Re-Evaluating the Necessity of Third-Party Antivirus Software on Windows Operating System

Faisal A. Garba[1], Rosemary M. Dima[2], A. Balarabe Isa[3], A. Abdulrazaq Bello[4], A. Sarki Aliyu[5], F. Umar Yarima[6], S. Abbas Ibrahim[7]

[1,3,5,6,7]Sa'adatuRimi College of Education, Kano, Nigeria
[2]Federal University Dutsinma, Katsina State, Nigeria
[4]Federal Polytechnic, Bauchi, Nigeria

Emails: alifa2try@gmail.com; rocinta976@gmail.com ; balarabesadeeq@gmail.com; ibnahmadbello@gmail.com; sarkialu@gmail.com; farroukhyarima@gmail.com ; shazaliabbas82@gmail.com

Abstract

There is a general assumption that one must purchase costly antivirus software products to defend one's computer system. However, if one is using the Windows Operating System, the question that arises is whether one needs to purchase antivirus software or not. The Windows operating system has a market share of 31.15% behind Android with a market share of 41.56% worldwide amongst all the operating systems. This makes Windows a prime target for hacking due to its large user base. Windows 11 a recent upgrade to the Windows operating system has claimed to have taken its security to the next level. There is a need to evaluate the capability of the Windows 11 default security against antivirus evasion tools. This research investigated the capability of Windows 11 default security by evaluating it against 6 free and open-source antivirus evasion tools: TheFatRat, Venom, Paygen, Defeat Defender, Inflate and Defender Disabler. The criteria for the selection of the antivirus evasion tools were free and open source and recently updated. A research lab was set up using Oracle VirtualBox where two guest machines were installed: a Windows 11 victim machine and the Kali Linux attacking machine. The antivirus evasion tools were installed on the Kali Linux machine one at a time to generate a malware and pass it to the victim machine. Apache web server was used in holding the malicious sample for the Windows 11 victim machine to download. A score of 2 was awarded to an antivirus evasion tool that successfully evaded the Windows 11 security and created a reverse connection with the attacking machine. From the research results: TheFatRat had a 25% evasion score, Venom had 20% while the rest had a 0% evasion score. None of the payloads generated with the antivirus evasion tools was able to create a connection with the Kali Linux attacking machine. The research results imply that the default Windows 11 security is good enough to stand on its own. A third-party antivirus solution will only supplement the already good protection capability of Windows 11.

Keywords: malware; antivirus; evasion; Windows.

1. Introduction

Antivirus applications are especially created to neutralize computer infections through malicious software detection, removing the malicious application and disinfecting the computer. Malicious applications can be grouped into Trojans, viruses (infectors), rootkits, droppers, worms among others. Antivirus software is aimed at providing much better protection than the security provided by

Doi : https://doi.org/10.54216/JCIM.090105
Received: April 11, 2022 Accepted: July 17, 2022

the underlying operating systems such as Windows or Mac OS X. Antivirus first objective is prevention and when that fails the antivirus (AV) application will then resort to disinfecting the infected program or wiping away the malicious application from the computer [1]. There is a general assumption that one must purchase costly antivirus software products to defend one's computer system. However, if one is using the Windows Operating System, the question that arises is whether one needs to purchase antivirus software or not [2]. A research was performed by [2] to investigate the necessity of using third party antivirus solution on Windows operating system. Firstly, [2] examined the performance efficiency of standard user activities to find out if there was a negative or positive impact on the computer performance arising from the use of third-party antivirus software in comparison with the default Windows security. Secondly, [2] investigated the detection ability of selected antivirus by examining the documentation that relates to the selected antivirus software. In this research, we examine the malware detection capability of the default security of Windows operating system. This is achieved by examining the malware detection capability of Windows 11 operating system against malwares generated via free antivirus evasion tools. Antivirus evasion tools are software that seeks to make malware more effective by adding antivirus evasion feature to the generated malicious sample. The antivirus evasion tools selected are: TheFatRat, Venom, Defeat Defender, Paygen, Inflate and Defender Disabler. These tools are those that have been recently updated as seen in Table 1. In [3] Veil Framework, TheFatRat, Shellter, Unicorn, Venom, Phantom evasion, Onelinepy, MSFMania and Paygen were evaluated against Bitdefender antivirus solution. In this research we omitted Veil Framework, Shellter, Unicorn, Phantom Evasion, Onelinepy and MSFMania as the tools have not been kept up to date.

.

