FUDMA Journal of Sciences (FJS)
ISSN online: 2616-1370
ISSN print: 2645 - 2944
Vol. 4 No. 1, March, 2020, pp 89 – 92

EVALUATING THE EFFECTIVENESS OF ANTIVIRUS EVASION TOOLS AGAINST WINDOWS PLATFORM

[1]Aminu Shawwal Adam, [2]Zahraddeen Sufyanu, [3]Tajuddeen Sani and [4]Abdullahi Idris

[1,2,3]Department of Computer Sciences, Faculty of Computing, Federal University Dutse (FUD), Jigawa State
[4]Department of Computer Sciences, College of Sciences and Technology, Jigawa State Polytechnics, Dutse

[1,2,4] aminushawwal@gmail.com , sufyanzzzz@gmail.com , sankararng@gmail.com
[1,3]amshal2005@yahoo.com, tajuddeensani@yahoo.com

ABSTRACT

Despite the prevalence of cyber-crimes, information and communication technology ICT has become the most convenient medium of communication and information exchanges. With this development, the information security breach is now one of the complex and challenging issues software developers are facing. The tools that have been developed for penetration testing with the purpose to raise the level of security strength, have been used also by malicious intruders to gain access to our devices. This paper aimed to evaluate the effectiveness of some selected antivirus (AV) evasion tools: Avet, Veil 3.0, PeCloak.py, Shellter, and a Fat Rat, against a Window platform. The selection of these tools was made for the purpose of testing how they can generate undetectable malware against the current best Antivirus Solution products in the market. This, in turn, revealed AV solutions with the best performance in detecting malware with evasion capability. The paper adopted an experimental research design, in a Virtual lab setup with VMware Oracle VirtualBox, consisted of two machines (attacking and target machine). The results obtained indicated that the software evasion ranges from 0% to 83%. The Avet and PeCloak.py AV evasion tools were the best, while Kaspersky and Bitdefender antivirus appeared to be the best performing software protection in detecting the malware evasion tricks.

Keywords: Antivirus, Evasion Tools, Malware, Metasploit, Hackers.

INTRODUCTION

The development of computer and internet technologies have made many organizations and individuals rely heavily on computer network services, such as access to the Web sites, digital video and audio, shared use of application and storage servers, and other intercommunication services (Shrestha, 2012). Nowadays globalization system enables organizations to operate, collaborate and share information resources among themselves but at the same time exposes them to various threats both within and outside of the organization. As a result of that, organizations need to protect their information resources (Yoo et al., 2017). The network security breaches may result in loss of business reliabilities and productivity. Meanwhile, the time and labor involved in reorganizing the infected systems pose a significant expense (Shrestha, 2012).

Ogeto (2004) argued that, within the realm of an internetwork, heavily relying on computers and other technology poses a new set of security needs. The information systems and the networks are increasingly faced with security threats from hackers within or outside the network and becoming one of the most complex and important issues of concern.

Nikolaos (2018) believed that penetration testers are motivated to indulge and developed tools and techniques similarly used by real hackers, to attack systems and reveal its security flaws. This probes the weaknesses of the systems of an organization and identifies what it needs to defend itself from a real intrusion.

Network expertise often focuses on security assessment as an important means to get a better understanding of the information system security state. Hence, the assessment results are important bases to build up a network and security solution (Johnston & Garcia, 2002). However, new methods and means for network security assessment are developing and changing all the time and new research can still exploit the opportunity to cover the gap with the current literature. Nevertheless, hackers use malware to gain access to target computers through networks. Over time they began to call malware or scripts “payloads” that they would use against their targets in the same way the military pilot used missile against their physical target.

It has been explained by Techopedia (2019) that present-day malware is less likely to incorporate a payload that causes damage to system files; instead, they enable backdoors to access user’s computer and theft of sensitive information. These malicious payloads are usually generated using exploitation tools such as Core Impact, Canvas, and Metasploit Framework.

There are three main techniques used in detecting malware by antivirus software protection, these include **Signature-Based, Behavior-Based and Heuristic Based techniques** (Barriga et al., 2017).In cyber-attacks, Antivirus protection is one of the front lines of defense attackers faced when they try to hack a computer. And to avoid detection, antivirus evasion tools inventors also deploy a variety of techniques. These techniques are **obfuscation, code reuse attacks encryption,**

oligomorphism, polymorphism, and metamorphism. Antivirus evasion tools are used by both malicious attackers and penetration testers. The practice used by security professionals to assess system security strength is known as a penetration test. A penetration test involves attacking the system so as to uncover vulnerabilities that could be exploited by malicious hackers. Hence, the assessment results are important bases to build up a network and security solution (Johnston & Garcia, 2002). Therefore, there is a need to evaluate the effectiveness of these antivirus evasion tools used by malicious intruders and penetration testers respectively.

