applied sciences

MDPI

Article

Can Windows 11 Stop Well-Known Ransomware Variants? An Examination of Its Built-in Security Features

Yousef Mahmoud Al-Awadi [1], Ali Baydoun [1,*] and Hafeez Ur Rehman [1,2]

[1] School of Computing and Data Sciences, Oryx Universal College with Liverpool John Moores University, Doha 34110, Qatar; 101769@oryx.edu.qa (Y.M.A.-A.); hafeez.r@oryx.edu.qa (H.U.R.)
[2] Department of Computer Science, National University of Computer and Emerging Sciences, Islamabad 44000, Pakistan
* Correspondence: ali.b@oryx.edu.qa

Abstract: The ever-evolving landscape of cyber threats, with ransomware at its forefront, poses significant challenges to the digital world. Windows 11 Pro, Microsoft's latest operating system, claims to offer enhanced security features designed to tackle such threats. This paper aims to comprehensively evaluate the effectiveness of these Windows 11 Pro, built-in security measures against prevalent ransomware strains, with a particular emphasis on crypto-ransomware. Utilizing a meticulously crafted experimental environment, the research adopted a two-phased testing approach, examining both the default and a hardened configuration of Windows 11 Pro. This dual examination offered insights into the system's inherent and potential defenses against ransomware threats. The study's findings revealed that Windows 11 Pro does present formidable defenses. This paper not only contributes valuable insights into cybersecurity, but also furnishes practical recommendations for both technology developers and end-users in the ongoing battle against ransomware. The significance of these findings extends beyond the immediate evaluation of Windows 11 Pro, serving as a reference point for the broader discourse on enhancing digital security measures.

Keywords: cybersecurity; malware; ransomware; Windows 11; cyberattack

check for updates

Citation: Al-Awadi, Y.M.; Baydoun, A.; Ur Rehman, H. Can Windows 11 Stop Well-Known Ransomware Variants? An Examination of Its Built-in Security Features. *Appl. Sci.* **2024**, *14*, 3520. https://doi.org/10.3390/app14083520

Academic Editors: Peter R. J. Trim and Yang-Im Lee

Received: 2 January 2024
Revised: 17 February 2024
Accepted: 20 February 2024
Published: 22 April 2024

Copyright: © 2024 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (https://creativecommons.org/licenses/by/4.0/).

1. Introduction

Our increasing reliance on technology has led to growth not only in its benefits but also in the threats it poses, as cyber-attacks occur at an alarming rate of once every 39 s [1]. Among these threats, ransomware particularly has proven to be one of the most damaging [2,3]. Ransomware stands out as an especially menacing adversary. Originating as simple scareware that tricked users into paying, ransomware has evolved into a sophisticated tool of cyber extortion, encrypting victims' data and demanding a ransom for its release [4]. This evolution underscores the increasing complexity and sophistication of cyber threats as most economic, commercial, cultural, social, and governmental activities are now being carried out in cyberspace, making them potential targets [5]. These escalating trends underline the need for robust cybersecurity measures embedded within modern operating systems like Microsoft Windows 11. In the face of this escalating threat, tech giants like Microsoft have risen to the challenge. With the introduction of Windows 11, Microsoft has ushered in advanced security features to mitigate such cyber onslaughts, particularly those posed by ransomware [6]. However, as these features are novel, their real-world efficacy against a spectrum of ransomware threats remains to be thoroughly assessed. This study is set to make a valuable contribution to the field of cybersecurity by assessing the effectiveness of Windows 11's built-in security features against a selection of the most widespread ransomware variants, focusing specifically on the MortalKombat ransomware variant. The results of this research could have important implications for a wide range of stakeholders, including individual users and organizations, developers, policymakers, academics, and professionals.

2. Literature Review

This review delves into the intricate details of ransomware and the robust security features incorporated in Windows 11 Pro. In doing so, it aims to provide a comprehensive context for the subsequent examination of the effectiveness of Windows 11 Pro's built-in security features against ransomware. This review comprehensively covers the important aspects of the ransomware variants we selected in the research and the robust security features incorporated in Windows 11 Pro.

2.1. Ransomware Overview

Ransomware is malware utilized to lock users out of their systems or encrypt their data, making it inaccessible [7]. Victims are then presented with ransom demands, primarily in the form of messages to make them aware of the encryption and instruct how the ransom should be paid for them to receive the decryption key [8]. Ransomware may impact different data or files on victims' devices [9]. The ransomware attack process can generally be broken down into five phases:

1. Delivery: Involves the delivery of the malicious payload to the targeted network by using spam emails, social engineering, etc. [10].
2. Deployment: Involves the extraction of a second payload from the initial malware, which can bypass detection by disguising itself as benign or routine network traffic [11].
3. Destruction: Begins searching for specific file types (pdf, docx, jpeg, etc.) across all accessible volumes in the system to encrypt them. The ransomware then communicates with the attacker's command and control server (C&C) to retrieve the encryption keys [12].
4. Dealing: Generates a ransom demand on the victim's screen. It includes instructions on how to pay the ransom and how the encrypted files can be retrieved after payment. However, it is worth noting that paying the ransom does not guarantee that the decryption keys will be provided or that the files can be recovered successfully [12].
5. Exfiltration and Persistence: Siphons off sensitive data, which can be used as additional leverage against victims or sold on the dark web, further monetizing the attack. Additionally, some ransomware variants aim to maintain persistence in the infected systems, often using methods such as creating or modifying registry keys, scheduled tasks, or injecting code into other processes [13].

2.2. Ransomware Variants

There are many notable ransomware variants in the extended literature, including WannaCry, CryptoLocker, Locky, Hive, Maze, Conti, MortalKombat, Cerber, etc. [14–16]. For the research's credibility and relevance, a representative set of well-known ransomware variants was selected for inspection. Table 1 illustrates the three main ransomware variants presented in the literature.

Table 1. Well-Known Ransomware Variants.

Ransomware Variant	Year of Discovery	Origin	Key Features	Encryption Method	Decryptor Available
Hive [14,17]	2021	Unclear	RaaS, Wiper capabilities, Double extortion methods	Proprietary	Version 5 variant only
MortalKombat [16,18]	2023	Unknown	Xorist ransomware family offshoot	TEA (Tiny Encryption Algorithm)	Yes
Cerber [19,20]	2016	Unknown	RaaS, Geographic targeting mechanism	AES and RSA-2048	Yes

These variants were chosen based on multiple criteria, including their prevalence in recent cyberattacks, their notoriety within the cybersecurity community, and their varied modes of operation, ensuring a comprehensive testing spectrum.

2.3. Windows 11 Security Characteristics

When Microsoft Windows 11 Pro was released in January 2022, Microsoft claimed that Windows 11 Pro brought several security enhancements compared to its predecessor, Windows 10. It introduces robust security features designed to guard against advanced, persistent threats, including ransomware, effectively integrating with a broader cybersecurity approach. Table 2 depicts the main security features of Microsoft Windows 11 Pro.