2. Literature Review

Windows 11

Windows is a graphical user interface operating system created by Microsoft. It gives users the ability to manipulate files, execute software, play games, watch videos and provides connectivity to the Internet [4]. The Windows OS has a market share of 31.15% behind Android with a market share of 41.56% [5] worldwide amongst all the operating systems. Microsoft launched Windows 11 on October 5, 2021, as a free upgrade to Windows 10 [6]. Windows 11 is available for download from Microsoft[1]. Windows 11 is also available as a free evaluation copy in the form of virtual machine[2]. Zero trust capability, hardware-based isolation, encryption, and malware prevention features are turned on by default in Windows 11. The option for passwordless login is another design feature added to Windows 11. Computers must have at least an 8th generation or newer Intel Core processor or an AMD Ryzen 2000 or newer processor, have 4GB of RAM, a minimum of 64GB of storage and be compatible with DirectX 12 or later with WDDM 2.0 driver to run Windows 11. Computers must be equipped with TPM 2.0 security chip to fully access Windows 11 security upgrades. A TPM chip is a secure crypto processor that runs cryptographic operations. The chip includes a physical security mechanism that makes it tamper-resistant, and malware cannot tamper with the security functions of the TPM [7].

Windows 11 Security Features

a. Zero Trust Security

The hardware and silicon-assisted security features of Windows 11 including Trusted Platform Module (TPM) 2.0, firmware and identity protection, direct memory access and memory integrity protection are built on the principles of zero trust to assist in safeguarding core parts of the Operating System (OS) and user's credentials as the device is turned on. Since attackers have shifted their attention to hardware, Microsoft proposed the use of Microsoft Pluton Security Processor to counter that. Pluton is a Microsoft's security processor that is co-designed with AMD [8]. Pluton possesses numerous major capabilities that arise from its direct incorporation into the Central Processing Unit (CPU) and the Operating System (OS). Firstly, like other windows component,

[1] https://www.microsoft.com/software-download/windows11
[2] https://developer.microsoft.com/en-us/windows/downloads/virtual-machines/

Doi : https://doi.org/10.54216/JCIM.090105
Received: April 11, 2022 Accepted: July 17, 2022

Pluton is the only security processor that is kept constantly up to date with security and functionality updates. Pluton does not require enterprises to take the traditional measure of firmware update which makes it easier to stay secure. Secondly, Pluton is enhanced for the best performance and reliability in Windows 11 since the Pluton firmware is created by the same Windows team that developed the features that uses it like Windows Hello and Bitlocker. A first-rate penetration testing alongside external bug bounty program is carried out on Pluton to ensure it remains secure. Pluton direct integration with the CPU empowers it to provide protection against physical attacks [9].

b. Smart App Control Security

Smart App Control is another key improvement to the Windows 11 security model that prevents users from executing malwares on Windows devices that by default block untrusted or unsigned applications [9]. Smart App Control is significant security improvement for Windows 11 that was integrated with the OS at the process level to block users from running malware using code signing coupled with an AI model [10]. The Smart App control was extended to the core of the OS at the process level in addition to the previous built-in browser protections. The new Smart App Control only allows processes to be executed that are predicted to be safe based on either code certificates or an AI model for application trust within the Microsoft cloud. Using the latest threat intelligence that make available trillions of signals, the model inference occurs 24 hours a day. Windows 11 check a new application core signing and core features against this model to ensure only known safe applications are executed [9]. Smart App Control uses similar techniques as SmartScreen protections features inbuilt in Microsoft Edge. While SmartScreen utilizes several alerts to inform you that a website might attack your computer through malware or a phishing attack, Smart App Control is inbuilt into the Windows 11 operating system to provide similar protections against malicious apps one may download without knowing if they are safe or not. Each new app that is executed on Windows 11 is checked against this threat intelligence to find out if it will be potentially harmful or not [8].

c. Increased account and credential security

The Microsoft Defender SmartScreen in Windows 11 was equipped with phishing detection and protection to protect users from phishing attacks by spotting and notifying users when they are logging their Microsoft credentials into a malicious application or a compromised site. This makes Windows 11 the world's first OS with phishing safeguard built directly into the platform and shipped out-of-box to end users. Credential theft attack techniques like pass-the-hash or pass-the-ticket are prevented in Windows 11 using hardware-backed virtualization-based security. Malware is prevented from accessing system secrets even if its process is executed using admin privileges [9]. Microsoft has blocked over 25.6 billion Azure Active Directory brute force authentication attacks and was able to intercept more than 35.7 billion phishing emails before landing in the recipients' inboxes in 2021 alone, as a validation of SmartScreen's effectiveness [10].

d. Personal Data Encryption adds a Second Layer of Security for Personal Data

In Windows 11, a platform for use by applications and IT called Personal Data Encryption safeguards user files and data when no one is logged into the device. Users must first authenticate with Windows Hello for Business to have access to the data thereby linking data encryption keys with the user's passwordless details. In the event that a device is lost or stolen, the device will be more resistant to attack and sensitive data will have gotten additional layer of protection. Drivers with known vulnerabilities are blocked automatically in Windows 11 with vulnerable driver blocklist that uses Windows Defender Application Control (WDAC). This hardens the Windows system against any third-party driver with any of these characters:

i. known vulnerability that attackers can abuse to escalate privilege in the Windows kernel.

ii. malicious traits or certificates used to sign malware.

iii. behaviors that are not necessarily malicious but frustrate the Windows Security Model and could be abused by attackers to escalate privileges[10].

