

Security Informatics and Law Enforcement

Series Editor

Babak Akhgar

CENTRIC (Centre of Excellence in Terrorism, Resilience,
Intelligence and Organised Crime Research)
Sheffield Hallam University
Sheffield, UK

The primary objective of this book series is to explore contemporary issues related to law enforcement agencies, security services and industries dealing with security related challenges (e.g., government organizations, financial sector insurance companies and internet service providers) from an engineering and computer science perspective. Each book in the series provides a handbook style practical guide to one of the following security challenges:

Cyber Crime – Focuses on new and evolving forms of crimes. Books describe the current status of cybercrime and cyber terrorism developments, security requirements and practices.

Big Data Analytics, Situational Awareness and OSINT – Provides unique insight for computer scientists as well as practitioners in security and policing domains on big data possibilities and challenges for the security domain, current and best practices as well as recommendations.

Serious Games – Provides an introduction into the use of serious games for training in the security domain, including advice for designers/programmers, trainers and strategic decision makers.

Social Media in Crisis Management – explores how social media enables citizens to empower themselves during a crisis, from terrorism, public disorder, and natural disasters.

Law enforcement, Counterterrorism, and Anti-Trafficking – Presents tools from those designing the computing and engineering techniques, architecture or policies related to applications confronting radicalisation, terrorism, and trafficking.

The books pertain to engineers working in law enforcement and researchers who are researching on capabilities of LEAs, though the series is truly multidisciplinary – each book will have hard core computer science, application of ICT in security and security / policing domain chapters. The books strike a balance between theory and practice.

Iman Almomani • Leandros A. Maglaras •
Mohamed Amine Ferrag • Nick Ayres
Editors

Cyber Malware

Offensive and Defensive Systems

 Springer

Editors

Iman Almomani
Security Engineering Lab
Prince Sultan University
Riyadh, Saudi Arabia

Computer Science Department
The University of Jordan
Amman, Jordan

Mohamed Amine Ferrag
AI and Digital Science Research Center
Technology Innovation Institute
Masdar City, Abu Dhabi, United Arab
Emirates

Leandros A. Maglaras
School of Computing
Edinburgh Napier University
Edinburgh, UK

Nick Ayres
School of Computer Science and
Informatics
De Montfort University
Leicester, UK

ISSN 2523-8507

ISSN 2523-8515 (electronic)

Security Informatics and Law Enforcement

ISBN 978-3-031-34968-3

ISBN 978-3-031-34969-0 (eBook)

<https://doi.org/10.1007/978-3-031-34969-0>

© The Editor(s) (if applicable) and The Author(s), under exclusive license to Springer Nature Switzerland AG 2024

This work is subject to copyright. All rights are solely and exclusively licensed by the Publisher, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, reuse of illustrations, recitation, broadcasting, reproduction on microfilms or in any other physical way, and transmission or information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed.

The use of general descriptive names, registered names, trademarks, service marks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations and therefore free for general use.

The publisher, the authors, and the editors are safe to assume that the advice and information in this book are believed to be true and accurate at the date of publication. Neither the publisher nor the authors or the editors give a warranty, expressed or implied, with respect to the material contained herein or for any errors or omissions that may have been made. The publisher remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

This Springer imprint is published by the registered company Springer Nature Switzerland AG

The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

Paper in this product is recyclable.

PREFACE

The threat landscape is changing very quickly. With billions of connected IoT devices, mostly reactive detection and mitigation strategies, and finally big data challenges, we face an extremely rapidly expanding attack surface with a variety of attack vectors, a clear asymmetry between attackers and defenders, and a rapidly expanding attack surface. Additional arguments suggest that cybersecurity approaches must be rethought in terms of reducing the attack surface, making the attack surface dynamic, automating detection, risk assessment, and mitigation, and investigating the prediction and prevention of malware attacks with the use of emerging technologies like blockchain, artificial intelligence, and machine learning. Additionally, there is a clear asymmetry of attacks and an enormous amount of data.

This book provides the foundational aspects of malware attack vectors and appropriate defense mechanisms against malware. In addition, the book equips you with the necessary knowledge and techniques to successfully lower risk against emergent malware attacks. The book discusses both theoretical, technical, and practical issues related to malware attacks and defense making it an ideal reading material.

Many aspects motivated the decision toward the creation of this book. As mentioned in recent threat landscape reports, malware is on the rise again after the decrease that was noticed and linked to COVID-19. Malicious actors frequently employ malware in their campaigns. Gaining and maintaining control of assets, evading and deceiving defenses, and carrying out post-compromise actions all require this fundamental capability. The book has two clear goals. The first is to bring in front important security problems that arise in the advent of malware, and the second is to highlight

a variety of possible solution approaches that might be able to address them. Specialists and experts present their significant efforts to fulfill these goals.

This book starts with an introductory chapter about the emerging trends of cyber-malware, and then it includes nine chapters that are organized into the following three parts:

Part 1 presents solutions on Android OS malware static features extraction and detection of Android malware applications.

Part 2 contains many applications that use artificial intelligence for detecting fast flux service networks and malware.

Part 3 presents and discusses techniques that can be used for IoT and cloud malware analysis.

In Chap. 1, an effective vision-based multi-classification system for detecting various malware families in Android apps is presented. Malware in Android apps could be detected using the proposed system in visual color or grayscale formats. The tested evaluation metrics and acquired detection results performed in the chapter demonstrate that the proposed vision-based system is a promising option for Android OS malware analysis.

Based on network traffic behavior analysis, Chapter 2 proposes a novel privacy-preserving federated deep learning method that makes use of convolutional neural networks (CNN) to identify various kinds of malware. The proposed detection method is evaluated in terms of detection rate, accuracy, and performance under various federated learning settings.

The third version of the Android automatic Static Parsing tool (ASParse-V3), and its integration with other detection methods are discussed in Chap. 3 in terms of the significance of static analysis for feature extraction, dataset generation, and malware analysis systems. The results of the analysis can be fed to deep learning models and machine learning algorithms for malware analysis and detection. In addition, Android OS applications were used to demonstrate the system's capabilities.

The fast flux architecture, operation, and characterization of FFSNs are the primary topics of discussion in Chap. 4. In addition, the chapter provides a summary of fast flux detection mechanisms, highlighting the most significant difficulties and potential future research directions.

A static, graph-based approach is presented in Chap. 5 that uses machine learning to classify executable samples into malicious or benign API Call Graphs. A measure of the Abstract API Call Graph's similarity to the samples of a given dataset, which include labeled samples of malware and benign samples, is calculated by the proposed method. Additionally, it divides the similarity vector space and performs classification using the support vector machine (SVM) algorithm. Both unweighted and weighted Abstract API Call Graphs are used to evaluate the method, demonstrating high accuracy.