Table 2. Windows 11 Pro Security Characteristics.

Security Characteristic	Description
Virtualization-Based Security (VBS)	Uses hardware virtualization features to isolate key security processes, enhancing protection against attacks. VBS protects critical system components and sensitive data from ransomware [21].
Memory Integrity	Protects the memory from attacks, specifically from kernel-mode code injection techniques. It can significantly impede ransomware's ability to infiltrate and control system processes [22].
Mandatory Trusted Platform Module (TPM) 2.0	Provides hardware-based security by storing cryptographic keys and other sensitive data in an isolated and secure environment within the device, thereby preventing ransomware from accessing these crucial elements [23].
UEFI Secure Boot	Fortifies the boot process against unauthorized changes, ensuring that only trusted software is executed during the booting process and thereby preventing the loading of malicious bootloaders that could compromise the system [24].
Microsoft Pluton	Uses chip-to-cloud security technology designed to provide a new level of hardware security. It enhances protection against physical attacks and prevents the theft of credential and encryption keys [25].
Hardware-enforced Stack Protection	Adding another layer of defense against ransomware, it enhances system protection against Return Oriented Programming (ROP) attacks, a common exploitation method used by ransomware to hijack a program's control flow [26].
Regular Updates	Facilitates faster, less disruptive updates by minimizing the size of updates by up to 40% [27]. This encourages users to keep their systems updated with the latest security patches, which are vital in the fight against ransomware [27].

2.4. Related Studies

In the extensive realm of ransomware literature, there is a dire need for specific studies that delve deeper into the intricacies of modern defense mechanisms. While there is a plethora of information on general anti-ransomware strategies, a clear gap emerges when seeking an in-depth analysis of Windows 11's unique security features [28]. This study enthusiastically seeks to navigate this space, offering a keen focus on these features in the specific context of defending against crypto-ransomware. Notably, while contributions like those from [29] provide a broad-brush picture of the ransomware landscape and Windows 11's defenses, they stop short of presenting tangible tests or simulations. Recognizing this shortfall, our research endeavors to bridge this gap by creating a robust, controlled testing environment on a Windows 11 Pro virtual machine. The journey does not stop there. The literature space seems to skim over the detailed assessment of Windows 11's proactive

security features, especially in the throes of real-world ransomware scenarios. Our research seeks to offer this granularity, presenting a meticulous review of the effectiveness of these defenses. In [30], the authors ventured into a comparative realm, equating paid antivirus solutions with Windows Defender in the broader malware detection arena. However, a noticeable gap exists in the depth of exploration regarding how the nuanced features of Windows Defender measure up against the formidable challenge posed by ransomware. While the study aptly contrasts paid antivirus solutions with Windows Defender in the broader context of malware detection, it falls short in providing a comprehensive examination of the specific capabilities and limitations of Windows Defender in addressing the ransomware menace.

3. Methodology

This section presents the broad strategy of the research, including the experimental design, the specifics of the experimental environment, and the details of the system and network configurations. The research design for this study is rooted in a practical and experimental approach, which is deemed most appropriate for a comprehensive evaluation of Windows 11 Pro's security features against ransomware threats.

3.1. Experimental Environment Setup

3.1.1. Experimental Environment

The experimental environment is established on a dedicated physical machine running Windows 11 Pro, reflecting a typical user configuration. The machine is equipped with 6 Cores, 16 GB RAM, and a 512 GB hard disk, carefully configured to mirror real-world, up-to-date systems as closely as possible.

3.1.2. Network Isolation

This is facilitated through a router that also behaves as a switch, creating a specialized environment exclusively for testing. Central to this setup is the gateway firewall housed within the router. It is armed with a specific rule that denies any connection attempts between the test environment and other devices or networks on the local grid.

3.1.3. User Data Simulation

To improve the realism of the test environment and align it more closely with potential real-world targets, a diverse array of file types is included on the physical machine running Windows 11 Pro. These file types cover various scripts, text documents, Word and Excel files, and PNG and JPEG images, to name a few, of various sizes. Additionally, some well-known software that can be found on a typical machine will be installed, such as Google Chrome, Google Drive, and Zoom, among others. By including a variety of file types in our test environment, the study caters to the potential behaviors of diverse ransomware strains.

3.2. Windows 11 Pro Configuration

These configurations, both default and hardened, aim to provide a comprehensive understanding of Windows 11 Pro's capabilities against ransomware attacks under different security postures.

3.2.1. Default Configuration

The first phase of testing maintains the default security configurations within Windows 11 Pro. This environment represents a baseline, simulating a common user system that relies on the standard settings provided by the operating system. In the default environment, Windows 11 Pro's Windows Defender is configured with the following features illustrated in Table 3.

Table 3. Windows 11 Pro Default Security Configuration.

Security Feature	Description
Real-time protection [31]	- Uses heuristics and behavior analysis to detect unknown threats. - Monitors file and program activity, alerting users to suspicious behaviors and blocking potentially harmful actions.
Cloud-delivered protection [32]	- Leverages Microsoft's vast cloud infrastructure to quickly identify and respond to emerging threats. - Uses machine learning models and big data analysis to predict and counteract new malware strains.
Automatic sample submission [32]	- Uses a secure channel to send suspicious files to Microsoft's labs. - The analysis helps in refining heuristics and improving detection algorithms.
Tamper protection [33]	- Secures against root-level attacks that attempt to disable security features. - Integrates with system-level permissions, ensuring only authorized users can modify security settings.
Firewall [34]	- Uses stateful inspection to monitor active connections. - Implements packet filtering to analyze network data and block malicious traffic.
Smart App Control [35]	- Uses a combination of local heuristics and cloud-based analysis to evaluate app behaviors. - Integrates with Microsoft's app reputation database to determine the trustworthiness of applications.
Reputation-based protection [36]	- Employs URL filtering and reputation checks to block access to malicious sites. - Uses a continuously updated database of known phishing sites, malware domains, and other online threats.
Memory access protection [37]	- Implements hardware-based virtualization to isolate key processes. - Uses Virtualization-Based Security (VBS) to protect critical parts of the OS from tampering.
Device encryption [38]	- Uses BitLocker technology to encrypt the entire hard drive. - Employs the Trusted Platform Module (TPM) to store encryption keys securely.
Exploit protection [39]	- Control Flow Guard (CFG): Protects against memory corruption vulnerabilities by checking the legitimacy of target addresses during indirect calls. - Data Execution Prevention (DEP): Blocks execution of code from data pages, preventing buffer overflow attacks.