e. Protect users from themselves with Config Lock

Config Lock is a feature already in Windows 11 that monitors registry keys via mobile device management (MDM) policies to aid in making sure devices in a network abide by industrial and

Doi : https://doi.org/10.54216/JCIM.090105
Received: April 11, 2022 Accepted: July 17, 2022

company security baselines. Config Lock automatically revert a system to IT-desired state in seconds, upon detection of changes in registry keys [9]. It uses MDM policies to examine and revert registry keys to the original states if users are altering them, likely rendering their devices insecure and exposed to attacks [10].

f. Block vulnerable drivers by default with Hypervisor-Protected Code Integrity (HVCI)

HVCI feature stop attackers from injecting malware and make sure that all drivers loaded onto the OS are signed and trustworthy. The Microsoft Vulnerable and Malicious Driver Reporting Center enable Windows to automatically block known vulnerable drivers using data from the wider security community. Windows Defender Application Control (WDAC) is used by the Microsoft vulnerable driver blocklist to assist in preventing Advanced Persistent Threats (APTs) and ransomware attacks exploiting known vulnerable drivers. To prevent these drivers from being abused, the kernel blacklisting feature blocks their load in the Windows kernel. In devices running HVCI or Windows SE, blocklist is enabled by default. Moreover, the feature can be turned on within the Windows Security App [9].

Antivirus Evasion

To bypass a single or multiple antivirus software, malware writers, penetration testers and vulnerability researchers use antivirus evasion techniques. This enables the malware to perform its intended actions on the target machine without being hampered. Dynamic and static evasion techniques are two classes of evasion approaches used by malware writers. Static involves bypassing detection based on antivirus signature scanning algorithms. Dynamic evasion technique means evading detection that seeks to detect the behavior of malware sample when it is executing. Cyclic redundancy check algorithms (CRCs), fuzzy hashing techniques, modifying the binary contents of the sample to yield a different cryptographic hash are some of the techniques employed for static evasion. Dynamic evasion involves writing a malware that modify its behavior when it realizes that its being executed in a sandbox or antivirus emulator, or it could run an instruction that the emulator does not support. It could also attempt to get out of the sandbox or the "safe execution" environment that is set up by the antivirus software so it can execute the malicious programs without being monitored [1]. Antivirus evasion tools are used by attackers in the weaponization stage of the Cyber Kill Chain [11].

Antivirus Evasion Tools

The selected antivirus evasion tools used for the research are TheFatRat, Venom, Defeat-Defender-V1.2, Paygen, Inflate and Defender Disabler. The criteria for the antivirus selection of the tools are 1. recently updated tools and 2. free and open-source tools. These are presented in Table 1.

TheFatRat

TheFatRat is an antivirus evasion tool developed by Edo Maland which compiles malwares with well-known payloads targeting Linux, Windows, Mac, and Android operating systems. Backdoors and payloads which can bypass most antiviruses can be easily created with the TheFatRat [12, 13]. Since by changing a payload to C language, antivirus will not flag it as suspicious, TheFatRat yields a C language payload [14].

Venom

VENOM – Metasploit Shellcode generator, compiler, and listener tool. The script uses MSF Venom (Metasploit) to yield shellcode in various formats: C, Python, Ruby, DLL, MSI, HTA-PSH and inject the shellcode created into one function such as Python. The Python function will then run the shellcode in RAM and employ compilers like: GNU Cross Compiler (GCC), mingw32 or pyinstaller to generate an executable file. It then proceeds to launch a multi-handler to receive the remote connection (reverse shell or meterpreter session). Venom is obtainable from its Github repository[3]. The Venom framework is an innovative work of Pedro Nobrega and Chaitanya Haritash, who worked to a great extent to simplify shellcode and backdoor generation for various operating systems [15].

Defeat-Defender-V1.2

[3] https://github.com/r00t-3xp10it/venom

Doi : https://doi.org/10.54216/JCIM.090105
Received: April 11, 2022 Accepted: July 17, 2022

A powerful batch script that totally compromise Windows Defender protection and proceed to evade tamper protection goes by the name Defeat Defender V1.2[4]. Tamper protection prevents security settings from being modified through applications and ways such as configuring settings in Registry Editor on Windows device, altering settings through PowerShell cmdlets, and editing or removing security settings through Group Policy. Tamper protection achieved this by basically locking Microsoft Defender Antivirus to its secure, default values. Tamper protection is available for devices that are running one of the following versions of Windows [16]:

a. Windows 11

b. Windows 11 Enterprise multi-session

c. Windows 10

d. Windows 10 Enterprise multi-session

e. Windows Server 2022

f. Windows Server 2019

g. Windows Server, version 18.03 or later

h. Windows Server 2016

i. Windows Server 2012 R2

Exploiting the Windows feature which enables the download of any batch file from external network, Defeat-Defender-V1.2 first break down all security and defenders using the admin command prompt and then proceeds to download payloads from the target web server and run it without experiencing any issue.