Chapter 6 gives a thorough survey of cutting-edge deep learning-based malware analysis and detection solutions focusing on Microsoft Windows, over the time of 2015–2022. The section gives a detailed scientific classification that classifies these solutions as per different measures including the investigation task, the analysis task, the nature of the extracted features, the used features representation method, and the used deep learning algorithms. Besides, the section talks about these solutions concerning the size and nature of the testing dataset, the performance evaluation metrics for the various tasks, and the accomplished outcomes.

Threats to the Internet of Things (IoT) and smart systems are covered in Chap. 7, as is a brief overview of malware detection and evasion techniques. For the IoT and smart systems to be utilized to their full potential, it is essential to investigate novel cyberattacks while simultaneously developing and implementing countermeasures. The objectives of this chapter are to investigate various strategies for the detection and evasion of cybersecurity threats in the IoT domain as well as evaluate security issues that are anticipated to limit IoT deployment.

In Chap. 8, a method for multiclass classification employing XG-Boost and CatBoost to classify the intrusion attack's category type is proposed. The proposed strategy aimed to develop a recent multiclass classification to classify the category type labels of IoT intrusion attacks. Precision, recall, f1-score, and G-mean were used to evaluate the experiments, which were then compared to other basic classifiers.

Malware attacks and methods for preventing malware threats in cloud computing architecture are examined in Chap. 9. Data breaches, malicious insiders, man-in-the-middle attacks, denial-of-service (DOS) and distributed denial-of-service (DDOS) attacks, cookie poisoning attacks,

and wrapping attacks are among the most frequently reported security threats, according to the study. The majority of these attacks are the result of multiple malware variants.

Riyadh, Saudi Arabia
Edinburgh, UK
Masdar City, Abu Dhabi,
United Arab Emirates
Leicester, UK

Iman AlMomani
Leandros A. Maglaras
Mohamed Amine Ferrag

Nick Ayres

INTRODUCTION: EMERGING TRENDS IN CYBER-MALWARE

Cyber-malware refers to malicious software that is designed to damage or gain unauthorized access to computer systems, networks, and data. Cyber-malware has become a significant threat to individuals, businesses, and governments worldwide, and its impact can be devastating [1].

The history of cyber-malware dates back to the 1970s when the first computer virus, known as the Creeper virus, was created as an experimental program. The Creeper virus was designed to move between computers on a network and display the message “I’m the Creeper, catch me if you can.” The first antivirus software, known as the Reaper, was then created to remove the Creeper virus from infected computers [2].

In the 1980s, as personal computers became more popular, cyber-criminals began developing malware to exploit vulnerabilities in operating systems and software. In 1986, the first computer worm, known as the Morris worm, was created by a graduate student named Robert Morris. The Morris worm caused widespread damage to computer systems and resulted in significant financial losses. This incident prompted the creation of the Computer Emergency Response Team (CERT), which provides guidance and support for organizations affected by cyber-attacks [3].

In the 1990s, cybercriminals began developing more sophisticated malware, such as Trojans and keyloggers, to steal sensitive information from individuals and businesses [4]. The first known ransomware attack, known as the AIDS Trojan, was also created in 1990. The AIDS Trojan would encrypt the victim’s files and demand payment in exchange for the decryption key.

In the 2000s, cyber-malware attacks became more prevalent, with high-profile incidents such as the ILOVEYOU virus and the Code Red worm causing significant damage to computer systems worldwide [5]. Additionally, cybercriminals began using social engineering techniques, such as phishing emails and fake websites, to trick individuals into giving up their login credentials and other sensitive information.

One of the most significant cyber-attacks involving malware in recent years was the SolarWinds attack. In December 2020, it was discovered that Russian hackers had gained access to the computer systems of several US government agencies and private companies by exploiting a vulnerability in the SolarWinds software [6]. The malware used in the attack, known as Sunburst, was a sophisticated piece of software that allowed the hackers to access sensitive information and carry out other malicious activities undetected for months.

Another recent cyber-attack involving malware was the Colonial Pipeline hack. In May 2021, a group of cybercriminals known as DarkSide used ransomware to gain access to the computer systems of Colonial Pipeline, a major US fuel pipeline operator. The attack forced the company to shut down its pipeline, causing widespread fuel shortages and price hikes across the eastern United States. The group demanded a ransom of \$4.4 million in Bitcoin, which Colonial Pipeline ultimately paid [7].

In March 2021, Microsoft announced that Chinese hackers had been using malware to target organizations around the world. The hackers were exploiting four zero-day vulnerabilities in Microsoft Exchange Server, a popular email and collaboration platform used by many businesses and organizations [8]. The hackers used the malware to steal data and carry out other malicious activities, and the attack affected thousands of organizations in at least 115 countries.

In April 2021, cybersecurity researchers discovered a new type of malware known as Silver Sparrow. Unlike many other types of malware, Silver Sparrow was designed to target Apple computers, and it was found on nearly 30,000 Macs around the world [9]. While the malware was not actively causing any harm, its presence on so many devices was a cause for concern.

In recent years, cybercriminals have continued to evolve their tactics, with the development of more sophisticated ransomware, such as the WannaCry and NotPetya attacks, and the rise of cryptojacking, which involves using the victim's computer to mine cryptocurrency without their knowledge or consent [10].

As technology continues to advance, cyber-malware attacks are likely to become even more sophisticated and difficult to detect. However, cybersecurity professionals and organizations are also developing new tools and strategies to combat cyber-malware and protect against future attacks. So, the evolution of cyber-malware has been marked by increasingly sophisticated attacks and techniques. From the early days of the Creeper virus to the modern-day threats of ransomware and cryptojacking, cyber-criminals have continuously adapted their tactics to exploit vulnerabilities in computer systems and networks [11]. However, through collaboration and innovation in cybersecurity, individuals, businesses, and governments can work to stay one step ahead of cyber-malware threats.

Individuals can become victims of cyber-malware through various means, including phishing emails, infected downloads, and social engineering attacks. Once the malware infects an individual's device, it can steal sensitive information such as login credentials, financial information, and personal data [3–5]. In some cases, cyber-malware can lock users out of their devices and demand payment for the return of access, also known as ransomware.

Businesses are at an even higher risk of cyber-malware attacks, as they often store large amounts of sensitive data that can be targeted by cybercriminals. The impact of cyber-malware on businesses can range from financial losses to reputational damage [7]. For instance, if a company's financial data is breached, it can result in significant financial losses and a loss of customer trust. Additionally, if a company's reputation is damaged due to a cyber-attack, it can lead to a decline in sales and revenue.

Governments are also vulnerable to cyber-malware attacks, as they often store classified information and sensitive data. A cyber-attack on a government's system can have severe consequences, including the theft of sensitive information, disruption of essential services, and even sabotage [9]. In some cases, cyber-malware attacks on governments have been carried out by state-sponsored hackers, leading to tensions between nations.