3.2.2. Hardened Configuration

Following the initial testing, the Windows 11 Pro testing machine will be wiped clean, and specific enhancements and configurations will be applied to fortify the system against ransomware attacks. This "hardened" environment showcases how a more security-conscious user might configure their system, emphasizing particular features and settings to enhance resilience against malware and other threats. For the hardened environment, Windows 11 Pro's Windows Defender is configured with enhanced features. Table 4 shows the hardened configuration of the Windows 11 Pro testing machine.

Table 4. Windows 11 Pro Hardened Configuration.

Security Feature	Description
Controlled folder access	- Windows employs a feature called Controlled Folder Access in Windows 11 to implement this protective measure. It protects specific folders from unauthorized changes, acting as a defense layer against threats like ransomware. By default, it ensures the security of user directories, including but not limited to Documents, Pictures, Videos, and others.
Account protection	- Enhances the security of sign-in options.
Potentially unwanted app blocking	- Actively prevents potentially unwanted applications (PUAs) from being installed.
Memory integrity	- A part of Core isolation in device security, it is turned on to enhance memory protection.
Exploit protection adjustments	- Settings like forcing randomization for images (Mandatory ASLR) are activated.
Smart App Control	- Adjusted from 'Evaluation' mode to 'On' mode. In this mode, it actively assesses any app initiated on Windows, blocking it if deemed harmful or unwanted.
Isolated browsing	- While not installed by default, for the purpose of this study, it will be configured to provide an additional layer of protection during web browsing.

3.3. Rationale for Selecting the Ransomware

A representative set of known ransomware variants were chosen for testing. These samples should reflect the diversity of ransomware threats that real-world users might encounter. the scope was narrowed down to focus on three specific ransomware variants. This shift in the number of tested ransomware variants is aimed at delivering a more detailed and focused evaluation of Windows 11's resilience and detection capabilities.

These samples were chosen based on multiple criteria, including their prevalence in recent cyberattacks, their notoriety within the cybersecurity community, and their varied modes of operation, ensuring a comprehensive testing spectrum. This selection aims to provide a realistic representation of the threats that everyday users and businesses might face in real-world scenarios.

In the context of this research, MortalKombat, Hive, and Cerber ransomware variants were chosen for experimentation. This choice stems from their classification as recent ransomware variants and their deliberate focus on users of Windows operating systems. Furthermore, it is important to highlight the scarcity of literature addressing the definitions and operations of these ransomware variants, adding to the significance of this research endeavor.

3.4. Testing Procedures

The tests are conducted on a designated physical machine running Windows 11 Pro, specifically set up to evaluate Windows Defender's effectiveness against ransomware variants. This physical environment replicates a real-world scenario, allowing for a more authentic analysis. Figure 1 outlines the penetration testing procedures for assessing Windows Defender against ransomware variants. After setting up the testing environments, we introduce selected ransomware variants and meticulously observe the system's reactions. The figure highlights a structured approach that is designed to generate experimental data, offering insights into the effectiveness of Windows 11 Pro's security.

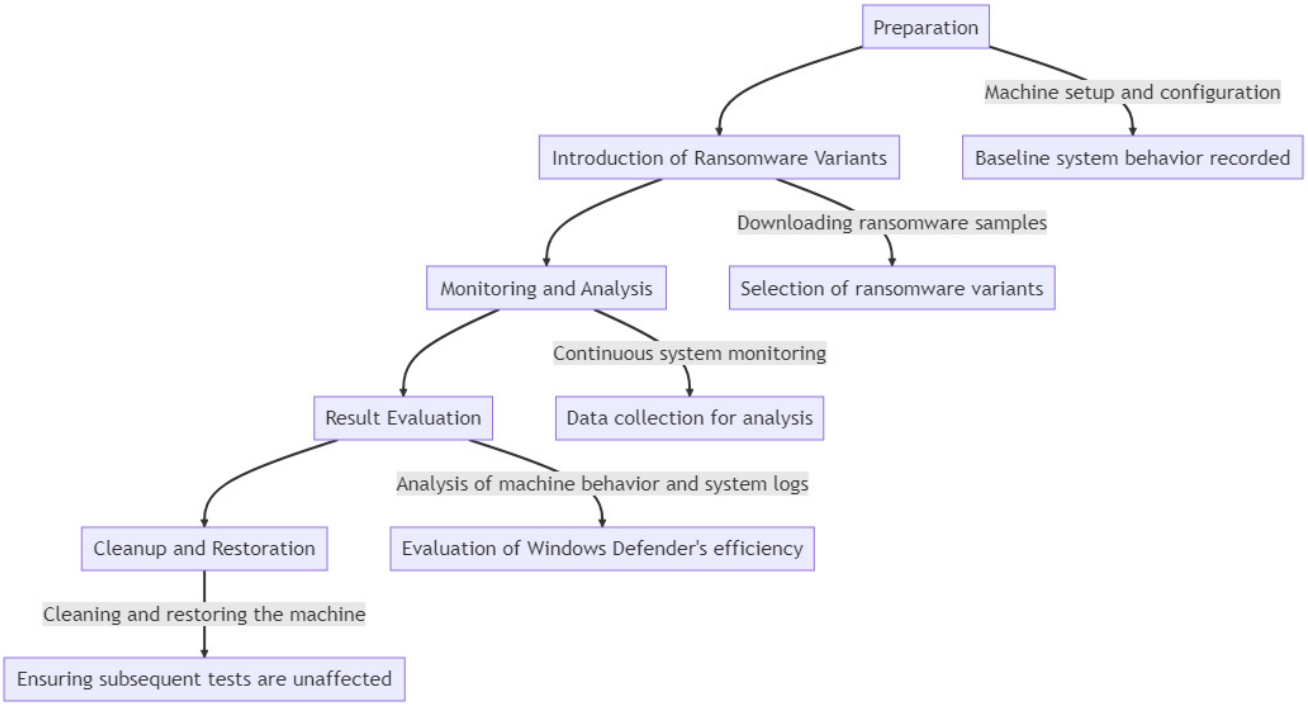

Figure 1. Flow Chart of Penetration Testing Procedures for Evaluating Windows Defender against Ransomware Variant.

3.4.1. Testing Procedures in the Default Environment

The default environment represents the baseline configuration, where the systems and networks operate without any specialized hardening or advanced security measures. The testing procedures conducted within this environment aim to evaluate the vulnerability of typical systems against ransomware attacks.

- Experiment Setup

In the default environment, all operating systems, applications, and network devices were configured to their out-of-the-box settings. Standard user privileges were granted, and no additional firewalls, intrusion detection systems, or endpoint protection mechanisms were deployed.

- Attack Simulation

Utilizing a controlled isolated network, a ransomware attack was simulated using a known ransomware strain. The efficiency and effectiveness of the attacks were measured based on the time to infiltration, the extent of encryption, and the ability to detect the attack.