PayGen

This is a fully undetectable payload creation tool obtainable from its Github[5] repository. Features of PayGen include automated payload creation with MSFVenom, creation of a handler.rc file, undetectable stop security services, killing of AV processes, auto port forwarding via Ngrok, automatic executable signing and generation of android payloads.

Inflate

Inflate[6] is a quick and a basic script that can be used to inflate binary files by padding them out with null bytes. To operate it, just run the script with the name or location of the binary you want to inflate plus an integer value to inflate it by. It has been used by the author to successfully evade AV and EDR solutions since many security vendors simply do not check large files.

Defender Disabler

Defender Disabler[7] is a simple tool that disables Windows Defender, task manager, registry tools, CMD, bypass tamper protection among others. "It destroys Windows Defender so hard that it doesn't even know it exists anymore". It disables the following Windows protection features and lots more others:

a. PUA Protection

b. Automatic Sample Submission

c. Windows Firewall

[4] https://github.com/swagkarna/Defeat-Defender-V1.2.0
[5] https://github.com/youhacker55/PayGen
[6] https://github.com/nayjones/inflate.py

[7] https://github.com/Rdimo/Defender-disabler

Doi : https://doi.org/10.54216/JCIM.090105
Received: April 11, 2022 Accepted: July 17, 2022

d. Windows Smart Screen (Permanently)

e. Windows Defender Security Center

f. Defender Tamper Protection

g. Defender Real-time protection

h. Defender Anti-spyware

i. Defender MpEnablePlus

j. Defender Behavior Monitoring

k. Defender IOAVProtection

l. Defender OnAccessProtection

m. Defender RealtimeMonitoring

n. Defender RoutinelyTakingAction

o. Defender Notification

Some ways of compiling the batch file to a.exe have been outlined on the Github page.

Table 1: Selected Antivirus Evasion Tools

Tool	Language of development	Last update	Date downloaded	Version
TheFatRat	C, C++, RenderScript, Shell, Python and Ruby.	20/02/2022	13/06/2022	1.9.8
Venom	Shell, PowerShell, Python, HTML, Ruby, C and others.	20/09/2021	02/07/2022	1.0.17
Defeat-Defender-V1.2	Batchfile, Python, AutoHotkey	21/06/2022	09/07/2022	1.2
PayGen	Python, C#, PowerShell, HTML, VBScript.	30/03/2022	11/07/2022	
Inflate	Python	09/04/2022	12/07/2022	
Defender Disabler	Batchfile	13/04/2022	12/07/2022	

Doi : https://doi.org/10.54216/JCIM.090105
Received: April 11, 2022 Accepted: July 17, 2022

Review of Related Works

In [3] evaluation of antivirus evasion tools: Veil Framework, TheFatRat, Shellter, Unicorn, Venom, Phantom Evasion, Onelinepy, MsfMania and PayGen against Bitdefender antivirus solution was carried out. Phantom Evasion, Onelinepy and PayGen had the highest evasion score of 50% each. Shellter and Unicorn had the least evasion score of 0%. The evaluation procedure employed by [3] tested not only for evasion but the capability of the generated malware sample to create a remote connection.

A comparison of pyRAT and Phantom antivirus tools was conducted by [17] on Windows platform. PyRAT and Phantom are antivirus evasion tools that produce executable payloads that are used alongside Metasploit to compromise a computer system. PyRAT had the highest evasion score of 67% while Phantom had an evasion score of 50%. Avira, Bitdefender, Avast, Kaspersky, AVG and Panda were the antivirus product tested against.

A comparative performance analysis of antivirus software - Avast, Kaspersky, Bitdefender and Norton was carried out by [18]. Scanning methods –quick scan, full scan and custom scans were employed as parameters to test the effectiveness of the antivirus software. [18] did not single out any antivirus application as the best. Each of the antivirus application performed well under various metrics such as: malware detection rate, memory usage of the installed antivirus and interface launch time.

A research was carried out by [19] to increase the understanding of the effectiveness of antiviruses in real life scenarios by evaluating the operating mode that is the response time and detection regression and also creating a broader characterization of current antiviruses' modes of operation. In characterization, they considered distinct file types, operating systems, datasets, and time frames. This was achieved with 28,875 distinct samples collected from two malware sources and submitted to the VirusTotal (VT) service over a 30-day period. For each day, the submitted samples' detection rates and assigned labels were collected, resulting in a total of more than 1 million distinct VT submissions. A longitudinal evaluation of AVs was conducted on the samples based on their operations – detection rates, in real-life scenarios, with their strengths and weaknesses highlighted. The research carried out by [19] resulted in the following findings: phishing contexts were particularly a challenge for all AVs as they made malicious web page detectors less effective than malicious file detectors. Generic procedures employed by antivirus were insufficient to ensure broad detection coverage, they had lower detection rates for datasets (e.g., country-specific) than for those with world-wide collected samples. Detection rates were unstable since all the antivirus presented detection regression effects after scans in different time frames using the same dataset. Antivirus long response times in delivering new signatures/heuristics created a significant attack opportunity window within the first 30 days after a malicious binary was identified.

