A Detailed Review For Malicious Software Threat

1. Abstract

Malicious software, or malware, represents a significant threat to digital security, with various types causing widespread harm. This review document examines the harmful effects of malware, identifies the most common types, and explores the primary methods of malware propagation. Recognizing the critical signs of malware infection is essential for timely intervention. Techniques such as injecting malware with binders and hiding it from antivirus programs demonstrate the sophistication of modern threats. The role of antivirus software in malware detection and protection is discussed, emphasizing the need for advanced methods to uncover hidden malware. This study aims to provide a comprehensive overview of malware threats and effective countermeasures, contributing to enhanced cybersecurity practices.

Keywords: Malicious software threat, harmful effects of malwares, malware types, spreading malwares, signs of malware infection, injecting malwares with binders, hiding malwares from anti virus programs, antivirus softwares, protection from malware, detection of hidden malware.

2. Introduction

2.1 Problem Definition

In the realm of digital security, malicious software, or malware, poses a significant and evolving threat. The diverse range of malware types, including viruses, worms, Trojans, ransomware, and spyware, can cause extensive harm to individuals, organizations, and systems. The sophistication of modern malware has escalated, with advanced techniques such as injecting malware with binders and concealing it from antivirus programs complicating detection and mitigation efforts. This problem is exacerbated by the myriad methods of malware propagation, including phishing, drive-by downloads, and social engineering, which facilitate widespread infection. Recognizing the critical signs of a malware infection early is paramount for effective intervention and damage control.

Current antivirus solutions, while essential, often struggle to keep pace with the rapidly evolving landscape of malware threats. Traditional detection methods can be inadequate against malware that employs obfuscation and polymorphic techniques to evade detection. Therefore, there is an urgent need for advanced detection and protection mechanisms that can effectively uncover and neutralize hidden malware. This study seeks to address these challenges by providing a thorough examination of the harmful effects of malware, analyzing the most prevalent types and propagation methods, and exploring advanced strategies for malware detection and protection. By doing so, it aims to enhance cybersecurity practices and fortify defenses against the pervasive threat of malware.

2.2 Definition and History of Malicious Software

Malicious software, commonly known as malware, is any software intentionally designed to cause damage to a computer, server, client, or computer network. It can take various forms, including viruses, worms, Trojans, ransomware, spyware, adware, and more. Malware can disrupt operations, steal sensitive information, or gain unauthorized access to systems. Understanding the types and behaviors of malware is crucial for implementing effective security measures. [1]

The evolution of malware began in the 1980s with Elk Cloner, the first large-scale virus, spreading via floppy disks on Apple II systems. The 1990s saw a surge in viruses targeting Microsoft Windows, especially through macro viruses in Word documents. From 2002 to 2007, IM worms spread through messaging platforms like AOL AIM and MSN Messenger, often using social engineering tactics.

Adware attacks proliferated from 2005 to 2009, while social networks became malware vectors around 2007. Ransomware emerged in 2013 with CryptoLocker and surged until 2017. Cryptojacking appeared in 2017, followed by a resurgence of ransomware targeting businesses from 2018 to 2019, with attacks increasing by 365%. [1]

2.3 Harmful Effects of Malwares

The impact of malware infections varies. For home users, minor infections might result in the loss of unimportant information, while severe infections could lead to financial loss through access to bank accounts. On corporate networks, minor infections might increase communication traffic, but severe infections could cause network breakdowns or loss of critical business data, leading to significant financial and operational disruptions. [2] Malware attacks are a significant threat to individuals, businesses, and even governments. These attacks can be summarized as below [3]:

• **Unauthorized Access:** Exploiting weak passwords and infiltrating systems deeply, makes detection and removing challenging.
• **Network and System Disruption:** Spreading across networks, infecting multiple devices, disrupting daily operations, and causing downtime.
• **Data Breaches and Theft:** Leading to identity theft and frauding by stealing data, which can be sold on the dark web or used for corporate espionage.
• **File Encryption and Ransomware:** Locking important files and demanding payment for their release, causing significant financial damage.
• **Ad Spam and Redirects:** Degrading system performance by spamming users with ads and redirecting them to malicious websites.
• **Cyberwarfare and Espionage:** Used by governments against other countries or corporations to stealing secrets and conducting sabotage.
• **Extortion and Financial Exploitation:** Demanding ransom for decryption keys or use ransomware-as-a-service models for profit.
• **Cryptocurrency Mining:** Using victims' computers to mine cryptocurrencies without their consent.
• **Botnets and DDoS Attacks:** Creating botnets to overload servers, causing service disruptions.

Figure-1: Live Cyberthreat Map Which Shows Current BotNet Attacks [4]

2.4 Most Common Malware Types (Their Unique Characteristics and Behaviours)

• **Router Viruses:** Router viruses infect Wi-Fi routers, redirecting users to malicious websites that capture personal data. These infections can be challenging to remove and pose significant risks by compromising the network's security.

• **Trojans:** Trojans disguise themselves as legitimate software or hide within tampered software, sneaking onto devices to install additional malware. They are often used to steal financial information, gain unauthorized access, or install ransomware, making them one of the most dangerous types of malware.

• **Spyware:** Spyware secretly monitors user activities, collecting data such as passwords, GPS location, and financial information. It hides in the background and sends the gathered information to attackers, but it is usually straightforward to remove from systems.

• **Keyloggers:** Keyloggers are a type of spyware that records all keystrokes on a device. They capture sensitive information like login credentials and credit card numbers, posing a significant threat to personal and financial security.