- Data Collection and Analysis

Logs, alerts, and forensic data were collected during the attack simulation. The default environment's response was analyzed to identify potential weaknesses and entry points exploited by the ransomware, providing insights into commonly targeted vulnerabilities.

3.4.2. Testing Procedures in the Hardened Environment

The hardened environment refers to the configuration where the systems and networks are specifically fortified against potential ransomware attacks through the implementation of enhanced security measures.

- Experiment Setup

The hardened environment employed a combination of advanced firewalls, intrusion detection and prevention systems (IDPS), endpoint protection platforms (EPP), and re-

stricted user privileges. All configurations were meticulously crafted to align with industry best practices for ransomware mitigation.

- Attack Simulation

Ransomware attack simulations were conducted under the same isolated conditions, utilizing the same strains as in the default environment. The focus here was to evaluate the resilience of the hardened environment by assessing the ability of ransomware to penetrate the enhanced security layers and by examining any thwarted attempts to communicate or propagate.

- Data Collection and Analysis

Comprehensive logs, alerts, and forensic data were collected to analyze the efficiency and effectiveness of the hardening measures. The analysis emphasized the points of resistance, identifying the specific mechanisms that successfully thwarted or mitigated the ransomware attacks. Comparative analysis with the default environment provided actionable insights into the value and impact of the applied hardening techniques.

3.5. Detection Procedure

Understanding how effectively the inherent security mechanisms in Windows 11, primarily Windows Defender, can detect the chosen ransomware variants is a central part of this study. Unlike penetration testing, this phase is tailored to evaluate the system's ability to recognize a malicious intrusion before serious harm occurs. Figure 2 depicts the detection testing process stages.

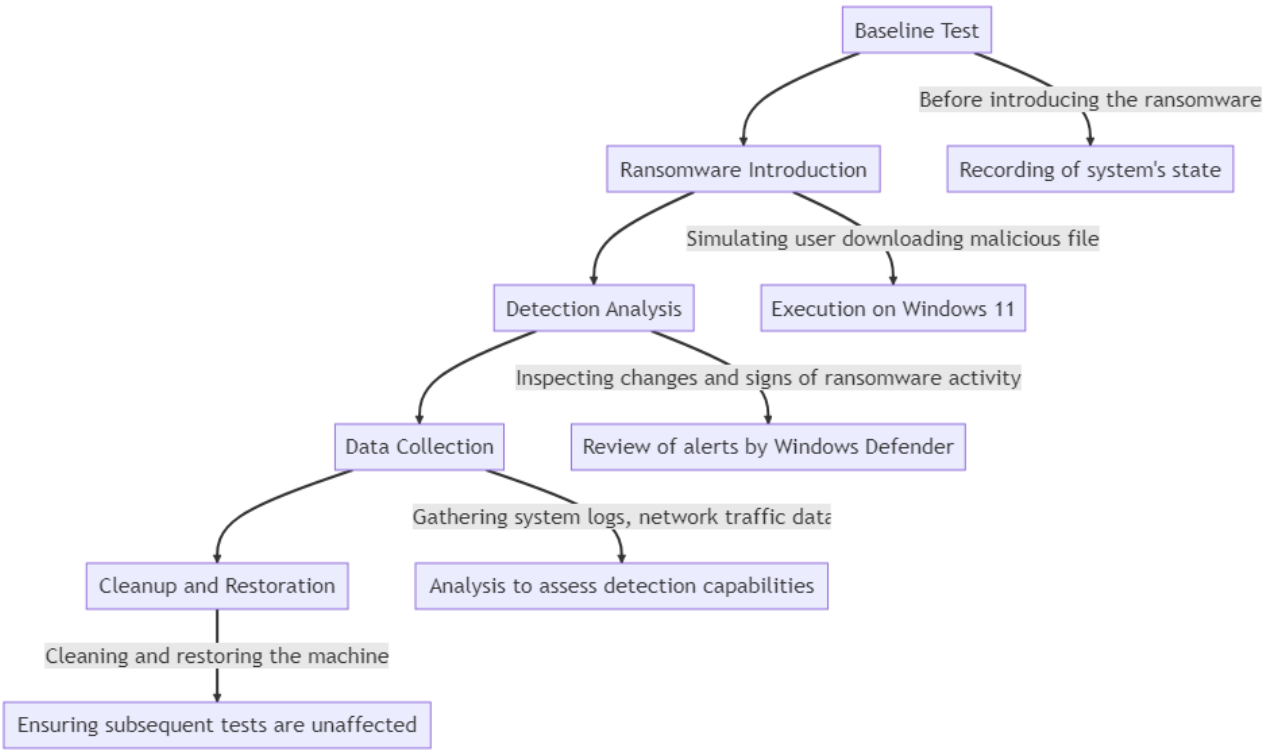

Figure 2. Flow Chart of Ransomware Detection Testing Process.

3.6. Testing Tools

For an accurate assessment of the malware's behavior and Windows Defender's response, various monitoring and filtering techniques were implemented. These strategies included:

- Sysinternals Suite: A collection of system utilities to monitor system behavior.
- Process Monitor: Observes real-time file system, registry, and thread activity.

- Windows Event Logs: Analysis of system logs to detect suspicious activity.
- Windows Defender Logs: Review of the logs specific to Windows Defender to evaluate its response to the malware.

4. Experimental Results

In this section, we present the outcomes of our assessment of Windows 11 Pro's defenses against three prominent ransomware variants: Cerber, Hive, and MortalKombat. The test was executed in two distinct environments: a Windows 11 Pro default configuration and a hardened configuration with enhanced security settings of Windows 11 Pro (As specified in the Section 3). The following section will delve into the system's responses, supplemented by detailed log insights, to provide a comprehensive understanding of Windows 11 Pro's capabilities and defense mechanisms.

4.1. MortalKombat

Default Environment Outcome

Upon unzipping the MortalKombat ransomware in the default environment, Microsoft Defender instantly detected the threat and took immediate action. The malware was detected as *Trojan:Win32/Vindor!pz*. Figure S1 illustrates the system behaviors as soon as the MortalKombat ransomware was unpacked.

Key Observations:

Subsequent to its detection, the ransomware was immediately quarantined, ensuring no further malicious actions could take place. The threat was isolated, and the system reported, "No additional actions required", signifying a successful containment of the threat.

Despite the user potentially attempting to execute the ransomware post-extraction, Windows Defender ensured that the ransomware remained non-functional. It is notable that there was no activity observed, underscoring the immediate action taken by Windows Defender, which prevented any further malicious operations from taking place. Figure S2 represents the Windows Defender logs, highlighting the severity of the ransomware and the status and the action taken.

4.2. Hardened Environment Testing Outcome

In the hardened environment, the download process for the MortalKombat ransomware was interrupted even before completion. This immediate halt can be seen in the log entries, as shown in Figure S3.

