta, D. Morato, E. Magaña, and M. Izal, "Crypto-ransomware detection using machine learning models in file-sharing network scenarios with encrypted traffic," *Exp. Syst. Appl.*, vol. 209, Dec. 2022, Art. no. 118299, doi: 10.1016/j.eswa.2022.118299.

[144] M. S. Abbasi, H. Al-Sahaf, M. Mansoori, and I. Welch, "Behavior-based ransomware classification: A particle swarm optimization wrapper-based approach for feature selection," *Appl. Soft Comput.*, vol. 121, May 2022, Art. no. 108744, doi: 10.1016/j.asoc.2022.108744.

[145] A. O. Almashhadani, D. Carlin, M. Kaiiali, and S. Sezer, "MFMCNS: A multi-feature and multi-classifier network-based system for ransomworm detection," *Comput. Secur.*, vol. 121, Oct. 2022, Art. no. 102860, doi: 10.1016/j.cose.2022.102860.

[146] C.-M. Hsu, C.-C. Yang, H.-H. Cheng, P. E. Setiasabda, and J.-S. Leu, "Enhancing file entropy analysis to improve machine learning detection rate of ransomware," *IEEE Access*, vol. 9, pp. 138345–138351, 2021, doi: 10.1109/ACCESS.2021.3114148.

[147] I. Ghafir, M. Hammoudeh, V. Prenosil, L. Han, R. Hegarty, K. Rabie, and F. J. Aparicio-Navarro, "Detection of advanced persistent threat using machine-learning correlation analysis," *Future Gener. Comput. Syst.*, vol. 89, pp. 349–359, Dec. 2018, doi: 10.1016/j.future.2018.06.055.

[148] I. Ghafir, K. G. Kyriakopoulos, S. Lambotharan, F. J. Aparicio-Navarro, B. Assadhan, H. Binsalleeh, and D. M. Diab, "Hidden Markov models and alert correlations for the prediction of advanced persistent threats," *IEEE Access*, vol. 7, pp. 99508–99520, 2019, doi: 10.1109/ACCESS.2019.2930200.

[149] C. Do Xuan, M. H. Dao, and H. D. Nguyen, "APT attack detection based on flow network analysis techniques using deep learning," *J. Intell. Fuzzy Syst.*, vol. 39, no. 3, pp. 4785–4801, Oct. 2020, doi: 10.3233/JIFS-200694.

[150] C. Xiong, T. Zhu, W. Dong, L. Ruan, R. Yang, Y. Cheng, Y. Chen, S. Cheng, and X. Chen, "Conan: A practical real-time APT detection system with high accuracy and efficiency," *IEEE Trans. Dependable Secur. Comput.*, vol. 19, no. 1, pp. 551–565, Jan. 2022, doi: 10.1109/TDSC.2020.2971484.

[151] R. P. Baksi and S. J. Upadhyaya, "Decepticon: A theoretical framework to counter advanced persistent threats," *Inf. Syst. Frontiers*, vol. 23, no. 4, pp. 897–913, Aug. 2021, doi: 10.1007/s10796-020-10087-4.

[152] S. Moothedath, D. Sahabandu, J. Allen, A. Clark, L. Bushnell, W. Lee, and R. Poovendran, "A game-theoretic approach for dynamic information flow tracking to detect multistage advanced persistent threats," *IEEE Trans. Autom. Control*, vol. 65, no. 12, pp. 5248–5263, Dec. 2020, doi: 10.1109/TAC.2020.2976040.

[153] L.-X. Yang, P. Li, Y. Zhang, X. Yang, Y. Xiang, and W. Zhou, "Effective repair strategy against advanced persistent threat: A differential game approach," *IEEE Trans. Inf. Forensics Security*, vol. 14, no. 7, pp. 1713–1728, Jul. 2019, doi: 10.1109/TIFS.2018.2885251.