• **Ransomware:** Ransomware locks up computers and files, demanding a ransom for their release. It is one of the most pressing malware threats today, causing downtime, data breaches, and significant financial losses for individuals and organizations.

• **Worms:** Worms are self-replicating malware that spread across networks without needing a host file. They can cause significant disruptions by consuming bandwidth and infecting numerous systems rapidly, as seen in the WannaCry ransomware outbreak.

• **Adware:** Adware bombards users with ads to generate revenue for attackers. While it undermines security by serving ads, it can also pave the way for other malware to enter the system. Adware is often bundled with legitimate software to trick users into installation.

• **Botnets:** Botnets are networks of infected computers controlled by attackers, often used for DDoS attacks, spamming, or spreading malware. They consist of "zombie" computers working together to carry out large-scale cyber attacks.

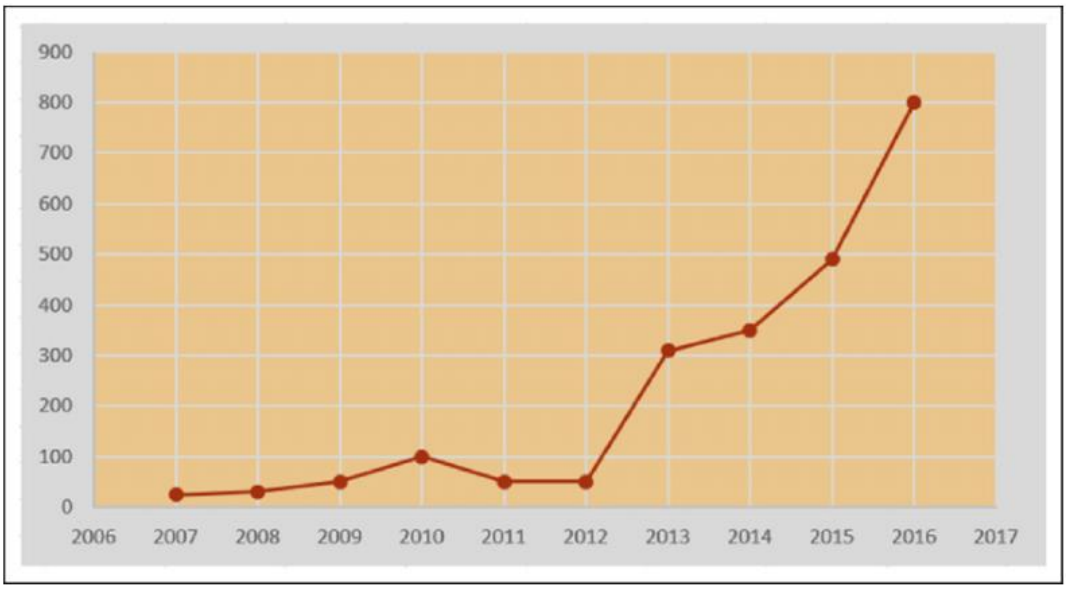

Figure-2: The Volume Sizes of DDoS Attacks In Gigabits Per Second (2007-2016) [7]

• **Rootkits:** Rootkits provide attackers with deep, hidden access to systems, often evading detection by antivirus software. They give hackers full administrative privileges, making them extremely difficult to remove without specialized tools.

• **Macro Viruses:** Macro viruses exploit macros in Microsoft Office applications like Word and Excel to infect devices. They can spread through documents, executing malicious code when the infected document is opened, often leading to data corruption or unauthorized access.

• **Scareware:** Scareware uses fake pop-ups to frighten users into downloading malicious "security" software. It tricks users by warning them of nonexistent threats, leading to unnecessary and potentially harmful software installations.

• **Browser Hijackers:** Browser hijackers modify web browser settings without user consent, redirecting to harmful websites or displaying excessive ads. While often simple to remove, they can compromise user security and privacy.

• **Cryptominers:** Cryptominer malware hijacks a computer's processing power to mine cryptocurrency for attackers. This type of malware often uses browser hijacking techniques, draining system resources and potentially causing significant performance issues.

• **Logic Bombs:** Logic bombs are malicious code designed to activate under specific conditions or at a certain time. They can cause significant damage by executing destructive actions when triggered, often lying dormant until the right moment.

Each of these malware types poses unique threats to computer systems and user data, emphasizing the need for robust cybersecurity measures and awareness. [1] [3] [5] [6]

Very Important Note: It is undeniable that data can be collected, processed, and used for various purposes even without malware. The best example of this is the Cambridge Analytica scandal that erupted in 2018. The Cambridge Analytica scandal began in 2013 when Aleksandr Kogan developed a personality quiz app on Facebook. This app collected information from users and their friends. Kogan transferred this data to Cambridge Analytica, which used it to develop microtargeting techniques. These methods were employed in the 2016 U.S. presidential election and the Brexit referendum. In 2018, The Guardian and The New York Times revealed that Cambridge Analytica had illicitly harvested data from approximately 87 million Facebook users for political advertising. The scandal led to widespread backlash, a significant drop in Facebook's stock, and spurred new data privacy regulations and serious scrutiny of Facebook's data handling practices. [8] [9] [10]