RELATED WORKS

To consider the previous relevant research works, Kalogranis (2018) evaluated four (4) antivirus evasion tools, against five (5) antivirus software products on the window platform. The best antivirus solutions according to his research work were selected. Afterward, the best evasion ratio was attained from the study conducted, whereby Avet and Veil evasion tools bypassed most of the antivirus protections and indicated as the best evasion tools.

Similarly, Themelis (2018) used the pyRAT evasion tool to automate the generation of Metasploit payload executable and invade systems without getting detected by most antivirus solutions. In his study, pyRAT met all the requirements of usability and made use of the penetration testing tool, called Metasploit Framework along with its features. The work presented pyRAT technology, and showed in a simple and clear way how to achieve an invasion on a system effectively and stealthy without getting caught by the majority of antiviruses.

Sukwong et al. (2011) evaluated the effectiveness of commercial antivirus software. They subjected each new malware they collected into the following six well-known commercial AV scans:

i. Avast 4.8 Professional v.4.8.1335,
ii. Kaspersky Internet Security 2009,
iii. McAfee Total Protection with Security Center v.9.15,
iv. Norton Internet Security 2009 v.16.5.0.135,
v. Symantec AntiVirus v.10.1.7.7000, and
vi. Trend Micro Internet Security Pro v.17.1.1250

Their empirical results showed that despite behavior-based detection; AV software can't effectively detect all current forms of malware. Nonetheless, behavior-based detection

Chua and Balachandran (2018) evaluated the Effectiveness of Android Obfuscation on Evading Anti-malware. According to them, the automation tool controls the VirusTotal application programming interface (API) to classify the malware samples. They further used 57 Antimalware Tools (AMTs) listed on VirusTotal, to evaluate the effectiveness of their proposed transformation techniques, and to make the evaluation scalable for a large number of malware samples. They used the command-line version of VirusTotal, which might be performing static analysis with a certain degree of the signature database. Their work proved that malware authors can increase malware's evasion rate by performing obfuscation techniques.

The novelty of their work was the identification of instability in detecting results for some AMTs. It was also highlighted that the AMTs did not build resilience/flexibility against the technique used to obfuscate the malware, but only update their signature database to be resilient to the specific variant of the malware. The trends highlighted in their work emphasized the ease of eventually evading current mainstream security tools for a malware author.

Rubenking (2019) listed out Avast Free Antivirus, Kaspersky Antivirus, AVG Free Antivirus, Bitdefender Antivirus Free Edition, Check Point ZoneAlarm Free Antivirus+ 2017, Sophos Home Free, Avira Antivirus, Adaware Antivirus Free, Comodo Antivirus 10 and Panda Free Antivirus as the best 10 free antivirus products.

In another review by Zacks (2019), the following were listed out: Norton Security Antivirus, McAfee Free Antivirus, Total AV Free Antivirus, Avira Free Antivirus, Panda Free Antivirus, Intrusta Antivirus, CYLANCE Antivirus, Heimdal Antivirus Free, Webroot SecureAnywhere Free, and Bitdefender Antivirus Free Edition.

Fisher (2019) mentioned that Avira Free Security Suite, Bitdefender Antivirus Free, Adaware Antivirus Free, Avast Free Antivirus, Panda Dome, AVG Antivirus Free, COMODO Antivirus Free, FortiClient, Immunet Antivirus, and Kaspersky Free are the best 10 free antivirus solutions.

Similarly, another review by Wagenseil (2019), the free antivirus solutions that made the first 10 lists are Kaspersky Free Antivirus, Bitdefender Free Antivirus, Avast Free Antivirus, Microsoft Windows Defender, AVG, Avira, Panda, Malwarebytes.

But, Allen (2019) presented 8 best free antivirus products as Avast, Bitdefender, AVG, Sophos Home Free, Panda Free Antivirus, ZoneAlarm Free Antivirus, Comodo Antivirus, and Avira Free Antivirus.

According to Orphanides (2019) Kaspersky Free Antivirus, Microsoft Windows Defender, Bitdefender Free Antivirus, Avira Free Antivirus, Avast Free Antivirus, and AVG Free Antivirus made the list of the 6 best antivirus free solutions.

Conversely, this study concerned with evaluating the effectiveness of the anti-virus evasion tools against the antivirus solutions, and not testing randomly collected malware samples that are not necessarily obfuscated.

Table 1 Show Summary of Related Works

S/N	Author(s)	Research	Strength	Weakness
1.	Kalogranis (2018)	AV Software Evasion: Evaluation of the Antivirus Evasion Tools	Use popular Metasploit reverse tcp meterpreter payload, and some sample files custom payload	Small number of evasion tools, and no encoding
2.	Themelis (2018)	Tool for AV Evasion: pyRAT	Use Metasploit Framework along with its features to automate the payload.	Employed predefined payload
3.	Sukwong et al., (2011)	Evaluate the Effectiveness of Commercial AV Software	Use variety of detection techniques	The test conducted on random collection of malware sample that are not necessary obfuscated
4.	Chua and Balanchandra (2018)	Evaluate the Effective ness of Android Obfuscation on Evading Malwares	Use large number of malware sample and 57 Anti-malware Tools (AMTs) on VirusTotal	Command- Line version is used that might be performing static analysis with certain degree of the signature database
5.	Present study (2019)	Evaluating the Effectiveness of AV Evasion Tools against Window Platform	Use popular Metasploit Framework and extending the number of Evasion software	Create payload from framework

Having reviewed many studies conducted it was found that, only a few works, evaluated the effective capability of the internet free evasion software on window platform protections. For this reason, this present study aimed at reconfirming but extending the work of kalogranis (2018), by creating the payload using popular metasploit framework. The selected AV evasion tools used in his study were re-evaluated and other AV evasion tools available in public circulations not included in the study also considered.