Evaluation of the effectiveness of antivirus evasion tools on Windows platform was carried out by [20]. Avet, Veil 3.0, PeCloak.py, Shellter and FatRat. Avet and PeCloak.py emerged the best antivirus evasion tools.

Bitdefender, Kaspersky, Avast, AVG and Avira antivirus solutions were evaluated by [21]. The free editions of Bitdefender, Avast and AVG were used while the commercial edition of Kaspersky and Avira were used. These antiviruses selected occupied the five top places of AV comparatives, an antivirus evaluation site. Reference [21] evaluated the antiviruses against TheFatRat, Phantom Evasion, Hercules, Sidestep and Veil Framework (version 3.1.14). Phantom-Evasion emerged the best with evasion score of 65%. Phantom-Evasion crashed Avira twice during the test. Research by [21] attributed the success of Phantom-Evasion to two factors: i. it was under active development. ii It was not as popular as Veil 3.1.14. Kaspersky was the best antivirus amongst the antiviruses. It had a detection rate of 100%. However, it was characterized by aggressive flagging making it susceptible to false positive. It was also the paid version with the full security features present.

In [2] the necessity of using third party antivirus software on Windows operating system was evaluated. This was achieved by investigating the detection capabilities and measuring the performance impact caused by third party antivirus software in comparison with the default Windows 10 antivirus service. The research was done by assessing the response time of certain user activities to establish how the user-experience was affected in different ways as a result of using third party antivirus software. There was a major increase in performance resulting from using third-party antivirus as shown by the performance yardstick.

Doi : https://doi.org/10.54216/JCIM.090105
Received: April 11, 2022 Accepted: July 17, 2022

From the reviewed literature we can see that no research work was carried out to understand the relevance of using only Windows default antivirus protection as the sole remedy against malicious software. This research work seeks to evaluate the security of Windows 11 against free antivirus evasion tools.

3. Research Method

A lab was set up to carry out the experiments on Pop OS[8] Linux machine whose configuration is shown in Figure 1 using Oracle VirtualBox[9]. The lab consisted of two machines – Windows 11[10] and Kali Linux 2021.3[11] as seen in Figure 2. Kali Linux was used as the attacking machine while Windows 11 was the victim machine. The method followed in conducting our research was installing the antivirus evasion tools one at a time on the Kali Linux attacking machine, create a malicious payload from the tool and make it available to the victim Windows 11 machine via Apache server which ran on the Kali Linux attacking machine. The Apache in this case played the role of a malware distribution server. In all cases, the malware type generated was a Remote Access Trojan (RAT). A payload which is basically a RAT was generated from each antivirus evasion tool, sent to the Windows 11 machine, ran and we attempted getting a connection via it using Metasploit Framework. For each test, the antivirus evasion tool got a score if: i. a payload generated from the tool successfully evaded the Windows 11 security ii. a connection was established between the Windows 11 and the Kali Linux attacking machine, since a RAT is only good enough if it creates a reverse connection back home [3].

Figure 1: Host OS (Pop OS) System Configuration

[8] https://pop.system76.com
[9] https://www.virtualbox.org/
[10] https://developer.microsoft.com/en-us/windows/downloads/virtual-machines/
[11] https://www.kali.org/

Doi : https://doi.org/10.54216/JCIM.090105
Received: April 11, 2022 Accepted: July 17, 2022

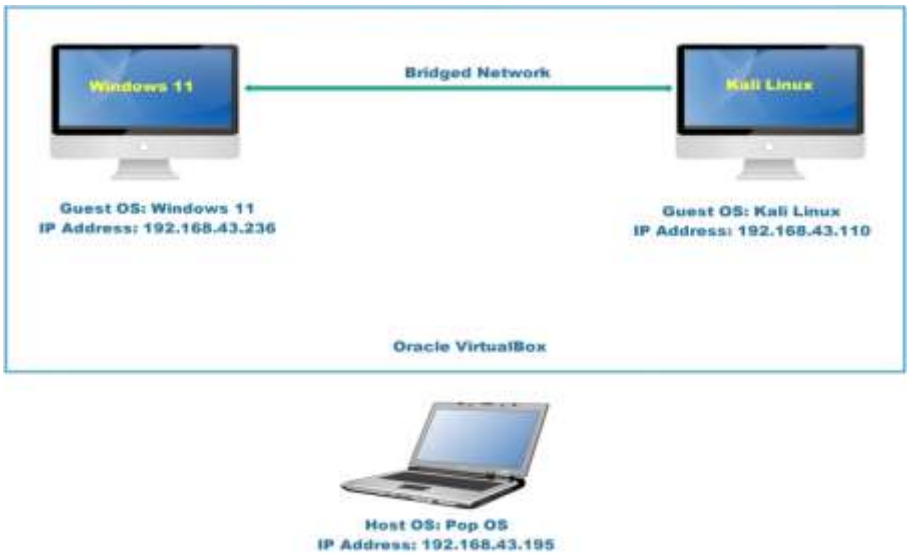

Figure 2: Virtual Lab Set Up for the Experiments

4. Result

This section presents the research results of testing antivirus evasion tools against the default Windows 11 security.