3. Background

3.1 Most Common Ways For Spreading Malwares

The complex properties of real-world systems encompass a wide range of physical and social networks. Technologies such as the Internet of Things (IoT) enable interaction and information sharing between humans and everyday objects. However, the limited computational and memory capabilities, diverse nature, and insufficient security measures in IoT devices lead to significant security and privacy concerns. These vulnerabilities make IoT devices attractive targets for attackers, who can exploit them and turn them into bots. Therefore, autonomous malware in different forms poses a constant threat in today’s Internet. [11] [12]

The two most common ways malware infiltrates systems are through the Internet and email. Essentially, anytime you're online, you're at risk. Malware can enter your computer when you browse compromised websites, encounter legitimate sites serving malicious ads, download infected files, install programs or

apps from unfamiliar sources, or open malicious email attachments (malspam) [1]. In summary, the most common methods for spreading malware include these: [5] [6]

3.1.1 - Exploiting System Vulnerabilities

Software Vulnerabilities: Security defects in software can be exploited by malware to gain unauthorized access to computers, hardware, or networks. Regular updates and patches are crucial to mitigate these risks. [6]

Backdoors: Intended or unintended openings in software, hardware, networks, or system security provide an easy entry point for malware. These backdoors can be inserted by developers for maintenance purposes or discovered by hackers. [6]

Privilege Escalation: Attackers gain escalated access to a computer or network, which they can use to mount more extensive attacks. Implementing strict access controls and continuously monitoring user activities are essential to prevent such escalations. [6]

Drive-by Downloads: Unintended downloads of software occur without the end user's knowledge, often when visiting compromised websites. Security software and cautious browsing habits are key to preventing these incidents. [6]

3.1.2 - Human Manipulation Tactics

Phishing: Cybercriminals trick individuals into clicking malicious links or providing personal information by posing as trustworthy entities. These emails or messages often mimic legitimate sources, making them highly effective. [5]

Spoofing: Hackers disguise themselves to send emails from familiar or trusted organizations. This deception persuades recipients to open harmful attachments or follow malicious links. [5]

Manipulative Marketing: Misleading marketing tactics promote seemingly helpful tools or services. Once downloaded, these tools can install malware on the victim's device. [5]

3.1.3 - Software and Application Exploitation

Software Backdoors: Similar to system backdoors, these are vulnerabilities in software that allow hackers easy access to your device. These can be due to bugs or intentional design choices. [5]

Software Packages: Hidden add-ons or plugins within a program can carry malware. Always scrutinize software for unexpected components before installation. [5]

Mobile Apps: Malicious pop-ups and download links in mobile apps can lead to malware infections. Vigilance and the use of trusted app sources are critical in preventing mobile-based malware. [5]

3.1.4 - Advanced Malware Spreading Tactics

Blended Threats: These are malware packages that combine characteristics from multiple types of malware, making them harder to detect and stop. They can exploit various vulnerabilities simultaneously, requiring comprehensive security solutions. [6]

Homogeneity: Systems running the same operating system and connected to the same network are at higher risk. Diversifying operating systems and segmenting networks can reduce spread of malware. [6]

Comparison Parameter	Traditional	New Generation
Implementation level	simple coded	hard coded
State of behaviors	static	dynamic
Proliferation	each copy is similar	each copy is different
Through spreading	uses .exe extension	uses also different extensions
Permanence in the system	temporal	persistent
Interaction with processes	a few processes	multiple processes
Use concealment techniques	none	yes
Attack type	general	targeted
Defensive challenge	easy	difficult
Targeted devices	general computers	many different devices

Figure-3: Traditional Versus New Generation Malware [15]

3.2 Most Important Signs of Malware Infection

3.2.1 - Performance Issues

• **Slow Computer:** Malware can drastically reduce the speed of your operating system, whether you're navigating the Internet or just using local applications. You might notice your computer's fan working harder than usual, indicating high resource usage in the background. [1] [3] [5]

• **Frequent Crashes and Freezing:** Malware can cause your computer to freeze or crash, often resulting in a Blue Screen of Death (BSOD) on Windows systems. Sustained high CPU usage may also indicate a malware infection. [1] [3] [5]

3.2.2 - Unusual System Behavior

• **Unexpected Pop-up Ads:** Frequent and persistent pop-up ads, especially those promising prizes or free services, are a common sign of adware and other malware. These pop-ups often come bundled with additional hidden threats. [1] [3] [5]

• **Browser Changes:** If your homepage changes or you notice new toolbars, extensions, or plugins that you didn't install, it's likely a sign of malware. Browser redirects to unfamiliar websites can also indicate a malware infection. [3] [5]

• **Unfamiliar Apps:** Discovering programs or icons on your device that you didn't download is another indication of malware. [3]

• **Unauthorized System Changes:** If you notice system settings being changed without your permission, such as altered security settings or disabled features, this can be a sign of malware tampering with your system. [1] [3]

3.2.3 - Security and Access Issues

• **Disabled Antivirus:** If your antivirus program stops working and you cannot turn it back on, it's a sign that malware may have disabled your security software. [1]

• **Loss of Access to Files:** Ransomware often announces its presence by encrypting your files and leaving a ransom note on your desktop or changing your wallpaper to a ransom demand. This malware type requires payment for file decryption. [3]

3.2.4 - Disk and Network Activity

• **Mysterious Loss of Disk Space:** Malware can occupy significant hard drive space, often due to hidden or bloated files. [1]

• **Increased Internet Activity:** Unexplained spikes in Internet activity can be a sign of malware such as Trojans, botnets, or spyware communicating with control servers. [1]

3.2.5 - File and Data Integrity

• **Deleted or Corrupted Files:** Malware may delete or corrupt files to cause chaos or to further its malicious goals. [1] [3]

• **Strange Messages Sent to Contacts:** Some malware spreads by sending emails or messages to your contacts without your knowledge. [3]

3.3 Injecting Malwares To Different Files With Binders

Currently, numerous malware variants are designed to infiltrate the IT infrastructure of companies. Every month, millions of harmful applications and programs are created. Many of these malware are so well-disguised that they effectively conceal their true purpose. [13] Additionally, the use of binders to inject malware into various legitimate applications is becoming increasingly common, making it even more challenging to detect and prevent these threats. This technique allows malicious code to run unnoticed within trusted software, further compromising the security of the affected systems.