Such an immediate response can be attributed to the enhanced security layers in this configuration. The layered defenses, specifically features like Smart App Control, actively assess every file or application being introduced into the system. Given the intelligence of Smart App Control, it likely recognized the download as a potential threat even before the download was completed, thereby halting the process. Figure S4 illustrates the detection process of Smart App Control. The incident also highlights the efficacy of the integrated Threat Intelligence feeds that continuously provide the security infrastructure with real-time updates on emerging threats and attack vectors. This up-to-date knowledge enables the security components to proactively anticipate potential threats and respond swiftly.

Additionally, the utilization of Behavioral Analysis within the security framework contributed significantly to thwarting the attack. By establishing a baseline of normal system behavior, any deviations from this pattern trigger alerts. This technology effectively identified the ransomware's attempts to encrypt files and initiate unauthorized connections, even though the specific signature of the MortalKombat ransomware might not have been previously known. Therefore, in summary, the collaborative nature of these security layers, each complementing the other's strengths, collectively created a multi-faceted defense mechanism that not only intercepted the MortalKombat ransomware but also actively deterred its progress. This scenario exemplifies the crucial importance of a proactive and comprehensive security strategy, especially in the face of ever-evolving cyber threats.

The incident serves as a testament to the dedication of the cybersecurity team and the effectiveness of their strategic planning and technological implementation. A process creation log for sdbinst.exe (a Windows file used to address compatibility issues [40]) indicated that the Application Compatibility Database Installer was invoked. This is a typical behavior to ensure compatibility when new software or applications are introduced. The initiation of SecurityHealthHost.exe suggests the activation of the Windows Security Health Host. This service assesses the overall security and health of the system. Its activation here might be in response to the potential threat detected during the download. Another notable process creation was smartscreen.exe, which is the Windows Defender SmartScreen. This is an integral part of Windows' security infrastructure, designed to warn users about potentially malicious websites and downloads.

A registry value was set by SecurityHealthHost.exe. This could be a notification or alert pertaining to the detected threat, showcasing how the system responds internally by setting flags or notifications. The log entry showing a change in the file creation time for the ransomware by MsMpEng.exe (Windows Defender's core process) suggests that Defender interacted with the file, possibly during its scanning or quarantining process.

4.3. Cerber

4.3.1. Default Environment Outcome

Upon extracting the Cerber ransomware in the default environment, Windows Defender instantly sprang into action even if the user tried to execute Cerber before Windows Defender took action. The attached appendices (Figures S5 and S6) provide all the screenshots associated with these actions. The Windows log also indicates the Windows Defender behaviors in detecting the Cerber ransomware. Figure S7 shows the logs of Windows Defender when it detected the Cerber ransomware. The subsequent section outlines the main observations from testing and executing the Cerber ransomware variant on the Windows 11 Machine.

Key Observations:

Origin: The threat was detected on the test machine, meaning the antivirus did not rely on cloud-based checks for this detection.

Type: The detection type was "Concrete", which suggests that the antivirus software was certain about the malicious nature of the file.

Source: The detection source being "System" means the system processes or the operating system itself flagged it.

User: The threat was executed or encountered under the system authority, which means it might have had elevated permissions.

Process Name: The process that initiated or was infected by the ransomware is not known, as per the log.

Action Taken: The Windows Defender antivirus took the action to "Quarantine" the file, effectively isolating it to prevent any harm. No further actions were required from the user's end as the threat was neutralized. The operation was successful, as indicated by the error description.

While the threat was automatically quarantined, a potential improvement could be allowing the notification to await user acknowledgment, ensuring they are informed about the detected threat. Currently, the notification is temporary and might be missed by the user.

The Windows Defender protection history offers insights, but we must ensure users can easily access this information. It is essential to prioritize user experience while maintaining stringent security.

4.3.2. Hardened Environment Outcome

Upon attempting to download the Cerber ransomware in the hardened environment, the process was interrupted even before the completion of the download. This immediate halt can be attributed to the log entries, shown in Figure S8. The instant disruption is

indicative of the comprehensive defense mechanisms that the hardened configuration offers, with multiple layers working in tandem to ensure the highest level of security.

The in-transit disruption happened only if the user tried to download the malicious file using Microsoft Edge, which reveals that the security feature that came into play is part of Microsoft Edge. If the user tried to download a malicious file using the most popular browser, Google Chrome, he/she would be given the option to keep the file, like any other executable (exe) file (Figure S9).

In the above case, it was observed that Real-time protection, which actively detected the ransomware in the default environment, took a backseat in the hardened mode. Instead, the responsibility for ransomware detection transitioned to Smart App Control as soon as the user attempted to execute the application (Figure S10). This shift in roles between the two features is not just an incidental behavior but reflects a deeper strategy in Windows 11 Pro's defense mechanisms.

The move from the default to the hardened setting showcased a marked shift in the dynamics of Windows Defender's behavior. While Real-time protection served as the initial line of defense in the default setting, actively identifying and handling threats, the hardened environment saw Smart App Control stepping up. The logic behind this shift can be attributed to the enhanced security layers in the hardened setting. Even as Real-time protection continues its vigil, scanning files in real-time, Smart App Control operates more at the application execution juncture.

In sum, the collaboration and prioritization of Real-time protection and Smart App Control in the hardened setting underline Windows 11 Pro's adaptability and strategic defense. It is a clear demonstration of the OS's dedication to equipping users with flexible and potent protection against modern threats.

4.4. Hive

4.4.1. Default Environment Outcome

Upon attempting to download the Hive ransomware in the default environment, Windows Defender instantly detected the malicious content and did not even allow the completion of the download. This immediate detection signifies that Windows Defender identified the ransomware pattern in real-time as the file was being downloaded. Figures S11 and S12 show the Windows Defender logs in the default testing environment when attempting to download the Hive ransomware. The key testing observations from executing the Hive ransomware variant on Windows 11 can be summarized as follows:

Key Observations:

The notification indicating the threat is a system-generated alert and does not necessitate any user acknowledgment. It serves to inform the user about the blocked content but does not require any further action on their part. The identified threat is termed as "Trojan:Script/Sabsik.TE.A!ml". This classification indicates that Hive contains malicious scripts commonly associated with Trojan activities. The detection source, "Downloads and attachments", reinforces the idea that Defender halted the ransomware during the download process itself.

Name of the Threat: Trojan:Script/Sabsik.TE.A!ml

This specifies the type and variant of malware detected. In this case, it is a Trojan, which is malicious software that masquerades as legitimate software. This is a unique identifier assigned to this specific threat by Microsoft Defender.

Severity: Severe.

This indicates the potential harm the detected threat can cause to the system. "Severe" indicates it can inflict significant damage or unauthorized access.

Category: Trojan.

This confirms the type of malware detected.

Detection Origin: Internet.

This means the malware was detected during a download or while interacting with online content.

Detection Source: Downloads and attachments.