The impact of cyber-malware on individuals, businesses, and governments is not limited to financial losses and reputational damage. Cyber-malware attacks can also result in a loss of privacy, psychological distress, and physical harm. For instance, cyber-malware can be used to gain access to medical devices and cause harm to patients or to disrupt critical infrastructure and cause widespread power outages [8–11].

To protect against cyber-malware, individuals, businesses, and governments must take proactive measures to secure their systems and data.

This includes implementing strong passwords, keeping software up-to-date, using anti-virus software, and educating employees and users about cyber threats. Additionally, governments must work together to develop international frameworks and regulations to combat cyber-malware and hold cybercriminals accountable for their actions. Thus, cyber-malware is a growing threat to individuals, businesses, and governments worldwide [12]. The impact of cyber-malware can range from financial losses to reputational damage and can even result in physical harm. To protect against cyber-malware, it is essential to take proactive measures to secure systems and data and to work together to develop international frameworks and regulations to combat cybercrime.

Cyber-malware attacks can target a wide range of individuals, businesses, and organizations. However, certain targets are more commonly targeted by cybercriminals due to their vulnerability or potential for financial gain. Some of the common targets of cyber-malware include [13]:

- *Individuals*: Cybercriminals often target individuals with phishing emails or malware disguised as legitimate software. Individuals can be targeted for their personal information, such as login credentials, banking information, and social security numbers. Additionally, cybercriminals may use malware to gain access to an individual's computer system, allowing them to steal sensitive information or use the victim's computer for illegal activities.
- *Small businesses*: Small businesses are often targeted by cybercriminals due to their limited resources and lack of robust cybersecurity measures. Small businesses may be targeted for their financial information, customer data, or intellectual property. Ransomware attacks are also common among small businesses, as cybercriminals may demand payment in exchange for restoring access to the victim's files or computer system.
- *Large corporations*: Large corporations are also common targets of cyber-malware attacks, as they may hold valuable intellectual property or financial information. Cybercriminals may use malware to gain unauthorized access to a corporation's network or use phishing emails to trick employees into giving up sensitive information.
- *Government agencies*: Government agencies are often targeted by cybercriminals seeking sensitive information or attempting to disrupt government operations. Cyber-malware attacks on government agen-

cies can result in the theft of classified information, disruption of critical infrastructure, and other significant consequences.

- *Healthcare providers:* Healthcare providers are another common target of cyber-malware attacks, as they may hold sensitive patient information, including medical records and billing information. Cybercriminals may use malware to gain unauthorized access to a healthcare provider's network or steal patient data for identity theft or insurance fraud.

Consequently, staying up to date with new trends in cyber-malware is incredibly important in today's digital age. With the increasing number of devices and networks connected to the internet, the threat of cyber-attacks is more prevalent than ever before. Malware, short for malicious software, is designed to damage, disrupt, or gain unauthorized access to computer systems. The technology used by cybercriminals is continually evolving, and new types of malware are being developed all the time. By staying up to date with the latest trends in cyber-malware, you can ensure that you are better prepared to defend against attacks and protect your digital assets.

One of the most significant reasons to stay up to date with cyber-malware trends is to identify new threats before they become widespread. Cybercriminals often use new malware to exploit vulnerabilities in systems before antivirus software and other security measures can be updated to address the threat [14]. By being aware of new types of malware, you can take steps to protect yourself and your organization before an attack occurs.

Another reason to stay up to date with cyber-malware trends is to keep your security measures current. As new malware is developed, antivirus software and other security measures are updated to protect against them. By staying informed about new threats, you can ensure that your security measures are up-to-date and effective [15]. Failure to update your security measures can leave your devices and networks vulnerable to attack.

Additionally, staying up to date with cyber-malware trends can help you stay ahead of the competition. Cybersecurity is becoming increasingly important in today's digital landscape, and companies that fail to take it seriously may suffer reputational damage or lose customers. By demonstrating that you are aware of the latest threats and taking steps to protect your digital assets, you can build trust with your customers and gain a competitive advantage.

In conclusion, staying up to date with new trends in cyber-malware is essential to protect yourself, your organization, and your customers from

cyber-attacks. By being aware of new threats and keeping your security measures current, you can stay one step ahead of cybercriminals and avoid the potentially devastating consequences of a successful cyber-attack.

MALWARE ANALYSIS TECHNIQUES

Cyber-malware, also known as malicious software, is a type of software designed to infiltrate, damage, or disrupt computer systems, networks, and devices. Cyber-malware is often used for criminal purposes, such as stealing sensitive information or extorting money from victims.

Common Types of Cyber-Malware

There are several types of cyber-malware, including [13, 14]:

- *Virus*: A computer virus is a type of malware that infects a computer system by inserting its code into legitimate programs or documents. Once infected, the virus can replicate itself and spread to other systems, causing damage and stealing sensitive information.
- *Trojan*: A Trojan is a type of malware that disguises itself as legitimate software, often through email attachments or downloads. Once installed, the Trojan can allow cybercriminals to gain unauthorized access to the victim's computer, steal sensitive data, and even take control of the system.
- *Worm*: A worm is a self-replicating malware that spreads through networks and can cause significant damage to computer systems and networks. Worms often exploit vulnerabilities in software or operating systems, allowing cybercriminals to gain unauthorized access and steal sensitive information.
- *Ransomware*: Ransomware is a type of malware that encrypts the victim's files or computer system, rendering it unusable. The cybercriminals then demand payment, often in cryptocurrency, to provide the decryption key and restore access to the victim's data or system.
- *Adware*: Adware is a type of malware that displays unwanted or intrusive advertisements on the victim's computer system. Adware can also collect personal information, browsing history, and search queries for targeted advertising purposes.
- *Spyware*: Spyware is a type of malware that collects sensitive information, such as login credentials, browsing history, and personal data, without the victim's knowledge or consent. Cybercriminals can

then use this information for identity theft, financial fraud, or other malicious purposes.

- *Rootkit*: A rootkit is a type of malware that allows cybercriminals to gain administrative access to the victim's computer system. Rootkits often remain hidden from antivirus software and can be difficult to detect and remove, allowing cybercriminals to maintain access to the victim's system for an extended period.

To conclude, cyber-malware is a type of malicious software that can cause significant damage and disrupt computer systems, networks, and devices. There are several types of cyber-malware, including viruses, Trojans, worms, ransomware, adware, spyware, and rootkits [16, 17]. Understanding the different types of cyber-malware and taking proactive measures to protect against them is essential for individuals, businesses, and governments.

Dynamic and Static Analysis

Dynamic and static analysis are two techniques commonly used in cybersecurity to detect and analyze malware [17]. Static analysis involves examining the code of a program or file without actually executing it. This can involve using specialized tools and techniques to scan the code for known patterns or characteristics of malware. Static analysis is often used as a first step in malware analysis to quickly identify potential threats and determine whether further analysis is necessary.