[154] S. Rass, S. König, and S. Schauer, "Defending against advanced persistent threats using game-theory," *PloS One*, vol. 12, no. 1, 2017, Art. no. e0168675.

[155] B. N. Sanjay, D. C. Rakshith, R. B. Akash, and D. V. V. Hegde, "An approach to detect fileless malware and defend its evasive mechanisms," in *Proc. 3rd Int. Conf. Comput. Syst. Inf. Technol. Sustain. Solutions (CSITSS)*, Dec. 2018, pp. 234–239, doi: 10.1109/CSITSS.2018.8768769.

[156] P. Borana, V. Sihag, G. Choudhary, M. Vardhan, and P. Singh, "An assistive tool for fileless malware detection," in *Proc. World Autom. Congr.*, Aug. 2021, pp. 21–25, doi: 10.23919/WAC50355.2021.9559449.

[157] R. Chaganti, V. Ravi, and T. D. Pham, "Deep learning based cross architecture Internet of Things malware detection and classification," *Comput. Secur.*, vol. 120, Sep. 2022, Art. no. 102779, doi: 10.1016/j.cose.2022.102779.

[158] M. A. Abdullah, Y. Yu, K. Adu, Y. Imrana, X. Wang, and J. Cai, "HCL-classifier: CNN and LSTM based hybrid malware classifier for Internet of Things (IoT)," *Future Gener. Comput. Syst.*, vol. 142, pp. 41–58, May 2023, doi: 10.1016/j.future.2022.12.034.

[159] S. H. Khan, T. J. Alahmadi, W. Ullah, J. Iqbal, A. Rahim, H. K. Alkahtani, W. Alghamdi, and A. O. Almagrabi, "A new deep boosted CNN and ensemble learning based IoT malware detection," *Comput. Secur.*, vol. 133, Oct. 2023, Art. no. 103385, doi: 10.1016/j.cose.2023.103385.

[160] S. K. Smmarwar, G. P. Gupta, and S. Kumar, "AI-empowered malware detection system for industrial Internet of Things," *Comput. Electr. Eng.*, vol. 108, May 2023, Art. no. 108731, doi: 10.1016/j.compeleceng.2023.108731.

[161] S. Ali, O. Abusabha, F. Ali, M. Imran, and T. Abuhmed, "Effective multitask deep learning for IoT malware detection and identification using behavioral traffic analysis," *IEEE Trans. Netw. Serv. Manag.*, vol. 20, no. 2, pp. 1199–1209, Jul. 2022, doi: 10.1109/TNSM.2022.3200741.

[162] M. Golmaryami, R. Taheri, Z. Pooranian, M. Shojafar, and P. Xiao, "SETTI: A self-supervised adversarial malware detection architecture in an IoT environment," *ACM Trans. Multimedia Comput. Commun. Appl.*, vol. 18, no. 2, pp. 1–21, 2022, doi: 10.1145/3536425.

[163] J. Tang, R. Li, Y. Jiang, X. Gu, and Y. Li, "Android malware obfuscation variants detection method based on multi-granularity opcode features," *Future Gener. Comput. Syst.*, vol. 129, pp. 141–151, Apr. 2022, doi: 10.1016/j.future.2021.11.005.

[164] H. Zhu, H. Wei, L. Wang, Z. Xu, and V. S. Sheng, "An effective end-to-end Android malware detection method," *Exp. Syst. Appl.*, vol. 218, May 2023, Art. no. 119593, doi: 10.1016/j.eswa.2023.119593.

[165] P. Bhat, S. Behal, and K. Dutta, "A system call-based Android malware detection approach with homogeneous & heterogeneous ensemble machine learning," *Comput. Secur.*, vol. 130, Jul. 2023, Art. no. 103277, doi: 10.1016/j.cose.2023.103277.

[166] E. Kolodenker, W. Koch, G. Stringhini, and M. Egele, "PayBreak: Defense against cryptographic ransomware," in *Proc. ACM Asia Conf. Comput. Commun. Secur.*, 2017, pp. 599–611, doi: 10.1145/3052973.3053035.