This indicates that the malware was detected as part of a downloaded file or an email attachment.

Action: Quarantine.

This is the action Defender took upon detecting the threat. "Quarantine" means the suspicious file was isolated to prevent it from causing harm.

Action Status: No additional actions required.

After quarantining the threat, Windows Defender determined no further actions were needed. The threat has been contained.

4.4.2. Hardened Environment Outcome

In the hardened configuration, the behavior observed was consistent with that of the default environment. Once again, Hive could not complete its download process due to Windows Defender's intervention. This outcome reinforces the robustness of the hardened configuration and its ability to block known threats even before they land on the system.

Key Observations:

Hive seems to be distinct in its immediate detection during download, unlike some other ransomware. This could be attributed to its signature or behavioral patterns being prominently recognized as malicious.

The utilization of a different browser, Chrome, resulted in a different user experience. Chrome presented a warning but still gave an option to proceed, suggesting that the blocking mechanism in Edge (Figure S13) is more rigid, possibly due to tighter integration with Windows Defender or the OS's inherent security features. This variation highlights the importance of browser-level security and its coordination with the OS.

The detection source being "Internet" in both logs implies that the ransomware was detected during its transit from the web server to the local machine, halting its download.

Hive's detection by Windows Defender during the download phase, irrespective of the configuration, is a testament to the potency of modern anti-malware solutions. Several factors could be contributing to this agile response:

Prominence: Hive's prominence in the cyber threat landscape might have led to its prioritization. Being a known ransomware variant, it is plausible that security solutions have been fine-tuned to detect it with heightened sensitivity.

Signature Recognition: Every piece of malware has a signature—a unique set of characteristics that define it. Hive's signature might be particularly distinct or overtly malicious, making it an easy target for real-time scanning engines like Windows Defender.

Behavioral Patterns: Modern cybersecurity solutions have evolved beyond mere signature-based detections. Behavioral analysis plays a significant role in identifying threats. There is a possibility that even during its initial download stages, Hive exhibits certain behaviors or patterns that act as red flags for detection systems.

Cloud-backed Analysis: The integration of cloud-backed analysis in security solutions like Windows Defender provides an additional layer of rapid threat detection. If Hive has been flagged, analyzed, and documented in a cloud repository recently, its details would be fresh in the database. This can lead to an almost instantaneous detection as soon as it begins downloading, given the real-time synchronization between the local machine and the cloud database. The prompt detection of Hive underscores the importance of keeping security solutions updated. As ransomware variants evolve, so do detection mechanisms, and the tussle continues. The immediate recognition of Hive serves as a reassuring indicator of Windows Defender's capabilities, especially when configured for maximum security. Table 5 below shows the testing results for the three said ransomware variants.

Table 5. Testing comparison between different ransomware variants.

MortalKombat Ransomware		**Cerber Ransomware**		**Hive Ransomware**	
Default	**Hardened**	**Default**	**Hardened**	**Default**	**Hardened**
After unzipping the MortalKombat ransomware, Windows 11 takes immediate quarantine action, and the logs indicate the following actions: - Name of the Threat: Trojan:Win32/Vindor!pz - Severity: Severe - Action: Quarantine - Action Status: No additional action required Despite the user potentially attempting to execute the ransomware post-extraction, Windows Defender ensured that the ransomware remained non-functional.	- The download process was interrupted - Proactively anticipated a potential ransomware threat - Behavioral Analysis effectively identified the ransomware's attempts to encrypt files and initiate unauthorized connections, even though the specific signature of the MortalKombat ransomware might not have been previously known.	Upon extracting the Cerber ransomware in the default environment, Windows Defender instantly took the following actions: - Name of the Threat: Ransom:Win32/Avaddon.P!MSR - Severity: Concrete - Action: Quarantine - Action Status: No further action is required Even if the user tries to execute Cerber, Windows Defender takes prompt blocking action.	- Upon attempting to download the Cerber ransomware in the hardened environment, the downloading process was interrupted even before the completion of the download. - Smart App Control took immediate action as soon as the user attempted to execute the Cerber ransomware.	Upon attempting to download the Hive ransomware in the default environment, Windows Defender instantly detected the malicious content and did not even allow the completion of the download. - Name of the Threat: Trojan:Script/Sabsik.TE.A!ml - Severity: Severe - Category: Trojan - Action: Quarantine - Action Status: No further action is required Defender halted the ransomware during the download process itself.	- Hive could not complete its download process due to Windows Defender's intervention. This outcome reinforces the robustness of the hardened configuration and its ability to block known threats even before they land on the system. - Hive seems to be distinct in its immediate detection during download, unlike some other ransomware. This could be attributed to its signature or behavioral patterns being prominently recognized as malicious.

5. Discussion

The testing of the MortalKombat, Hive, and Cerber ransomware variants on Windows 11 Pro offers a comprehensive insight into the operating system's defense mechanisms, both in default and hardened configurations. Here, we provide a discussion of the responses to these ransomware variants to understand the overall robustness and strategy of Windows 11 Pro's security features.

The hardened environment demonstrated Smart App Control's dominance in ransomware detection, even overshadowing Real-time protection. When the ransomware variants were introduced, Smart App Control, backed by its cloud intelligence, probably identified the file's hash or metadata matching with known threats, resulting in an immediate halt of the download.

While Real-time protection is designed to scan and detect malicious files actively, the Smart App Control feature is more reactive, awaiting an execution attempt. The advantage is that even if a user momentarily disables Real-time protection, Smart App Control remains vigilant.

In essence, the behavior exhibited against the ransomware variants reinforces the strategic interplay between Real-time protection and Smart App Control, offering users a robust and dynamic defense mechanism.

- Detection Timing:

Detection happened after unzipping in the default and in pre-download completion in the hardened environment.

- Security Feature Engagement:

In the default setting, Real-time protection was the primary defense mechanism. In the hardened mode, Smart App Control took the reins, reflecting the strategic shift in defense based on the configuration.

- User Interaction and Notifications:

Both variants triggered notifications which, though temporary, were effective in informing the user about the detected threat.

- Sysmon Observations:

Sysmon logs revealed that various system processes were invoked, reflecting the operating system's response to a potential threat.

- Adaptability of Defense Mechanisms:

The testing of these ransomware variants showcased Windows 11 Pro's dynamic response based on the configuration. While the default setting relies heavily on Real-time protection, the hardened mode introduces a layered defense strategy, emphasizing the role of Smart App Control.

While the threat was automatically quarantined, a potential improvement could be allowing the notification to await user acknowledgment, ensuring they're informed about the detected threat. Currently, the notification is temporary, which might be missed by the user.

Relevance to End-Users: The Windows Defender protection history offers insights, but we must ensure users can easily access this information. It is essential to prioritize user experience while maintaining stringent security.