Dynamic analysis, on the other hand, involves executing the program or file in a controlled environment to observe its behavior. This can involve running the program or file in a virtual machine or sandboxed environment to prevent any harm to the host system. Dynamic analysis can provide more detailed information on the behavior of malware, including its interactions with the operating system, network connections, and other processes.

Both dynamic and static analysis have their advantages and limitations [18]. Static analysis is often faster and less resource-intensive than dynamic analysis, making it a useful tool for quickly identifying potential threats. However, static analysis may not always be able to detect more advanced or sophisticated malware that is designed to evade detection.

Dynamic analysis, on the other hand, provides a more comprehensive view of the behavior of malware, which can be useful in understanding how the malware operates and identifying potential vulnerabilities in the system.

However, dynamic analysis can be more time-consuming and resource-intensive than static analysis, as it requires the execution of the malware in a controlled environment.

In practice, both dynamic and static analysis are often used in combination to provide a more comprehensive view of malware and its behavior. By using both techniques, cybersecurity professionals can quickly identify potential threats using static analysis, and then perform more detailed analysis using dynamic analysis to gain a deeper understanding of the malware's behavior and potential impact on the system [17, 18].

Malware Debugging Techniques

Malware authors are constantly evolving their techniques to evade detection and infect systems, which means that malware analysts need to constantly develop new techniques to detect and remove malware. One such technique is malware debugging [19].

Malware debugging is the process of analyzing malware by examining its code in a controlled environment. This allows analysts to identify the malware's behavior, the techniques it uses to evade detection, and the vulnerabilities it exploits. Several techniques can be used in malware debugging, including [20]:

- *Disassembly*: Disassembling the malware code is the process of converting the binary executable code into human-readable assembly code. This technique can help malware analysts to understand the behavior of the malware and identify potential vulnerabilities that it exploits.
- *Debugging tools*: Debugging tools, such as OllyDbg, IDA Pro, and WinDbg, can be used to analyze malware by allowing analysts to step through the code, set breakpoints, and view the contents of memory and registers. These tools can help to identify how the malware communicates with its command and control server, the files it creates on the infected system, and other behaviors that it exhibits.
- *Virtual machines*: Malware can be run in a virtual machine environment, such as VirtualBox or VMWare, to create a controlled environment for analysis. This technique can help to isolate the malware from the rest of the system, preventing it from infecting other files and processes on the host machine.

- *Sandboxing*: A sandbox is a virtual environment that isolates the malware from the rest of the system. This technique can help to prevent the malware from infecting other files and processes on the host machine while still allowing malware analysts to observe its behavior.
- *Dynamic analysis*: Dynamic analysis involves observing the malware as it runs in a controlled environment. This technique can help to identify the malware's behavior, such as the files it creates, the registry keys it modifies, and the network connections it establishes.
- *Code injection*: Code injection involves injecting code into the malware's process to modify its behavior or to observe its interactions with the operating system. This technique can help to identify the malware's communication with its command and control server, the data it exfiltrates, and other behaviors that it exhibits.

Identifying Malware Behavior

Identifying malware behavior is a critical step in malware analysis, as it can help security professionals to understand how a malware infection works and develop strategies for mitigating its impact. Malware behavior can include a range of activities, such as modifying system settings, stealing data, and communicating with remote servers. Here are some common techniques used to identify malware behavior [21–23]:

- *Static analysis*: This involves examining the malware code without actually running it. This can be done by examining the binary file or the source code and can help to identify the malware's behavior by looking at functions and routines used by the malware. Static analysis can also be used to identify specific strings or signatures associated with the malware.
- *Dynamic analysis*: This involves running the malware in a controlled environment to observe its behavior. This can be done in a sandbox, virtual machine, or other isolated environment. Dynamic analysis can help to identify the malware's activities, such as files it creates, registry keys it modifies, network connections it makes, and commands it sends or receives.
- *Network traffic analysis*: This involves monitoring network traffic to identify unusual activity. This can include unusual data transfers, unusual ports or protocols, and unusual server activity. Network traffic

analysis can help to identify malware that is communicating with remote servers.

- *Endpoint detection and response (EDR)*: EDR tools monitor activity on endpoints (such as desktops, servers, and mobile devices) to detect suspicious behavior. EDR tools can identify indicators of compromise (IoCs), such as suspicious processes, changes to the registry or file system, and attempts to bypass security controls.
- *Reverse engineering*: This involves decompiling or disassembling the malware code to identify its behavior. Reverse engineering can help to identify how the malware communicates with its command and control server, how it encrypts or decrypts data, and how it modifies system settings.
- *Memory analysis*: This involves examining the contents of the computer's memory to identify malware behavior. Memory analysis can help to identify malware that has been loaded into memory and identify any unusual processes or network connections.
- *Behavioral analysis*: This involves observing the malware's behavior in a virtual environment to identify any unusual or malicious activity. Behavioral analysis can help to identify the specific behavior of the malware, which can be used to develop targeted mitigation strategies.

In conclusion, identifying malware behavior is an important step in malware analysis. It involves using a combination of techniques, such as static analysis, dynamic analysis, network traffic analysis, endpoint detection and response, reverse engineering, memory analysis, and behavioral analysis, to identify the malware's activities and develop strategies for mitigating its impact [24]. By understanding the behavior of malware, security professionals can better protect their systems and networks against malware infections.

MALWARE DISTRIBUTION METHODS

Malware distribution methods refer to the various ways in which malicious software is disseminated to infect systems and devices. Malware can take many forms, including viruses, worms, Trojans, ransomware, and spyware, among others. Malware authors often use multiple distribution methods to increase the likelihood of infecting as many devices as possible. The most common malware distribution methods are as follows [25, 26]:

- *Email Attachments*: Malware authors use emails to distribute malware by attaching malicious files to emails. The recipient is tricked into downloading and opening the attachment, which infects their system. The attachments may appear as legitimate files, such as a PDF or a Word document, but once opened, the malware executes on the system.
- *Social Engineering*: Social engineering involves tricking users into downloading or installing malware by using psychological manipulation techniques. For example, attackers may use a fake website to convince users to download an application that is malware. Social engineering may also involve using fake antivirus alerts or fake software updates to trick users into installing malware.
- *Drive-By Downloads*: Drive-by downloads involve malware being installed on a user's computer without their knowledge or consent when they visit a website. This is typically accomplished by exploiting vulnerabilities in the user's web browser or other software.
- *Malvertising*: Malvertising is the distribution of malware through online advertisements. Attackers use legitimate-looking advertisements to lure users into clicking on them, which then leads to the installation of malware on the user's computer.
- *Infected Software*: Malware authors sometimes distribute infected software or applications that appear legitimate but are infected with malware. Once the software is downloaded and installed, the malware executes on the system.
- *USB Drives*: Malware can also be distributed through USB drives that are infected with malware. When the USB drive is inserted into a computer, the malware automatically executes on the system.
- *Watering Hole Attacks*: In a watering hole attack, attackers infect a website that is frequently visited by their target audience. The attackers then wait for their targets to visit the infected website, where they are infected with malware.
- *Phishing*: This method involves sending emails or messages that appear to be from a trusted source but contain links to malicious websites or attachments that download malware onto the victim's computer.
- *Software vulnerabilities*: Cybercriminals can exploit vulnerabilities in legitimate software applications to install malware onto a victim's computer.