Detecting unknown malware is significantly more challenging than identifying known threats. Steganography tools enable users to embed hidden data within carrier files such as videos, audio, or images, which can later be extracted. Attackers exploit this technique to conceal malware within images, deceiving victims. This method is often employed in phishing attacks, a common and well-known tactic used by cybercriminals. [14]

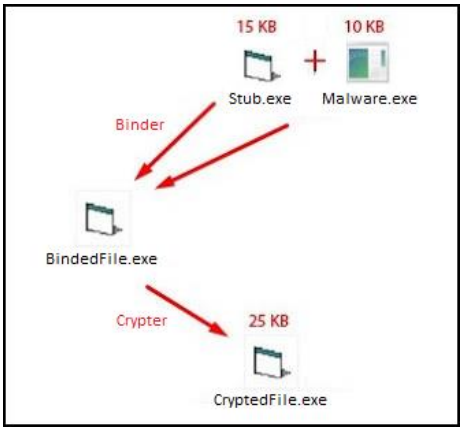

Figure-4: Working Principle of Binder Programs

3.4 Hiding Malwares From Anti Virus Programs

The difficulty of detecting malware in practice arises from the new generation of malware utilizing various obfuscation techniques, such as encryption, oligomorphic, polymorphic, metamorphic, stealth, and packing methods. These techniques significantly complicate the detection process, allowing malware to easily bypass protection software operating in kernel mode, like firewalls and antivirus programs. Moreover, some malware instances exhibit characteristics of multiple classes simultaneously, making it practically impossible to detect all malware with a single detection approach. The common obfuscation techniques are defined as follows: [15]

• **Encryption:** In encryption, malware employs encryption to conceal the malicious code within its overall code structure. [16] As a result, the malware becomes undetectable on the host system.

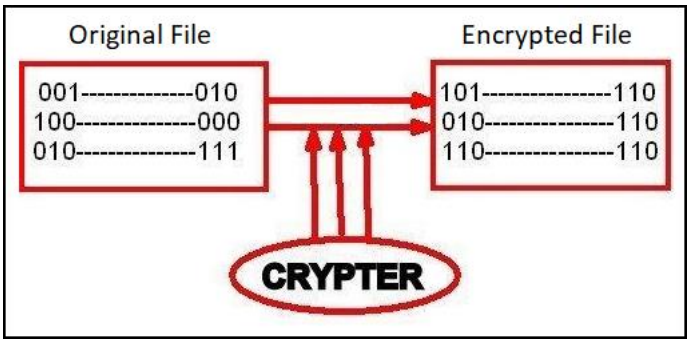

Figure-5: Working Principle Of Crypter Programs

• **Oligomorphic Method:** This method involves using a different key for each encryption and decryption of the malware payload. [17] This makes it more challenging to detect oligomorphic malware compared to malware that only uses encryption.

• **Polymorphic Method:** Similar to the oligomorphic method, the polymorphic method also uses different keys for encryption and decryption. [18] However, polymorphic malware includes multiple copies of the decoder and can have its payload encrypted in layers. [19] This makes detecting polymorphic malware even more difficult than oligomorphic malware.

• **Metamorphic Method:** This method avoids encryption altogether. Instead, it employs dynamic code obfuscation, altering the opcode with each execution of the malicious process. [20] This results in each new copy having a completely different signature, making detection extremely difficult.

• **Stealth Method:** Also known as code protection, the stealth method uses various countermeasures to evade proper analysis. [17] For example, it can alter system settings to remain hidden from detection systems.

• **Packaging:** Packaging is an obfuscation technique that compresses malware to avoid detection or hides the actual code through encryption. [21] [22] This allows malware to easily bypass firewalls and antivirus software. Packaged malware must be unpacked before analysis. Packers can be categorized into four groups: compressors, crypters, protectors, and bundlers.

This section summarizes the limitations of malware detection systems. Recent studies indicate that creating an algorithm capable of detecting all malware is nearly impossible. This difficulty arises because the computational complexity of malware remains unclear, and the malware detection problem has been proven to be NP-complete. Additionally, the use of new techniques such as obfuscation and packing during malware creation further complicates the detection process. [15] As a natural result of all these, it is possible to mislead anti-virus softwares just like in image below:

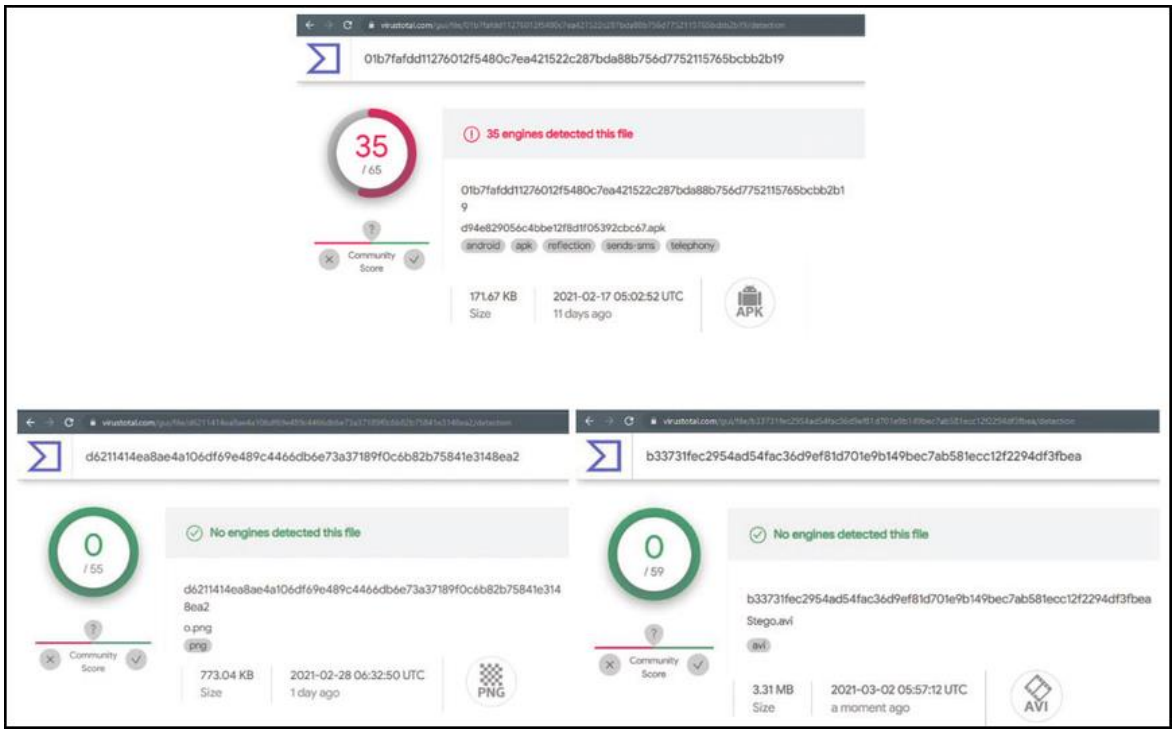

Figure-6: The Results of Virustotal Scanning Before and After Embedding The Ransomware APK File [23]

3.5 Most Common Methods Used For Security Against Malware

Malware spreads through various sophisticated tactics and methods that exploit both human and system vulnerabilities. Understanding these common strategies can help in better protecting systems and networks. By recognizing and understanding these tactics and methods, individuals and organizations can bolster their defenses against the constant threat of malware. Implementing robust security measures and maintaining vigilant digital hygiene are essential steps in mitigating these risks.

• **Antivirus and Anti-Malware Software:** Install reputable antivirus and anti-malware software and perform regular scans to detect and remove malware. Keep these programs updated to protect against the latest threats. Enable real-time protection features to monitor and block malicious activity as it occurs.

• **Firewalls:** Use a network firewall to block unauthorized access to your network. This helps prevent malware from communicating with command and control servers. Enable the host-based firewall on your operating system to provide an additional layer of security for your device.

• **Regular Software Updates:** Keep your operating system updated with the latest security patches and updates to protect against known vulnerabilities. Ensure all applications, especially web browsers and plugins, are updated regularly to close security loopholes.

• **Safe Browsing Practices:** Do not click on suspicious links or download attachments from unknown sources. This is a common method for malware distribution. Ensure websites use HTTPS encryption and be cautious of websites that do not have a secure connection.

• **Email Security:** Use email spam filters to reduce the likelihood of receiving phishing emails and malware-laden attachments. Be cautious when opening emails from unknown senders. Do not open attachments or click on links in these emails.

• **Regular Backups:** Regularly back up your data to an external hard drive or cloud service. This ensures that you can restore your system in case of a ransomware attack or data corruption. Keep backups isolated from your main network to protect them from malware infections.

• **User Education and Awareness:** Conduct regular training sessions to educate users about the dangers of malware and safe online practices. Teach users how to recognize phishing attempts and other common social engineering tactics.

• **Use of Strong Passwords:** Use strong, complex passwords for all accounts and change them regularly. Avoid using the same password across multiple sites. Use a password manager to generate and store unique passwords securely.

• **Multi-Factor Authentication (MFA):** Implement MFA on all accounts where possible to provide an additional layer of security beyond just passwords.

• **Application Whitelisting:** Use application whitelisting to control which programs are allowed to run on your devices. This can prevent unauthorized applications, including malware, from executing.

Note that, malicious apps can hide in seemingly legitimate applications, especially when they are downloaded from websites or direct links (in an email, text, or chat message) instead of an official app store. Here it's important to look at the warning messages when installing applications, especially if they seek permission to access your email or other personal information.