Test for TheFatRat

TheFatRat was installed on the Kali Linux machine as seen in Figure 3. Four payloads were generated from four modules of TheFatRat as seen in Table 1. Two of the payloads (*windows/shell/reverse_tcp* from module *Create bat file + Powershell (100% FUD)* and *windows/meterpreter/reverse_tcp*from module *Create bat file + Powershell (100% FUD)*) successfully evaded Windows 11.

Figure 3: TheFatRat installed on Kali Linux machine

However, a warning was produced before and after downloading the payloads as seen in Figure 4 and 5. None of the two payloads generated a meterpreter session however.

Doi : https://doi.org/10.54216/JCIM.090105
Received: April 11, 2022 Accepted: July 17, 2022

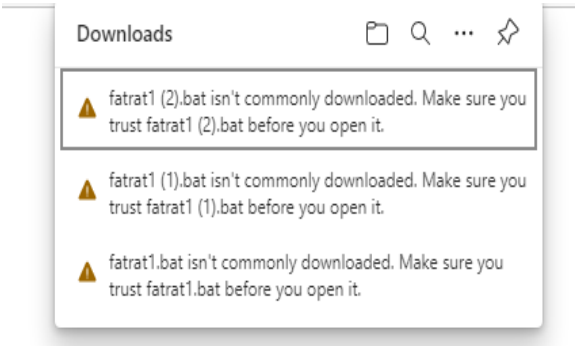

Figure 4: Windows 11 Security producing warnings on TheFatRat payload

Figure 5: A warning produced on TheFatRat payload

Two of the payloads (*windows/meterpreter/reverse_tcp* from module *Create exe file with C# + Powershell (FUD 100%)* and *windows/meterpreter/reverse_tcp* from module *Create exe file with apache + Powershell (FUD 100%)*) were outrightly detected by Windows 11 security as malware. Table 2 shows that TheFatRat had an evasion score of 2/8 (25%).

Table 2: Testing FatRat generated payloads against Windows 11 Security

Module	Payload	Detection	Meterpreter Session	Evasion Score	Remark
Create bat file + Powershell (100% FUD)	windows/shell/reverse_tcp	Not detected	No	1	The payload wasn't detected but there was a warning about it.
Create bat	windows/meterpreter/reverse	Not detec	No	1	The paylo ad

Doi : https://doi.org/10.54216/JCIM.090105
Received: April 11, 2022 Accepted: July 17, 2022

file + Powershell (100% FUD)	_tcp	ted			wasn't detected but there was a warning about it.
Create exe file with C# + Powershell (FUD 100%)	windows/meterpreter/reverse_tcp	Detected	No	0	
Create exe file with apache + Powershell (FUD 100%)	windows/meterpreter/reverse_tcp	Detected	No	0	
			Total Evasion Score	2/8	25%

Test for Venom Antivirus Evasion Tool

Venom antivirus evasion tool was installed on Kali Linux and five payloads were generated from five *Agents* using Venom antivirus evasion tool as seen in Table 3. Two payloads (*windows/meterpreter/reverse_tcp* from *Agent 3* and *windows/meterpreter/reverse_tcp* from *Agent 20*) successfully evaded the Windows 11 Security without generating meterpreter session through reverse connection. The rest of the three payloads (*windows/meterpreter/reverse_tcp* from *Agent 4*, *windows/meterpreter/reverse_tcp* from *Agent 5* and *windows/meterpreter/reverse_tcp* from *Agent 15*) were all detected by Windows 11 Security.

From Table 3, Venom has a total evasion score of 2/10 (20%).

Table 3: Testing Venom generated payloads against Windows 11 Security

Mod	Payloa	Detect	Meterpre	Evasi	Rema

Doi : https://doi.org/10.54216/JCIM.090105
Received: April 11, 2022 Accepted: July 17, 2022

ule	d	ion	ter Session	on Score	rk
Agent 3	windows/meterpreter/reverse_tcp	Not Detected	No	1	
Agent 4	windows/meterpreter/reverse_tcp	Detected	Not applicable	0	
Agent 5	windows/meterpreter/reverse_tcp	Detected	Not applicable	0	
Agent 15	windows/meterpreter/reverse_tcp	Detected	Not applicable	0	
Agent 20	windows/meterpreter/reverse_tcp	Not Detected	No	1	
			Total Evasion Score	2/10	20%

Defeat Defender

Following the instructions outlined on this page[12], we generated a malicious file using Defeat Defender version 1.2. But it was immediately detected by Windows 11. Defeat Defender is awarded a score of 0/2 (0%).