- *Malicious websites:* Cybercriminals can create malicious websites that contain malware. These websites may look legitimate, but they are designed to infect visitors' computers with malware. In some cases, simply visiting the website is enough to download the malware.
- *Social media:* Cybercriminals can use social media platforms to distribute malware. They may create fake profiles or pages that appear to be legitimate but contain links to infected websites or downloads.
- *File sharing networks:* Some malware is distributed through peer-to-peer (P2P) file-sharing networks. Cybercriminals may upload infected files, such as movies or music, and entice users to download them.
- *Mobile devices:* Malware can also be distributed through mobile devices, such as smartphones and tablets. Cybercriminals may create fake apps that contain malware or send infected links through text messages or social media.

Thus, malware distribution methods are constantly evolving, and attackers are becoming more sophisticated in their techniques. It is essential to remain vigilant when opening emails, downloading software, or visiting websites to avoid falling victim to malware. Keep your software updated, use reputable antivirus software, and be cautious of suspicious emails and websites. So, to protect against these malware distribution methods, it's important to keep software up to date, use antivirus software, be cautious when opening email attachments or clicking on links, and avoid downloading software from untrusted sources.

MALWARE PREVENTION AND MITIGATION STRATEGIES

Malware prevention and mitigation strategies are essential in today's digital age, where malware threats are prevalent and continue to evolve. Prevention and mitigation strategies are measures put in place to reduce the likelihood and severity of potential hazards, disasters, or crises. These strategies aim to prevent or mitigate the negative impact of these events on individuals, communities, and the environment [27].

Prevention strategies involve taking measures to prevent an event from occurring. These strategies can include implementing safety measures, such as using protective equipment, conducting safety training, or installing safety features in buildings or equipment. Preventive strategies can also involve enforcing regulations or laws to deter risky behaviors or practices.

Mitigation strategies involve taking steps to reduce the impact of an event that has already occurred. These strategies can include emergency

response plans, such as evacuation plans, first aid procedures, and disaster relief efforts. Mitigation strategies can also involve restoration efforts, such as rebuilding infrastructure or rehabilitating natural habitats [28].

Effective prevention and mitigation strategies are essential for reducing the impact of disasters and crises. By taking proactive steps to prevent events from occurring or mitigating their effects, we can reduce the risk of harm and save lives [29]. Additionally, these strategies can also help reduce the economic and environmental impact of disasters, making recovery and restoration efforts more manageable.

Examples of prevention and mitigation strategies include [27–29]:

- *Hazard assessments*: Conduct regular assessments to identify potential hazards and develop appropriate prevention and mitigation strategies.
- *Early warning systems*: Implement systems that provide early warning of potential hazards, such as natural disasters or industrial accidents, to allow for timely response and mitigation.
- *Infrastructure improvement*: Upgrade and maintain infrastructure, such as roads, bridges, and buildings, to make them more resilient to disasters.
- *Community education and outreach*: Educate communities about potential hazards, how to prepare for disasters, and what to do in case of emergency.
- *Disaster response planning*: Develop comprehensive plans for responding to disasters and crises, including evacuation plans, emergency communication systems, and disaster relief efforts.
- *Environmental protection measures*: Implement measures to protect the environment, such as reducing pollution and conserving natural resources, to prevent or mitigate the impact of disasters.
- *Risk assessments*: Conduct regular assessments to identify potential hazards and develop appropriate prevention and mitigation strategies.
- *Use Antivirus Software*: Install and regularly update a reputable antivirus software program on your computer or device. Antivirus software can help detect and remove malware from your system.
- *Keep Software Up-to-date*: Keep your operating system, web browser, and other software applications up-to-date with the latest security patches and updates. Cybercriminals often exploit vulnerabilities in outdated software.
- *Use Strong Passwords*: Use strong, unique passwords for all your accounts and avoid using the same password across multiple accounts.

Consider using a password manager to generate and store complex passwords.

- *Be Cautious of Email Attachments:* Do not open email attachments or click on links from unknown or suspicious sources. Malware can be spread through email attachments and links.
- *Enable Two-Factor Authentication:* Enable two-factor authentication (2FA) whenever possible. This adds an extra layer of security to your accounts by requiring a second form of authentication, such as a code sent to your mobile device.
- *Back Up Your Data:* Regularly back up your data to an external hard drive or cloud storage service. This can help mitigate the impact of malware if your system is infected.
- *Educate Yourself:* Stay informed about the latest threats and best practices for preventing and mitigating malware. Learn how to recognize and avoid phishing scams, and be cautious when downloading and installing software from the Internet.

FUTURE OF CYBER-MALWARE

The future of cyber-malware is a topic of concern for cybersecurity professionals and businesses worldwide. As technology continues to evolve and become more complex, so do the threats posed by cyber-malware. One trend that is likely to continue in the future is the use of artificial intelligence (AI) by cybercriminals to develop more sophisticated and effective malware. AI-powered malware can adapt to its environment, evade detection, and target specific vulnerabilities in a network or system. This type of malware can also learn from its actions and adjust its behavior accordingly, making it more difficult to stop.

Another potential development in cyber-malware is the increased use of ransomware attacks. Ransomware is a type of malware that encrypts a victim's files or data and demands payment in exchange for the decryption key. This type of attack has become increasingly common in recent years and is likely to continue in the future, as it can be highly profitable for attackers. In fact, some experts predict that ransomware attacks may become more targeted, with attackers focusing on specific industries or organizations with high-value data.

The Internet of Things (IoT) is another area of concern when it comes to the future of cyber-malware. IoT devices are often connected to the internet and can be vulnerable to attacks, as they may not have strong

security protocols in place. As the number of IoT devices continues to grow, so does the potential for cyber-attacks targeting them. This could lead to large-scale disruptions, such as attacks on critical infrastructure or widespread data breaches.

Finally, there is a growing concern about the use of nation-state-sponsored cyber-malware attacks. Governments may use cyber-malware to gain access to sensitive information, disrupt rival countries' infrastructure, or carry out espionage activities. These attacks can be difficult to trace and may have significant political and economic consequences.

So, the future of cyber-malware is likely to be characterized by increasingly sophisticated and targeted attacks. As technology continues to advance, so do the threats posed by cybercriminals. To mitigate these risks, businesses and individuals must remain vigilant and take steps to protect their networks, devices, and data. This includes implementing strong security protocols, keeping software up-to-date, and educating users about the risks of cyber-malware.