3.6 Most Common Methods Used For Detecting Hidden Malware

Every month, millions of malicious applications and programs are developed. Many of these malware types are heavily obfuscated to conceal their true purposes. While antivirus software and firewalls are available to help, they are not always sufficient. This is where malware analysis becomes crucial. [24]

Autonomously spreading malware, such as worms or bots, poses a significant threat on the modern Internet. Early sample collection is crucial for effectively combating these threats, as it allows for the development of antivirus signatures and other countermeasures. Consequently, traditional antivirus methods are often outpaced by hackers. To address this, new tools have been created that can automatically gather autonomously spreading malware samples. [25] However, the detection of hidden malware requires advanced methods, such as behavioral analysis and machine learning, to identify anomalies that traditional antivirus solutions might miss. [24]

The analysis and detection of malicious software are vital aspects of computer security. Traditionally, signature-based malware detection methods have been used effectively. However, malware creators can evade these methods through obfuscation techniques such as metamorphism and polymorphism. To counter this, machine learning-based methods have been introduced. Nonetheless, these approaches still face several challenges. [26]

In the realm of Computer Security, there are various methods and tools ranging from the combination of Artificial Intelligence, Machine Learning, and Data Science for Malware and Vulnerabilities Detection to Firewall Design and Implementation, as well as Intrusion Detection Systems. Additionally, advanced encryption techniques, behavior-based threat detection, and anomaly detection systems play crucial roles in safeguarding digital environments. These diverse approaches collectively enhance the ability to predict, prevent, and respond to security threats effectively. [15] [27] [28] Additionally several specially developed methods such as general behaviour monitoring [29], program DNS behaviour analysis [30], dynamic evolution analysis [31], periodically scheduled patching [32] exists. We can summarize them like in the image below:

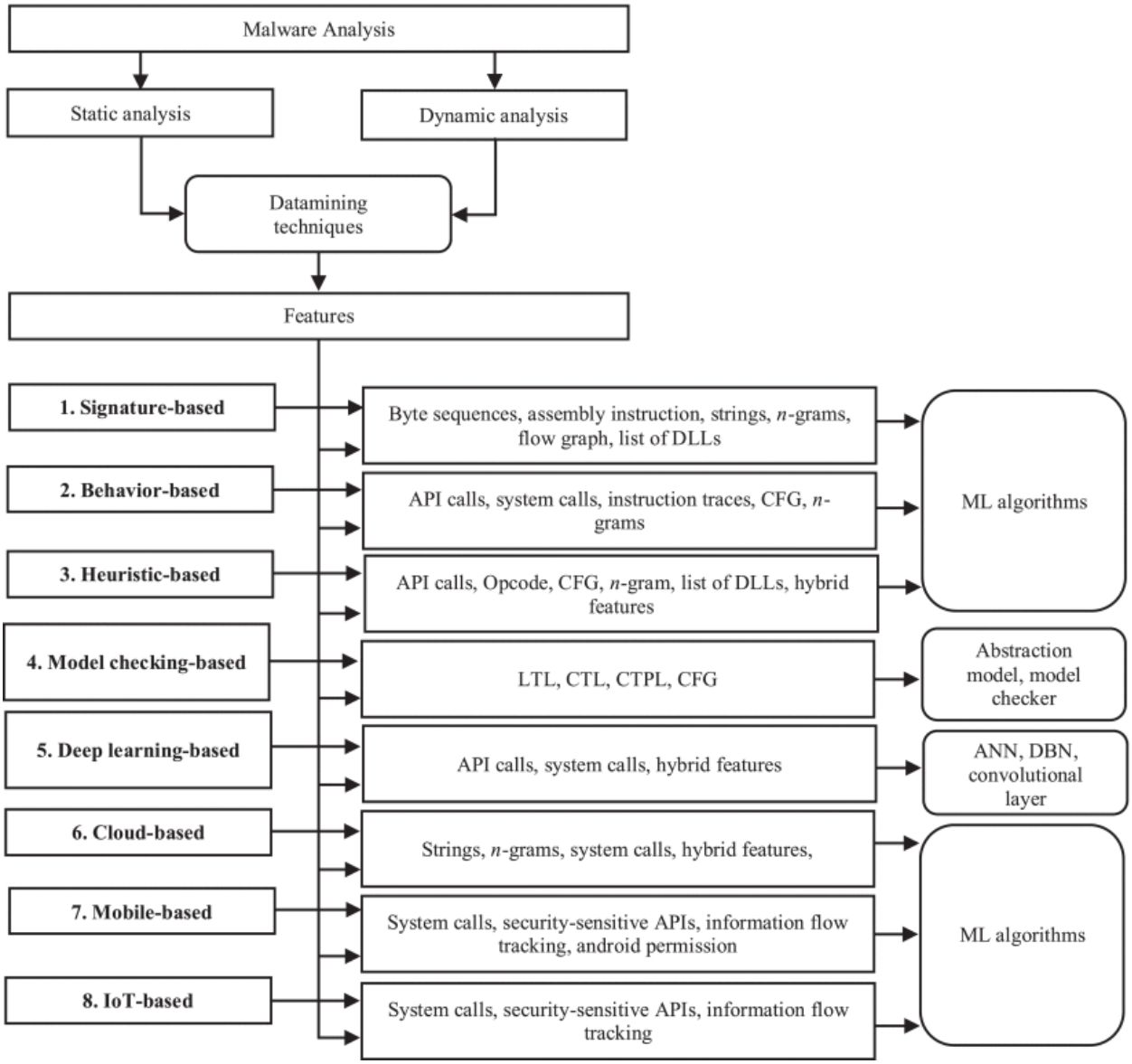

Figure-7: Malware Detection Approaches [15]

Important Note: In our BBM465 Information Security Lab course, we developed a project titled "Creating a Threat Intelligence for Anti-Phishing" using the C# programming language, incorporating medical processing techniques. We employed various local and global image feature extractors, such as FCTH, CEDD, SCD, SIFT, and HOG, to analyze images from websites. Our objective was to develop an artificial intelligence system to enhance phishing protection. Source code and project report is available on Github. [33]