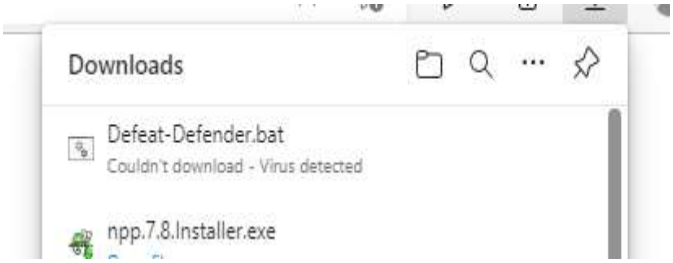

Figure 6: Malware generated with Defeat Defender was detected by Windows 11 Security

[12] https://secnhack.in/create-fud-fully-undetectable-payload-for-windows-10/

Doi : https://doi.org/10.54216/JCIM.090105
Received: April 11, 2022 Accepted: July 17, 2022

Paygen

Paygen was installed on Kali Linux as seen in Figure 8. We proceeded to generate a malware using Paygen but was detected by Windows 11 as seen in Figure 9. We scored Paygen a total evasion score of 0/2 (0%).

Figure 7: Paygen installed on Kali Linux

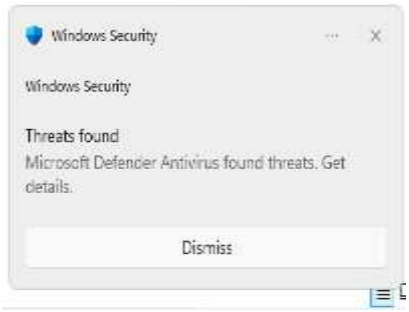

Figure 8: Malware generated using Paygen was detected by Windows 11 Security

Inflate

Inflate.py was installed on Kali Linux as seen in Figure 10. Using the malware generated from Paygen we proceeded to increase its size using Inflate.py as seen in Figure 10. It was however detected by Windows 11 Security. We therefore awarded it a score of 0/2 (0%).

Doi : https://doi.org/10.54216/JCIM.090105
Received: April 11, 2022 Accepted: July 17, 2022

Figure 9: Inflate.py Installed on Kali Linux

Defender Disabler

Defender Disabler is a Python script which when run disables Windows 11 Security. We ran it against the Window 11 machine as seen in Figure 11. It was however detected by the Windows 11 Security as seen in Figure 11.

Figure 10: Windows Disabler Detected by Windows 11 Security

Defender Disabler is awarded a total evasion score of 0/2 (0%).

Table 4: Percentage Evasion Score of Selected Antivirus Evasion Tools

S/N	Antivirus Evasion Tool	Percentage Evasion Score
1.	TheFatRat	25%
2.	Venom	20%
3.	Defeat Defender	0%
4.	Paygen	0%
5.	Inflate	0%
6.	Defender Disabler	0%

Doi : https://doi.org/10.54216/JCIM.090105
Received: April 11, 2022 Accepted: July 17, 2022

Table 4 gives a summary of the total percentage evasion score of the antivirus evasion tools tested against Windows 11 default security. From Table 4, TheFatRat has the highest evasion score of 25% followed by Venom with an evasion score of 20%. Defeat Defender, Paygen, Inflate and Defender Disabler all failed with a 0% evasion score. This is also plotted as a graph in Figure 12.

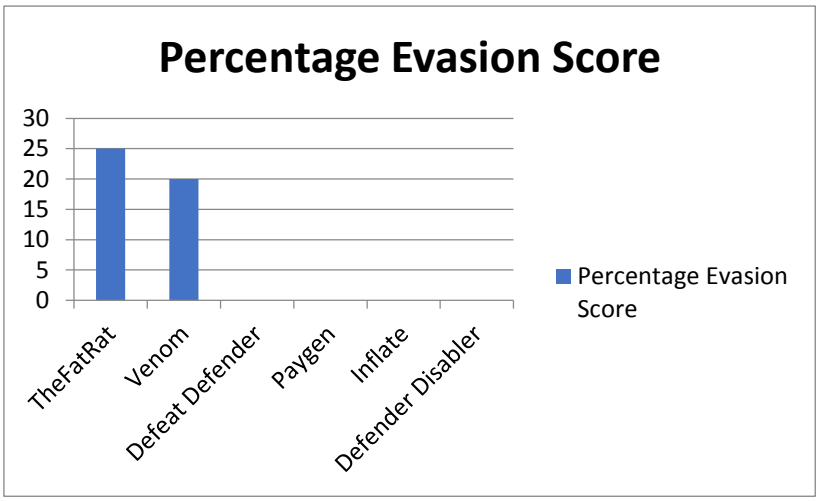

Figure 11: Percentage Evasion Score of Antivirus Evasion Tools against Windows 11.