[167] J. Yun, J. Hur, Y. Shin, and D. Koo, "CLDSafe: An efficient file backup system in cloud storage against ransomware," *IEICE Trans. Inf. Syst.*, vol. E100.D, no. 9, pp. 2228–2231, 2017, doi: 10.1587/transinf.2017EDL8052.

[168] D. R. Matos, M. L. Pardal, G. Carle, and M. Correia, "RockFS: cloud-backed file system resilience to client-side attacks," in *Proc. 19th Int. Middleware Conf.*, Nov. 2018, pp. 107–119, doi: 10.1145/3274808.3274817.

[169] J. Park, S. Lee, and J. Kim, "RansomBlocker: A low-overhead ransomware-proof SSD," in *Proc. 56th ACM/IEEE Des. Autom. Conf.*, Jul. 2019, pp. 1–6.

[170] N. Z. Gorment, A. Selamat, L. K. Cheng, and O. Krejcar, "Machine learning algorithm for malware detection: Taxonomy, current challenges and future directions," *IEEE Access*, early access, 2023, doi: 10.1109/ACCESS.2023.3256979.

[171] N. Sahani, R. Zhu, J.-H. Cho, and C.-C. Liu, "Machine learning-based intrusion detection for smart grid computing: A survey," *ACM Trans. Cyber-Phys. Syst.*, vol. 7, no. 2, pp. 1–31, Apr. 2023, doi: 10.1145/3578366.

[172] B. Shavazipour, J. H. Kwakkel, and K. Miettinen, "Multi-scenario multi-objective robust optimization under deep uncertainty: A posteriori approach," *Environ. Model. Softw.*, vol. 144, Oct. 2021, Art. no. 105134, doi: 10.1016/j.envsoft.2021.105134.

[173] S. F. U. Rehman, "Practical implementation of artificial intelligence in cybersecurity—A study," *IJARCCE*, vol. 11, no. 11, Oct. 2022, Art. no. 111103, doi: 10.17148/ijarcce.2022.111103.

[174] U. Noor, Z. Anwar, A. W. Malik, S. Khan, and S. Saleem, "A machine learning framework for investigating data breaches based on semantic analysis of adversary's attack patterns in threat intelligence repositories," *Future Gener. Comput. Syst.*, vol. 95, pp. 467–487, Jun. 2019, doi: 10.1016/j.future.2019.01.022.

[175] S. Lee, H. K. Kim, and K. Kim, "Ransomware protection using the moving target defense perspective," *Comput. Electr. Eng.*, vol. 78, pp. 288–299, Sep. 2019, doi: 10.1016/J.COMPELECENG.2019.07.014.

[176] C. Keong Ng, S. Rajasegarar, L. Pan, F. Jiang, and L. Y. Zhang, "VoterChoice: A ransomware detection honeypot with multiple voting framework," *Concurrency Comput., Pract. Exper.*, vol. 32, no. 14, pp. 1–29, Jul. 2020, doi: 10.1002/cpe.5726.

[177] S. K. Shaukat and V. J. Ribeiro, "RansomWall: A layered defense system against cryptographic ransomware attacks using machine learning," in *Proc. IEEE Conf.*, Jul. 2018, pp. 356-363.

[178] A. Chowdhary, S. Pisharody, and D. Huang, "SDN based scalable MTD solution in cloud network," in *Proc. ACM Work. Mov. Target Defense, Co-Located (CCS)*, 2016, pp. 27–36, doi: 10.1145/2995272.2995274.

[179] P. Krishnan, S. Duttagupta, and K. Achuthan, "SDNFV based threat monitoring and security framework for multi-access edge computing infrastructure," *Mobile Netw. Appl.*, vol. 24, no. 6, pp. 1896–1923, Dec. 2019, doi: 10.1007/s11036-019-01389-2.