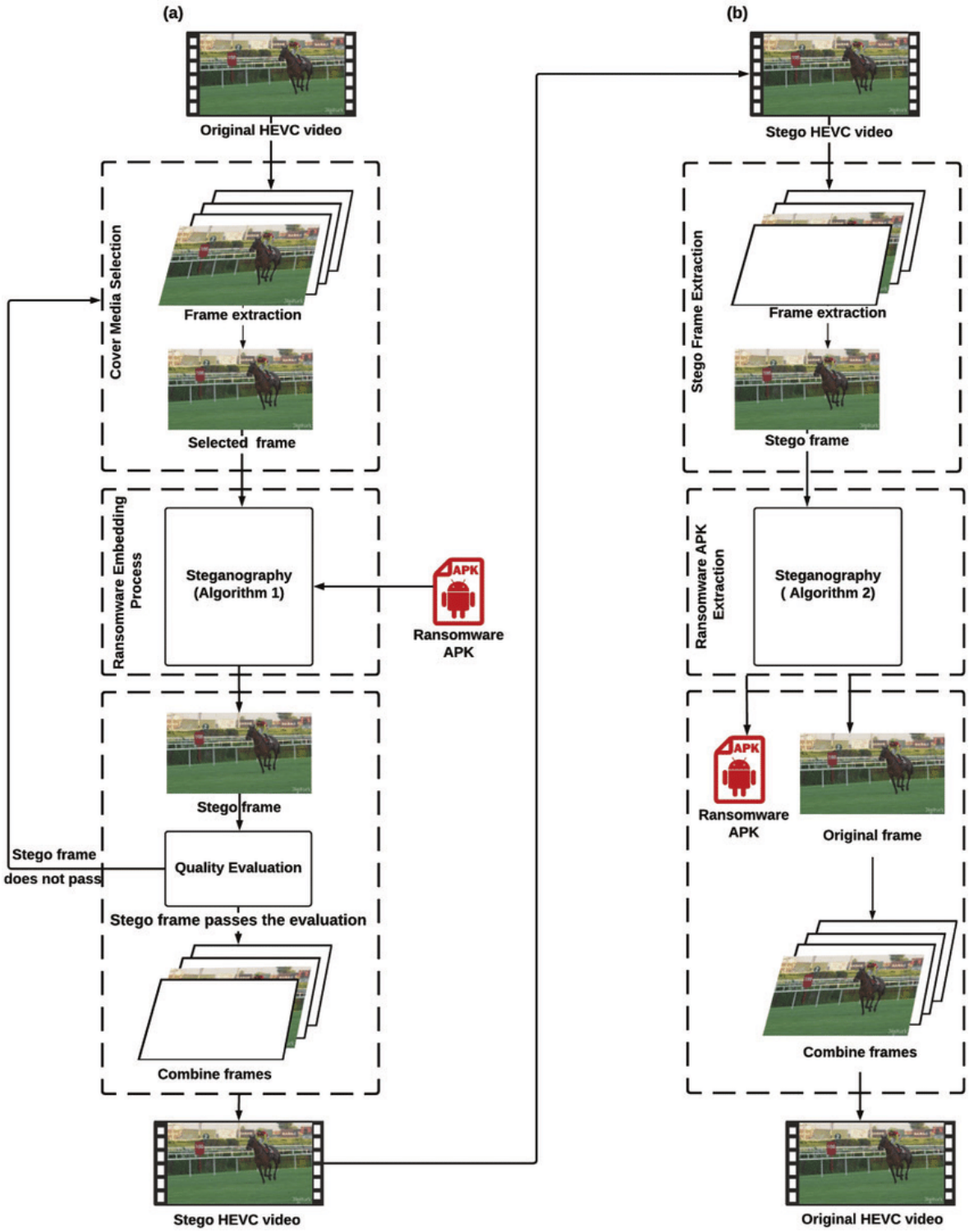

Figure-8: The proposed HEVC steganography-based ransomware hiding model (a) Ransomware Embedding Process (REP), (b) Ransomware Extraxting Process (RExP) [23]

4. Result

The rapid development and increasing reliance on technology in our daily lives have made cybersecurity and malware research crucial for protecting personal information. As digital environments expand, cybersecurity teams constantly strive to secure systems against evolving malware threats. This article aims to equip readers with essential knowledge to understand and combat these threats, contributing to a safer digital environment.

Our research presents a literature review of the historical evolution of malware, discussing its common characteristics, propagation methods, and the significant damages it has caused. By analyzing most popular malware, we offer solutions to detect and prevent these threats. Ultimately, this study provides valuable insights into the ever-evolving landscape of malware, emphasizing the importance of continuous vigilance and innovation in cybersecurity.