Trends and Predictions for Future Malware Development

Malware, or malicious software, has been a persistent threat to computer systems and networks since the dawn of the internet. Cybercriminals constantly seek out new ways to exploit vulnerabilities in software and hardware to gain unauthorized access to sensitive data or control systems for nefarious purposes. In recent years, malware development has become more sophisticated, and new trends are emerging that could shape the future of cybercrime [30]. Here are some predictions for trends in malware development in the near future [31].

- *Fileless malware:* Fileless malware attacks are on the rise, and this trend is likely to continue in the coming years. Fileless malware, also known as memory-resident malware, operates entirely in a computer's memory and leaves no trace on the system's hard drive. This makes it difficult to detect and remove, as traditional antivirus software relies on scanning files on a hard drive. As more businesses adopt cloud-based computing and mobile devices become more prevalent, fileless malware is likely to become a more significant threat.
- *Malware as a service:* Malware as a service (MaaS) is a growing trend in the cybercriminal underground. Just like software as a service (SaaS), MaaS allows cybercriminals to rent or purchase malware

from a third-party provider. This lowers the barrier to entry for less technically savvy criminals, who can now launch sophisticated attacks without having to develop their own malware. As MaaS becomes more prevalent, we can expect to see more varied and sophisticated malware being developed and deployed.

- *Advanced evasion techniques:* As cybersecurity defenses become more sophisticated, malware developers are turning to advanced evasion techniques to avoid detection. These techniques include using encryption to hide malicious code, exploiting vulnerabilities in antivirus software, and creating polymorphic malware that can change its code to evade detection. As evasion techniques become more sophisticated, it will become increasingly difficult to detect and prevent malware attacks.
- *Targeted attacks:* Rather than launching mass attacks, cybercriminals are increasingly targeting specific individuals or organizations. This allows them to conduct more sophisticated attacks, such as spear-phishing, that are tailored to the victim's interests or behaviors. As more data becomes available on individuals and organizations, we can expect to see more targeted attacks that leverage this information to bypass defenses and gain access to sensitive data.
- *IoT malware:* With the rise of the Internet of Things (IoT), there is a growing concern about the security of these devices. IoT devices are often not designed with security in mind and can be easily hacked, giving cybercriminals access to sensitive data or control over critical infrastructure. As the number of IoT devices continues to grow, we can expect to see more malware specifically designed to target these devices.
- *Machine Learning-Based Malware:* Machine learning has become a powerful tool for cybersecurity, and malware developers are no exception. By using machine learning algorithms, malware can adapt to its environment and learn how to evade detection.
- *Deepfakes:* Deepfakes are videos or images that have been manipulated using artificial intelligence to make them appear real. In the future, we can expect to see more malware that uses deepfakes to trick users into downloading or installing malicious software.
- *Mobile Malware:* With the increasing use of mobile devices, mobile malware has become a growing concern. In the future, we can expect to see more mobile-specific malware that can steal sensitive data or take control of the device.

Consequently, malware development is constantly evolving, and new trends and techniques are emerging all the time. As cybersecurity defenses become more sophisticated, cybercriminals will continue to find new ways to bypass them. Individuals and organizations need to stay informed about the latest trends in malware development and take appropriate measures to protect their systems and data.

Emerging Threats and Attack Vectors

As the digital landscape continues to evolve, so do the threats and attack vectors that cybercriminals use to compromise systems and steal data. Here are some emerging threats and attack vectors to be aware of [30, 31]:

- *Supply Chain Attacks:* Supply chain attacks involve targeting a third-party vendor that supplies software or hardware components to a larger organization. The attackers compromise the vendor's systems, injecting malware into the products or services that the vendor provides. When the larger organization installs or uses the compromised product or service, the malware spreads to their systems, giving the attackers access to sensitive data.
- *Zero-Day Exploits:* Zero-day exploits are vulnerabilities in software or hardware that are unknown to the vendor or manufacturer. Attackers exploit these vulnerabilities before the vendor can patch them, giving them access to the affected systems. Zero-day exploits are particularly dangerous because there are no known defenses against them.
- *Phishing:* Phishing attacks are social engineering attacks that attempt to trick users into revealing sensitive information or installing malware. Phishing attacks can take many forms, including emails, text messages, or phone calls. These attacks are becoming increasingly sophisticated, using tactics such as personalized messaging and spoofing trusted sources.
- *Ransomware:* This is a type of malware that encrypts an organization's data and demands payment in exchange for the decryption key. Ransomware attacks are becoming increasingly common and can cause significant disruption and financial losses.
- *Social engineering:* Social engineering attacks involve tricking individuals into divulging sensitive information or performing an action that compromises the security of an organization. Common techniques include phishing emails and pretexting.

- *Machine learning attacks:* Machine learning algorithms are vulnerable to attack, which can lead to inaccurate predictions or even malicious behavior. Adversarial attacks, where an attacker deliberately modifies data to trick the algorithm, are becoming increasingly common.
- *Insider threats:* Insider threats can be intentional or unintentional, but they can cause significant damage to an organization's security. Organizations need to implement policies and procedures to detect and prevent insider threats.
- *AI-Powered Attacks:* As artificial intelligence (AI) becomes more prevalent in cybersecurity, attackers are using AI-powered tools to automate attacks. AI can be used to automate phishing attacks, identify vulnerabilities, and evade detection by security measures.
- *Cloud-Based Attacks:* Cloud computing has become a popular choice for businesses, but it has also created new attack vectors for cybercriminals. Cloud-based attacks can include exploiting vulnerabilities in cloud infrastructure, stealing login credentials, or compromising data stored in the cloud.
- *Internet of Things (IoT) Attacks:* IoT devices, such as smart home devices and industrial control systems, are becoming more prevalent in our lives. However, these devices often have weak security measures and are vulnerable to attack. Attackers can use IoT devices to launch attacks, such as Distributed Denial of Service (DDoS) attacks, or to steal sensitive data.

Therefore, as technology continues to advance, cybercriminals will continue to find new and more sophisticated ways to compromise systems and steal data. It is important to stay informed about emerging threats and attack vectors and take proactive measures to protect our systems and data. This includes regularly updating software, using strong passwords, and implementing multi-factor authentication.

The Role of Artificial Intelligence in Malware Development and Detection

Artificial intelligence (AI) is playing an increasingly important role in both malware development and detection. On the one hand, AI can be used to create more sophisticated and effective malware, while on the other hand, it can also be used to develop more advanced detection and prevention techniques [32].

One of how AI is being used in malware development is through the use of machine learning algorithms. By training these algorithms on large datasets of existing malware, researchers can develop new malware that is specifically designed to evade existing detection methods. Machine learning can also be used to create more sophisticated attack strategies, such as spear-phishing campaigns that are tailored to individual victims.