The hardened configuration in Windows 11 Pro acknowledges that many modern threats are not solely dependent on the presence of malicious files, but rather on the behavior of applications and processes. Attackers often exploit legitimate applications to execute malicious actions, making it challenging for traditional antivirus methods to detect such activities solely based on file signatures or patterns.

Interpreting Windows Defender's Defensive Dynamics

Several key observations and patterns were discerned. Windows Defender showcased its efficacy in both default and hardened configurations, effectively neutralizing the ransomware attempts and underscoring its robust capability to identify and combat a range of threats. The juxtaposition between the default and hardened configurations was enlightening. While the default configuration leaned heavily on Real-time protection, detecting and quarantining ransomware either post-download or during execution attempts, the hardened environment exhibited more proactive defense mechanisms. The download processes were often interrupted, a testament to the layered security approach in this advanced setting. An integral part of the analysis was recognizing the role of browser-based protections. The granular insights from the Sysmon logs offered an in-depth view into the processes and system alterations instigated by ransomware and the corresponding responses triggered by Windows Defender. In many scenarios, these logs displayed an absence of malicious activity, a clear indication of Windows Defender's swift and effective interventions. A fascinating dynamic was evident in the interplay of Windows Defender features. Particularly in the hardened setting, while Real-time protection remained the frontline defense in the default mode, Smart App Control assumed a more dominant role during the application execution phase. Conclusively, this comprehensive exploration underscores that Windows 11 Pro's security features, irrespective of default or hardened configurations, present a formidable defense against ransomware threats.

6. Conclusions

The digital age has brought with it a plethora of opportunities, but it has also introduced numerous challenges, not least of which is the threat of ransomware. This paper set out to explore the capabilities of Windows 11 Pro in mitigating well known ransomware variants threats and to evaluate its embedded security features thoroughly. Through systematic testing in both default and hardened configurations, this research has shown that while Windows 11 Pro offers significant defenses against ransomware, there is always room for improvement. As ransomware evolves, so too must the defenses against it. The security features in Windows 11 Pro, such as Controlled Folder Access and Smart App Control, provide robust protection, but their efficacy is closely tied to user understanding and interaction. Thus, striking a balance between user-friendly features and robust security measures remains a challenge. An important takeaway from this study is the realization that security is not just about having advanced features; it is about the constant adaptation and updating of these features in response to emerging threats. Moreover, user awareness and behavior play a pivotal role in system security. Even the most sophisticated features can be compromised if not used correctly or if users are not vigilant.

Supplementary Materials: The following supporting information can be downloaded at: https://www.mdpi.com/article/10.3390/app14083520/s1, Figure S1. Evident of detecting the MortalKombat ransomware by Windows Defender; Figure S2. Windows Defender logs after detection the MortalKombat variant; Figure S3. Windows Defender logs showing the detection of the MortalKombat ransomware download; Figure S4. Smart App Control popup when attempting to run the MortalKombat executable; Figure S5. Windows Defender detecting Cerber upon extraction; Figure S6. Windows Defender prevented the user from manually executing the Cerber exe; Figure S7. Windows Defender logs showing the detection of the Cerber ransomware; Figure S8. The Windows Defender logs entries in the hardened environment indicating the detection of Cerber ransomware; Figure S9. Chrome giving the user the option to allow executables; Figure S10. Smart App Control popup when attempting to run the Cerber executable; Figure S11. Windows Defender Logs showing the detection of Hive Ransomware in the Default testing environment; Figure S12. Windows Defender Logs showing action taken to protect local machine from Hive Ransomware; Figure S13. Hive Ransomware being detected in transit in Microsoft Edge browser.

Author Contributions: Conceptualization, A.B. and H.U.R.; methodology, A.B. and Y.M.A.-A.; software, Y.M.A.-A.; validation, Y.M.A.-A., A.B. and H.U.R.; formal analysis, A.B. and H.U.R.; investigation, Y.M.A.-A.; resources, A.B. and H.U.R.; data curation, Y.M.A.-A.; writing—original draft preparation, Y.M.A.-A., A.B. and H.U.R.; writing—review and editing, A.B. and H.U.R.; visualization, Y.M.A.-A., A.B. and H.U.R.; supervision, A.B.; project administration, A.B.; funding acquisition, Y.M.A.-A., A.B. and H.U.R. All authors have read and agreed to the published version of the manuscript.

Funding: We are extremely thankful to the Qatar National Library for supporting the Open Access publication charges of this publication.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: The original contributions presented in the study are included in the article/supplementary material, further inquiries can be directed to the corresponding author.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Lavieille, P.; Atlas, I.A.H. IsoEx: An explainable unsupervised approach to process event logs cyber investigation. *arXiv* **2023**, arXiv:2306.09260.
2. Eren, M.E.; Bhattarai, M.; Rasmussen, K.; Alexandrov, B.S.; Nicholas, C. MalwareDNA: Simultaneous Classification of Malware, Malware Families, and Novel Malware. In Proceedings of the 2023 IEEE International Conference on Intelligence and Security Informatics (ISI), Charlotte, NC, USA, 2–3 October 2023; pp. 1–3.
3. Aldauiji, F.; Batarfi, O.; Bayousef, M. Utilizing cyber threat hunting techniques to find ransomware attacks: A survey of the state of the art. *IEEE Access* **2022**, *10*, 61695–61706. [CrossRef]
4. Razaulla, S.; Fachkha, C.; Markarian, C.; Gawanmeh, A.; Mansoor, W.; Fung, B.C.; Assi, C. The Age of Ransomware: A Survey on the Evolution, Taxonomy, and Research Directions. *IEEE Access* **2023**, *11*, 40698–40723. [CrossRef]
5. Li, Y.; Liu, Q. A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments. *Energy Rep.* **2021**, *7*, 8176–8186. [CrossRef]
6. Numminen, A. Windows Technical Hardening against the Most Prevalent Threats. 2023. Available online: http://urn.fi/URN:NBN:fi:jyu-202305293330 (accessed on 19 December 2023).
7. Humayun, M.; Jhanjhi, N.; Alsayat, A.; Ponnusamy, V. Internet of things and ransomware: Evolution, mitigation and prevention. *Egypt. Inform. J.* **2021**, *22*, 105–117. [CrossRef]
8. Ryan, M. *Ransomware Revolution: The Rise of a Prodigious Cyber Threat*; Springer: Berlin/Heidelberg, Germany, 2021.
9. McIntosh, T.; Kayes, A.; Chen, Y.-P.P.; Ng, A.; Watters, P. Ransomware mitigation in the modern era: A comprehensive review, research challenges, and future directions. *ACM Comput. Surv. CSUR* **2021**, *54*, 1–36. [CrossRef]
10. O'Kane, P.; Sezer, S.; Carlin, D. Evolution of ransomware. *IET Netw.* **2018**, *7*, 321–327. [CrossRef]
11. Lee, W. *Malware and Attack Technologies Knowledge Area Issue*; CyBOK: Bristol, UK, 2021.
12. Moussaileb, R.; Cuppens, N.; Lanet, J.-L.; Bouder, H.L. A survey on windows-based ransomware taxonomy and detection mechanisms. *ACM Comput. Surv. (CSUR)* **2021**, *54*, 1–36. [CrossRef]
13. Gittins, Z.; Soltys, M. Malware persistence mechanisms. *Procedia Comput. Sci.* **2020**, *176*, 88–97. [CrossRef]
14. Kim, G.; Kim, S.; Kang, S.; Kim, J. A method for decrypting data infected with hive ransomware. *J. Inf. Secur. Appl.* **2022**, *71*, 103387. [CrossRef]
15. Kurniawan, A.; Riadi, I. Detection and analysis cerber ransomware based on network forensics behavior. *Int. J. Netw. Secur.* **2018**, *20*, 836–843.
16. Jeffrey, C. Hackers Hit US Windows Systems with "Mortal Kombat" Ransomware. Available online: https://www.techspot.com/news/97608-hackers-hit-us-windows-systems-mortal-kombat-ransomware.html (accessed on 4 December 2023).
17. Jethva, B.; Traoré, I.; Ghaleb, A.; Ganame, K.; Ahmed, S. Multilayer ransomware detection using grouped registry key operations, file entropy and file signature monitoring. *J. Comput. Secur.* **2020**, *28*, 337–373. [CrossRef]
18. Wright, R. Bitdefender Releases Decryptor for MortalKombat Ransomware. Available online: https://www.techtarget.com/searchsecurity/news/365531919/Bitdefender-releases-decryptor-for-MortalKombat-ransomware (accessed on 4 December 2023).
19. Kara, I.; Aydos, M. Static and dynamic analysis of third generation cerber ransomware. In Proceedings of the 2018 International Congress on Big Data, Deep Learning and Fighting Cyber Terrorism (IBIGDELFT), Ankara, Turkey, 3–4 December 2018; pp. 12–17.
20. Adamov, A.; Carlsson, A. The state of ransomware. Trends and mitigation techniques. In Proceedings of the 2017 IEEE East-West Design & Test Symposium (EWDTS), Novi Sad, Serbia, 29 September–2 October 2017; pp. 1–8.
21. Microsoft. Virtualization-Based Security (VBS). Available online: https://learn.microsoft.com/en-us/windows-hardware/design/device-experiences/oem-vbs (accessed on 4 December 2023).