5. References

[1] “Malware”, malwarebytes.com, https://www.malwarebytes.com/malware (accessed May. 16, 2024).
[2] “Malware Damage”, kaspersky.com, https://usa.kaspersky.com/resource-center/threats/malware-damage (accessed May. 16, 2024).
[3] “What Is Malware? The Ultimate Guide to Malware”, avg.com, https://www.avg.com/en/signal/what-is-malware (accessed May. 16, 2024).
[4] “Cyberthreat Real-Time Map” kaspersky.com, https://cybermap.kaspersky.com/ (accessed May. 16, 2024).
[5] “Spyware”, norton.com, https://us.norton.com/blog/malware/spyware (accessed May. 16, 2024).
[6] “22 Types of Malware and How to Recognize Them”, upguard.com, https://www.upguard.com/blog/types-of-malware (accessed May. 16, 2024).
[7] “A survey of distributed denial-of-service attack, prevention, and mitigation techniques”, Dec. 2017, available: https://www.researchgate.net/publication/321775189 (accessed May. 16, 2024)
[8] “Facebook–Cambridge Analytica data scandal”, Wikipedia, https://en.wikipedia.org/wiki/Facebook–Cambridge_Analytica_data_scandal, (accessed May. 17, 2024)
[9] “History of the Cambridge Analytica Controversy”, Mar. 2023, Bipartisian Policy, https://bipartisanpolicy.org/blog/cambridge-analytica-controversy/ (accessed May. 17, 2024)
[10] “Cambridge Analytica, LLC, In the Matter of”, Dec. 2019, Federal Trade Comission, https://www.ftc.gov/legal-library/browse/cases-proceedings/182-3107-cambridge-analytica-llc-matter (accessed May. 17, 2024)
[11] “Measurement and Analysis of Autonomous Spreading Malware in a University Environment”, 2007, Springer Link, https://link.springer.com/chapter/10.1007/978-3-540-73614-1_7 (accessed May. 18, 2024)
[12] “Mitigating Mirai Malware Spreading in IoT Environment”, Dec. 2018, IEEE, https://ieeexplore.ieee.org/abstract/document/8554643 (accessed May. 18, 2024)
[13] “Automated Malware Identifier and Analyzer”, June 2020, https://link.springer.com/chapter/10.1007/978-981-15-4851-2_9 (accessed May. 19, 2024)
[14] “Developing Malware and Analyzing it Afore & After Steganography with OSINTs”, November 2020, https://ieeexplore.ieee.org/abstract/document/9298288 (accessed May. 19, 2024)
[15] “A Comprehensive Review on Malware Detection Approaches”, January 2020, https://ieeexplore.ieee.org/abstract/document/8949524 (accessed May. 20, 2024)
[16] K. Alzarooni, "Malware variant detection", 2012.
[17] P. Szor, The Art of Computer Virus Research and Defense, Upper Saddle River, NJ, USA:Pearson Education, 2005.
[18] W. Stallings and L. Brown, Computer Security: Principles and Practice, Upper Saddle River, NJ, USA:Pearson Education, 2012.
[19] P. Szor and P. Ferrie, "Hunting for metamorphic", Proc. Virus Bull. Conf., 2001.
[20] S. Alam, R. Horspool, I. Traore and I. Sogukpinar, "A framework for metamorphic malware analysis and real-time detection", Comput. Secur., vol. 48, pp. 212-233, Feb. 2015.
[21] M. D. Preda, Code Obfuscation and Malware Detection by Abstract Interpretation, Nov. 2019

[22] W. Yan, Z. Zhang and N. Ansari, "Revealing packed malware", IEEE Secur. Privacy Mag., vol. 6, no. 5, pp. 65-69, Sep. 2008.
[23] “Novel Ransomware Hiding Model Using HEVC Steganography Approach”, Sept. 2021, https://www.researchgate.net/publication/354477993_Novel_Ransomware_Hiding_Model_Using_HEVC_Steganography_Approach (accessed May. 21, 2024)
[24] “Automated Malware Identifier and Analyzer”, June 2020, https://link.springer.com/chapter/10.1007/978-981-15-4851-2_9 (accessed May. 21, 2024)
[25] “Collecting Autonomous Spreading Malware Using High-Interaction Honeypots”, https://link.springer.com/chapter/10.1007/978-3-540-77048-0_34 (accessed May. 21, 2024)
[26] “Techniques of Malware Detection: Research Review”, Oct. 2021, https://ieeexplore.ieee.org/document/9620415 (accessed May. 21, 2024)
[27] “A Comprehensive Review on Malware Detection Approaches”, Jan. 2020, https://ieeexplore.ieee.org/abstract/document/8949524 (accessed May. 21, 2024)
[28] “Malware and Vulnerabilities Detection and Protection”, 2022 https://ieeexplore.ieee.org/document/9562709 (accessed May. 21, 2024)
[29] “Research on android malware detection and interception based on behavior monitoring”, Nov. 2012, https://link.springer.com/article/10.1007/s11859-012-0864-x (accessed May. 21, 2024)
[30] “Detecting Malware Injection with Program-DNS Behavior”, Sep. 2020, https://ieeexplore.ieee.org/abstract/document/9230384 (accessed May. 21, 2024)
[31] “Tipping point prediction and mechanism analysis of malware spreading in cyber–physical systems”, Mar. 2023, https://www.sciencedirect.com/science/article/abs/pii/S100757042300165X (accessed May. 21, 2024)
[32] “Optimal Impulsive Control of Epidemic Spreading of Heterogeneous Malware”, Oct. 2017 https://www.sciencedirect.com/science/article/pii/S2405896317334341 (accessed May. 21, 2024)
[33] “My Github Page About Creating A Threat Intelligence For Anti Phishing” https://github.com/mrkaptantr/Hacettepe-University-Computer-Science/tree/main/BBM465%20-%20Information%20Security%20Laboratory/Programming%20Assignment%204%20-%20Creating%20A%20Threat%20Intelligence%20For%20Anti%20Phishing%20%5BC%23%5D