However, AI is also being used to develop new and more effective methods for detecting and preventing malware. For example, AI can be used to analyze network traffic and identify patterns of behavior that are indicative of a malware infection. Similarly, machine learning algorithms can be trained to identify specific features of malware code, making it possible to detect and block new malware strains as they emerge.

Another area where AI is having a significant impact on malware detection is in the development of so-called “next-generation” antivirus (NGAV) solutions. These solutions use a combination of machine learning algorithms and behavioral analysis techniques to detect and block malware in real time, even if it has never been seen before. NGAV solutions can also be used to identify and block previously unknown attack vectors, such as zero-day exploits, that traditional antivirus solutions are unable to detect [33].

Here are some of the new research trends for the role of AI in malware development and detection [32, 33]:

- *Adversarial machine learning*: Adversarial machine learning is a technique where an attacker deliberately modifies data to trick the machine learning algorithm into making a wrong prediction. In the context of malware detection, attackers can use this technique to evade detection by creating malware that appears benign to machine learning algorithms. New research is exploring how to develop machine learning algorithms that are more resilient to adversarial attacks.
- *Explainable AI*: Explainable AI is a technique that enables humans to understand how a machine learning algorithm is making its predictions. In the context of malware detection, explainable AI can help security analysts understand how a particular malware was detected and what features of the malware triggered the detection. This can help security analysts develop more effective detection strategies.
- *Deep learning*: Deep learning is a subfield of machine learning that involves training deep neural networks with multiple layers. New research is exploring how deep learning can be used to detect malware

by analyzing its behavior. For example, deep learning can be used to analyze network traffic and identify patterns of behavior that are indicative of a malware infection.

- *Reinforcement learning*: Reinforcement learning is a type of machine learning where an algorithm learns to make decisions by interacting with an environment. In the context of malware detection, reinforcement learning can be used to train an algorithm to make decisions about whether a particular file is malware or not based on feedback from the environment.
- *Generative adversarial networks (GANs)*: GANs are a type of deep learning algorithm that consists of two neural networks that compete against each other. One network generates samples, while the other network tries to distinguish between real and fake samples. In the context of malware detection, GANs can be used to generate synthetic malware samples that can be used to train machine learning algorithms.
- *Transfer learning*: Transfer learning is a technique that involves training a machine learning algorithm on one task and then transferring that knowledge to another task. In the context of malware detection, transfer learning can be used to train a machine learning algorithm on a large dataset of non-malicious software and then transfer that knowledge to detect malware.

In conclusion, while AI is being used to create more sophisticated and effective malware, it is also playing an important role in the development of new and more advanced malware detection and prevention techniques. As the threat landscape continues to evolve, AI will likely play an increasingly important role in both offensive and defensive cybersecurity strategies.

CONCLUSIONS AND FUTURE WORK

This chapter highlighted some of the latest trends and challenges in the field of malware detection and prevention. One of the key takeaways from this chapter is the increasing sophistication and complexity of malware attacks. Malware developers are becoming more adept at evading detection and are using more advanced techniques like artificial intelligence and machine learning to develop new strains of malware. As a result, traditional malware detection methods are becoming less effective. To combat this evolving threat landscape, researchers are exploring new approaches to malware detection and prevention. These include the use of artificial

intelligence and machine learning algorithms to analyze network traffic and identify patterns of behavior that are indicative of a malware infection. Next-generation antivirus solutions that use a combination of machine learning and behavioral analysis techniques are also emerging as an important defense against malware attacks.

Another important trend highlighted in this chapter is the increasing importance of collaboration between industry, academia, and government in the fight against cyber-malware. By working together and sharing information, researchers and cybersecurity professionals can stay ahead of emerging threats and develop more effective countermeasures. Looking to the future, the chapter concludes by suggesting that the field of malware detection and prevention will continue to evolve rapidly. New techniques and approaches will be developed to combat increasingly sophisticated attacks, and the role of artificial intelligence and machine learning in this field will continue to grow. In addition, the rise of the IoT is expected to introduce new challenges for malware detection and prevention, as these devices often lack the security features of traditional computers and servers.

In conclusion, this chapter provided a valuable overview of the latest trends and challenges in the field of malware detection and prevention. By staying abreast of these trends and developing new and innovative solutions, cybersecurity professionals can help to protect individuals, businesses, and organizations against the growing threat of cyber-malware.

Security Engineering Lab, Computer
Science Department
Prince Sultan University, Riyadh,
Saudi Arabia
Electronics and Electrical Communication
Engineering Department, Faculty of
Electronic Engineering
Menoufia University, Menouf, Egypt
e-mail: welshafai@psu.edu.sa;
walid.elshafai@el-eng.menofia.edu.eg

Walid El-Shafai

Security Engineering Lab,
 Prince Sultan University, Riyadh,
 Saudi Arabia
 Computer Science Department,
 The University of Jordan, Amman, Jordan
 e-mail: imomani@psu.edu.sa;
i.momani@ju.edu.jo
 School of Computing
 Edinburgh Napier University, Edinburgh,
 UK
 e-mail: l.maglaras@napier.ac.uk

Iman Almomani

Leandros A. Maglaras

REFERENCES

1. Aziz S, Irshad M, Haider SA, Wu J, Deng DN, Ahmad S (2022) Protection of a smart grid with the detection of cyber-malware attacks using efficient and novel machine learning models. *Front Energy Res* 10:1102
2. Choi KS, Lee CS, Merizalde J (2023) Spreading viruses and malicious codes. In: *Handbook on crime and technology*. Edward Elgar Publishing, Florida, United States, pp 232–250
3. Riebe T, Kaufhold MA, Reuter C (2021) The impact of organizational structure and technology use on collaborative practices in computer emergency response teams: an empirical study. *Proc ACM Hum-Comput Interact* 5(CSCW2):1–30
4. Gazet A (2010) Comparative analysis of various ransomware virii. *J Comput Virol* 6:77–90
5. Bridges L (2008) The changing face of malware. *Netw Secur* 2008(1):17–20
6. Alkhadra R, Abuzaid J, AlShammari M, Mohammad N (2021) Solar winds hack: in-depth analysis and countermeasures. In: *2021 12th international conference on computing communication and networking technologies (ICCCNT)*. IEEE, Kharagpur, India, pp 1–7