[180] S. Myneni, A. Chowdhary, D. Huang, and A. Alshamrani, "SmartDefense: A distributed deep defense against DDoS attacks with edge computing," *Comput. Netw.*, vol. 209, May 2022, Art. no. 108874, doi: 10.1016/j.comnet.2022.108874.

[181] F. Bonomi, R. Milito, J. Zhu, and S. Addepalli, "Fog computing and its role in the Internet of Things," in *Proc. 1st ACM Mob. Cloud Comput. Work.*, 2012, pp. 13–15, doi: 10.1145/2342509.2342513.

[182] J.-Y. Kim, S.-J. Bu, and S.-B. Cho, "Zero-day malware detection using transferred generative adversarial networks based on deep autoencoders," *Inf. Sci.*, vols. 460–461, pp. 83–102, Sep. 2018, doi: 10.1016/j.ins.2018.04.092.

[183] Z. He, A. Rezaei, H. Homayoun, and H. Sayadi, "Deep neural network and transfer learning for accurate hardware-based zero-day malware detection," in *Proc. Great Lakes Symp. VLSI*, vol. 1, no. 1. New York, NY, USA: Association for Computing Machinery, 2022, pp. 27–32.

[184] J. Zhao, S. Shetty, J. W. Pan, C. Kamhoua, and K. Kwiat, "Transfer learning for detecting unknown network attacks," *EURASIP J. Inf. Secur.*, vol. 2019, no. 1, pp. 1–13, Dec. 2019, doi: 10.1186/s13635-019-0084-4.

[185] W. El-Shafai, I. Almomani, and A. AlKhayer, "Visualized malware multi-classification framework using fine-tuned CNN-based transfer learning models," *Appl. Sci.*, vol. 11, no. 14, p. 6446, Jul. 2021, doi: 10.3390/app11146446.

JANNATUL FERDOUS received the Bachelor of Computing degree from the School of Computing and Mathematics, Charles Sturt University, Australia, and the master's degree in applied physics, electronics and communication engineering from Islamic University, Kushtia, Bangladesh. She is currently pursuing the Ph.D. degree with Charles Sturt University, focusing on malware analysis and classification, ransomware, and machine-learning techniques. She is also working on ransomware detection and mitigation using machine-learning methods.

RAFIQUL ISLAM is currently an Associate Professor with the Faculty of Business, Justice and Behavioral Sciences, School of Computing, Mathematics, and Engineering, Charles Sturt University, Australia. He has a strong research background in cybersecurity, focusing on malware analysis and classification, authentication, security in the cloud, privacy in social media, and the Internet of Things (IoT). He leads the cybersecurity research team and has developed a strong background in leadership, sustainability, and collaborative research. He has a strong publication record, with over 180 peer-reviewed research papers, chapters, and books. His contribution is recognized nationally and internationally through various professional, research, and leadership awards.

ARASH MAHBOUBI received the B.E. degree (Hons.) in computer science, specializing in computer security from Staffordshire University, Kuala Lumpur, Malaysia, in 2012, the master's degree in information security from the University of Technology Malaysia, Johor Bahru, Malaysia, in 2013, and the Ph.D. degree in computer science from the Queensland University of Technology (QUT), Brisbane, Australia, in 2018. Between 2016 and 2019, he was a Sessional Academic with the School of Electrical Engineering and Computer Science, QUT. Since 2019, he has been a Lecturer with the School of Computing and Mathematics, Charles Sturt University, Port Macquarie, NSW, Australia. His research interests include computer and mobile malware, ransomware, malware analysis, modeling, and the spread of malware epidemics.

MD. ZAHIDUL ISLAM is currently a Professor in computer science with the Faculty of Business, Justice, and Behavioural Sciences, Charles Sturt University. His main research interests include data mining, privacy, cyber security, and real-life applications of data mining and machine learning in various areas, including cyber security, agriculture, and health. He has published more than 120 peer-reviewed publications in journals and conferences.