5. Conclusion

From the research results, Windows 11 has a very good security. Six (6) antivirus evasion tools were tested, none of the tools was able to generate a malware capable of creating a reverse connection with the Windows 11. Even though TheFatRat and Venom were able to generate malicious samples that were not detected by the Windows 11, but none was able to create a reverse connection with the Kali Linux attacking machine. We can therefore claim that Windows 11 default security is good enough to stand on its own as the sole protection to the operating system. Third party antivirus protection can supplement the strong protection already provided by the Windows 11 default security. However, it is a cat and mouse game [3], it is only a matter of time before the antivirus evasion tool developers come up with tools strong enough to evade the Windows 11 security.

Funding: This research received no external funding

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

References

[1] Koret, J., &Bachaalany, E. (2015). The Antivirus Hacker's Handbook. Indianapolis: John Wiley & Sons, Inc.
[2] Baker, E. (2018). Evaluating the Necessity of Third-Party Antivirus Software. University of Skovde.
[3] Garba, F. A., Abdullahi, F. U., Abba, A., Yarima, F. U., Zakari, Z. A., Musa, A. L., et al. (2021). Evaluating Antivirus Evasion Tools Against Bitdefender. FINTECH-2021: International Conference on Fintech Opportunities and Challenges, Iqra University, Pakistan. Pakistan: Iqra University.
[4] JavatPoint. (2021). What is Windows? Retrieved April 24, 2022, from Javat Point: https://www.javatpoint.com/windows.
[5] GlobalStats, S. (2022, March). Operating System Market Share Worldwide. Retrieved April 23, 2022, from StatcounterGlobalStats: https://gs.statcounter.com/os-market-share
[6] Baxter, D., Hanson, M., &Weatherbed, J. (2022, February 04). Windows 11 features, pricing and everything you need to know. Retrieved April 21, 2022, from Techradar: https://www.techradar.com/news/windows-11-home-and-pro

[7] Olenick, D. (2021, June 25). Sizing Up the Security Features Slated for Windows 11. Retrieved April 23, 2022, from Bank Info Security: https://www.bankinfosecurity.com/sizing-up-security-features-in-windows-11-a-16943
[8] Hachman, M. (2022, April 5). This new Windows 11 security feature will force you to reset your PC. Retrieved April 23, 2022, from PC World: https://www.pcworld.com/article/629717/this-new-windows-11-security-feature-will-force-you-to-reset-your-pc.html
[9] David Weston . (2022, April 5). New security features for Windows 11 will help protect hybrid work. Retrieved April 12, 2022, from Microsoft:https://www.microsoft.com/security/blog/2022/04/05/new-security-features-for-windows-11-will-help-protect-hybrid-work/.
[10] Gatlan, S. (2022, April 5). Microsoft announces new Windows 11 security, encryption features. Retrieved April 23, 2022, from Bleeping Computer: https://www.bleepingcomputer.com/news/microsoft/microsoft-announces-new-windows-11-security-encryption-features/
[11] Garba, F. A. (2019). The Anatomy of Cyber Attack: Dissecting the Cyber Kill Chain. Scientific and Practical Cyber Security Journal (SPCSJ) , 29-44.
[12] Blackhat. (2020, February 2). Offensive Security Tool: TheFatRat.Retrieved July 26, 2021, from Blackhat Ethical Hacking.
[13] JavaRockstar. (2017, February 18). TheFatRat Tutorial – Generate Undetectable Payload FUD, Bypass Anti-Virus, Gain Remote Access. Retrieved July 26, 2021, from Hacking Vision:https://hackingvision.com/2017/02/18/the-fat-rat-tutorial-pwnwinds/.
[14] HackeRoyale. (2020, 6, 27). How FatRat Can Be Used To Create Exploits For Hacking: Tutorial. Retrieved July 26, 2021, from HackeRoyale: https://www.hackeroyale.com/fatrat-massive-exploit-tool/.
[15] Rahalkar, S., &Jaswal, N. (2019). The Complete Metasploit Guide.Packt Publishing.
[16] Microsoft. (2022, May 13). Protect security settings with tamper protection. Retrieved May 15, 2022, from Microsoft: https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/prevent-changes-to-security-settings-with-tamper-protection?view=o365-worldwide.
[17] Adam, A. S., &Sufyanu, Z. (2021). Performance Comparison of PyRAT and Phantom Antivirus Software. Sule Lamido UniversityJournal of Science and Technology, 65-72.
[18] Dogonyaro, N. M., Victor, W. O., Shafii, A. M., & Obada, S. L. (2021). Comparative Performance Analysis of Anti-virus Software. Springer Nature Switzerland AG.
[19] Botacin, M., Ceschin, F., Geus, P., &Grégio, A. (2020). We need to talk about antiviruses: challenges & pitfalls of AV. Computers & Security , 1-15.
[20] Adam, A. S., Sufyanu, Z., Sani, T., & Idris, A. (2020). Evaluating the Effectiveness of Antivirus Evasion Tools against Windows Platform.FUDMA Journal of Sciences, 89 – 92.
[21] Panagopoulos, I. (2020). Antivirus Evasion Methods. Piraeus.

Doi : https://doi.org/10.54216/JCIM.090105
Received: April 11, 2022 Accepted: July 17, 2022