7. Danisevskis J, Piekarska M, Seifert JP (2014) Dark side of the shader: mobile gpu-aided malware delivery. In: Information security and cryptology–ICISC 2013: 16th international conference, Seoul, Korea, November 27–29, 2013, Revised Selected Papers 16. Springer International Publishing, Seoul, Korea, pp 483–495
8. Singh UK, Joshi C, Kanellopoulos D (2019) A framework for zero-day vulnerabilities detection and prioritization. *J Inf Secur Appl* 46:164–172
9. Kumar R, Bawa SR (1979) Hepatic silver binding protein (Ag BP) from sparrow (*Passer domesticus*). *Experientia* 35:1621–1623
10. Lika RA, Murugiah D, Brohi SN, Ramasamy D (2018) NotPetya: cyber attack prevention through awareness via gamification. In: 2018 International conference on smart computing and electronic enterprise (ICSCEE). IEEE, Shah Alam, Malaysia, pp 1–6
11. Warmesley D, Waagen A, Xu J, Liu Z, Tong H (2022) A survey of explainable graph neural networks for cyber malware analysis. In: 2022 IEEE international conference on big data (big data). IEEE, Osaka, Japan, pp 2932–2939
12. Eboibi FE (2017) A review of the legal and regulatory frameworks of Nigerian Cybercrimes Act 2015. *Comput Law Secur Rev* 33(5):700–717
13. Wu M, Moon YB (2017) Taxonomy of cross-domain attacks on cybermanufacturing system. *Procedia Comput Sci* 114:367–374
14. Patel P, Kannoorpatti K, Shanmugam B, Azam S, Yeo KC (2017) A theoretical review of social media usage by cyber-criminals. In: 2017 International conference on computer communication and informatics (ICCCI). IEEE, Coimbatore, India, pp 1–6
15. Rogers MK (2011) The psyche of cybercriminals: a psycho-social perspective. In: *Cybercrimes: a multidisciplinary analysis*, Springer, Singapore, pp 217–235
16. Almomani I, Ahmed M, El-Shafai W (2022) Android malware analysis in a nutshell. *PloS One* 17(7):e0270647
17. Almomani I, AlKhayer A, El-Shafai W (2022) An automated vision-based deep learning model for efficient detection of android malware attacks. *IEEE Access* 10:2700–2720
18. El-Shafai W, Almomani I, AlKhayer A (2021) Visualized malware multi-classification framework using fine-tuned CNN-based transfer learning models. *Appl Sci* 11(14):6446

19. Afanian A, Niksefat S, Sadeghiyan B, Baptiste D (2019) Malware dynamic analysis evasion techniques: a survey. *ACM Comput Surv (CSUR)* 52(6):1–28
20. Chen P, Huygens C, Desmet L, Joosen W (2016) Advanced or not? A comparative study of the use of anti-debugging and anti-VM techniques in generic and targeted malware. In: *ICT systems security and privacy protection: 31st IFIP TC 11 international conference, SEC 2016, Ghent, Belgium, May 30–June 1, 2016, Proceedings* 31. Springer International Publishing, Ghent, Belgium, pp 323–336
21. Yu B, Fang Y, Yang Q, Tang Y, Liu L (2018) A survey of malware behavior description and analysis. *Front Inf Technol Electron Eng* 19:583–603
22. Shaid SZM, Maarof MA (2014) Malware behavior image for malware variant identification. In: *2014 International symposium on biometrics and security technologies (ISBAST)*. IEEE, Kuala Lumpur, Malaysia, pp 238–243
23. Almomani I, Alkhayer A, El-Shafai W (2022) A cryptosteganography approach for hiding ransomware within hevc streams in android iot devices. *Sensors* 22(6):2281
24. Almomani I, AlKhayer A, El-Shafai W (2021) Novel ransomware hiding model using HEVC steganography approach. *Comput Mater Contin* 70(2):1209–1228
25. Choi SY, Lim CG, Kim YM (2019) Automated link tracing for classification of malicious websites in malware distribution networks. *J Inf Process Syst* 15(1):100–115
26. Kim D (2019) Potential risk analysis method for malware distribution networks. *IEEE Access* 7:185157–185167
27. Rudd EM, Rozsa A, Günther M, Boulton TE (2016) A survey of stealth malware attacks, mitigation measures, and steps toward autonomous open world solutions. *IEEE Commun Surv Tutorials* 19(2):1145–1172
28. Kapoor A, Gupta A, Gupta R, Tanwar S, Sharma G, Davidson IE (2021) Ransomware detection, avoidance, and mitigation scheme: a review and future directions. *Sustainability* 14(1):8
29. Djenna A, Bouridane A, Rubab S, Marou IM (2023) Artificial intelligence-based malware detection, analysis, and mitigation. *Symmetry* 15(3):677

30. Gazzan M, Sheldon FT (2023) Opportunities for early detection and prediction of ransomware attacks against industrial control systems. *Future Internet* 15(4):144
31. Gorment NZ, Selamat A, Cheng LK, Krejcar O (2023) Machine learning algorithm for malware detection: taxonomy, current challenges and future directions. *IEEE Access*, 11:1–50
32. Samtani S, Zhao Z, Krishnan R (2023) Secure knowledge management and cybersecurity in the era of artificial intelligence. *Inf Syst Front* 25(2):425–429
33. Akhtar MS, Feng T (2023) Evaluation of machine learning algorithms for malware detection. *Sensors* 23(2):946

CONTENTS

Introduction: Emerging Trends in Cyber-Malware	ix
1 A Deep-Vision-Based Multi-class Classification System of Android Malware Apps	1
Iman Almomani, Walid El-Shafai, Mohammed Ahmed, Sara AlAnsary, Ghada AlMudahi, and Lama AlSwayeh	
2 Android Malware Detection Based on Network Analysis and Federated Learning	23
Djallel Hamouda, Mohamed Amine Ferrag, Nadjette Benhamida, Zine Eddine Kouahla, and Hamid Seridi	
3 ASParseV3: Auto-Static Parser and Customizable Visualizer	41
Iman Almomani, Rahaf Alkhadra, and Mohammed Ahmed	
4 Fast-Flux Service Networks: Architecture, Characteristics, and Detection Mechanisms	63
Basheer Al-Duwairi and Ahmed S. Shatnawi	
5 Efficient Graph-Based Malware Detection Using Minimized Kernel and SVM	91
Billy Tsouvalas and Dimitrios Serpanos	

6	Deep Learning for Windows Malware Analysis	119
	Mohamed Belaoued, Abdelouahid Derhab, Nassira Chekkai, Chikh Ramdane, Noureddine Seddari, Abdelghani Bouras, and Zahia Guessoum	
7	Malware Analysis for IoT and Smart AI-Based Applications	165
	Syed Emad ud Din Arshad, Moustafa M. Nasralla, Sohaib Bin Altaf Khattak, Taqwa Ahmed Alhaj and Ikram ur Rehman	
8	A Multiclass Classification Approach for IoT Intrusion Detection Based on Feature Selection and Oversampling	197
	Zayna Amierh, Lina Hammad, Raneem Qaddoura, Huthaifa Al-Omari, and Hossam Faris	
9	Malware Mitigation in Cloud Computing Architecture	235
	Sai Kumar Medaram and Leandros Maglaras	
	Index	279