22. Microsoft. Enable Virtualization-Based Protection of Code Integrity. Available online: https://learn.microsoft.com/en-us/windows/security/hardware-security/enable-virtualization-based-protection-of-code-integrity (accessed on 1 December 2023).
23. Microsoft. Windows Hello Biometrics in the Enterprise. Available online: https://learn.microsoft.com/en-us/windows/security/identity-protection/hello-for-business/hello-biometrics-in-enterprise (accessed on 15 November 2023).
24. Microsoft. Secure Boot. Available online: https://learn.microsoft.com/en-us/windows-hardware/design/device-experiences/oem-secure-boot (accessed on 21 November 2023).
25. Microsoft. New Security Features for Windows 11 Will Help Protect Hybrid Work. Available online: https://www.microsoft.com/en-us/security/blog/2022/04/05/new-security-features-for-windows-11-will-help-protect-hybrid-work/ (accessed on 1 December 2023).
26. Microsoft. Understanding Hardware-Enforced Stack Protection. Available online: https://techcommunity.microsoft.com/t5/windows-os-platform-blog/understanding-hardware-enforced-stack-protection/ba-p/1247815 (accessed on 12 December 2023).
27. Microsoft. Windows 11: The Optimization and Performance Improvements. Available online: https://techcommunity.microsoft.com/t5/microsoft-mechanics-blog/windows-11-the-optimization-and-performance-improvements/ba-p/2733299 (accessed on 30 November 2023).
28. Khan, I.U.K.U.; Ouaissa, M.; Ouaissa, M.; Abou El Houda, Z.; Ijaz, M.F. *Cyber Security for Next-Generation Computing Technologies*; CRC Press: Boca Raton, FL, USA, 2024.
29. Pogonin, D.; Korkin, I. Microsoft Defender Will Be Defended: MemoryRanger Prevents Blinding Windows AV. *arXiv* **2022**, arXiv:2210.02821.
30. Santos, D. Comparison of Paid Subscription vs. Freeware Software on Antivirus Program. 2021. Available online: http://hdl.handle.net/10790/6828 (accessed on 18 December 2023).
31. Microsoft. Stay Protected with Windows Security. Available online: https://support.microsoft.com/en-us/windows/stay-protected-with-windows-security-2ae0363d-0ada-c064-8b56-6a39afb6a963 (accessed on 8 November 2023).
32. Microsoft. Cloud Protection and Sample Submission at Microsoft Defender Antivirus. Available online: https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/cloud-protection-microsoft-antivirus-sample-submission?view=o365-worldwide (accessed on 2 December 2023).
33. Microsoft. Exploit Protection Reference. Available online: https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/exploit-protection-reference?view=o365-worldwide (accessed on 29 November 2023).
34. Microsoft. Windows Firewall: New and Upcoming Features for 2023. Available online: https://techcommunity.microsoft.com/t5/windows-events/windows-firewall-new-and-upcoming-features-for-2023/ev-p/3971637 (accessed on 12 November 2023).
35. Microsoft. What Is Smart App Control? Available online: https://support.microsoft.com/en-au/topic/what-is-smart-app-control-285ea03d-fa88-4d56-882e-6698afdb7003 (accessed on 5 November 2023).
36. Microsoft. Protect Your PC from Potentially Unwanted Applications. Available online: https://support.microsoft.com/en-us/windows/protect-your-pc-from-potentially-unwanted-applications-c7668a25-174e-3b78-0191-faf0607f7a6e (accessed on 16 November 2023).
37. Microsoft. Kernel DMA Protection (Memory Access Protection) for OEMs. Available online: https://learn.microsoft.com/en-us/windows-hardware/design/device-experiences/oem-kernel-dma-protection (accessed on 23 November 2023).
38. Microsoft. Device Encryption in Windows. Available online: https://support.microsoft.com/en-us/windows/device-encryption-in-windows-ad5dcf4b-dbe0-2331-228f-7925c2a3012d (accessed on 16 November 2023).
39. Microsoft. Enable Exploit Protection. Available online: https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/enable-exploit-protection?view=o365-worldwide (accessed on 1 December 2023).
40. Microsoft. Using the Sdbinst.exe Command-Line Tool. 2023. Available online: https://learn.microsoft.com/en-us/windows/deployment/planning/using-the-sdbinstexe-command-line-tool (accessed on 2 January 2024).

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.