METHODOLOGY

Selection of Free Antivirus Products

For the selection of free antivirus products, based on the sources reviewed, we awarded scores to each antivirus that made an appearance in a review to 1 point. Hence, the antivirus products with the highest points were selected for this study. As depicted in Table 2.

Table 2: Selection of AV products

Antivirus Score	J. N. Rubenking (2019)	T. Fisher (2019)	P. Wagenseil (2019)	J. Allen (2019)	K. G. Orphanides (2019)	**AV rating Scores**
Avast AV	1	1	1	1	1	**5**
Kaspersky AV	1	1	1	0	1	**4**
AVG Free AV	1	1	1	1	1	**5**
Bitdefender AV Free	1	1	1	1	1	**5**
Check Point	1	0	0	0	0	1
ZoneAlarm Free AV	0	0	0	1	0	1
Sophos Home Free	1	0	0	0	0	1
Avira Antivirus	1	1	1	1	1	**5**
Adaware AVFree	1	1	0	0	0	2
Comodo Antivirus 10.3	1	1	0	1	0	3
Panda Free Antivirus 4	1	1	1	0	1	**4**
Total AV Free	0	0	0	0	0	0
Norton Free AV	0	0	0	0	0	0
McAfee Free Antivirus	0	0	0	0	0	0
Intrusta Antivirus	0	0	0	0	0	0
CYLANCE Antivirus	0	0	0	0	0	0
Heimdal Antivirus Free	0	0	0	0	0	0
Webroot Secure A.Free	0	0	0	0	0	0
FortiClient	0	1	0	0	0	1
Immunet Antivirus	0	1	0	0	0	1
Windows Defender	0	1	0	0	1	2

ExperimentalProcedure

The experimentation was carried out in a laboratory, set up with VM VirtualBox on Windows 8 host machine of 64-bit core! 4 intel processor, 10GB RAM, and 500GB HDD. Two virtual machines, the malware generation machine "Kali Linux" and the target machine "Windows 10" were networked and used via Ethernet cable, NAT (Network Address Translation) as seen in Figure 1.

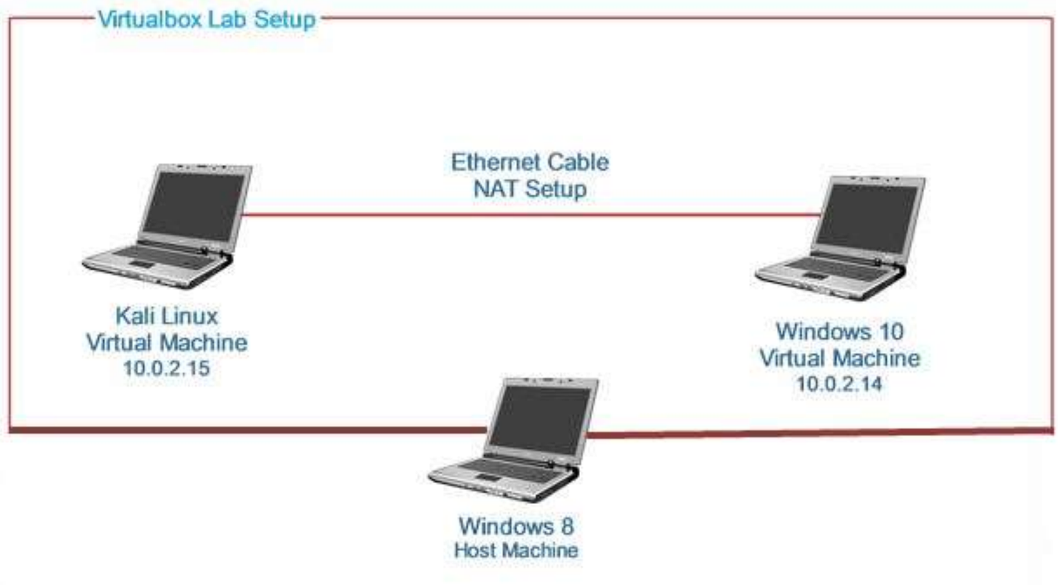

Figure 1: Virtual Laboratory Environment

All the evasion tools have been installed on the Kali Linux machine to generate the malware samples and deployed to the target machines (Windows 10) via malware distribution server for the target machines to download and run for executions. As further simplify in Figure 2.

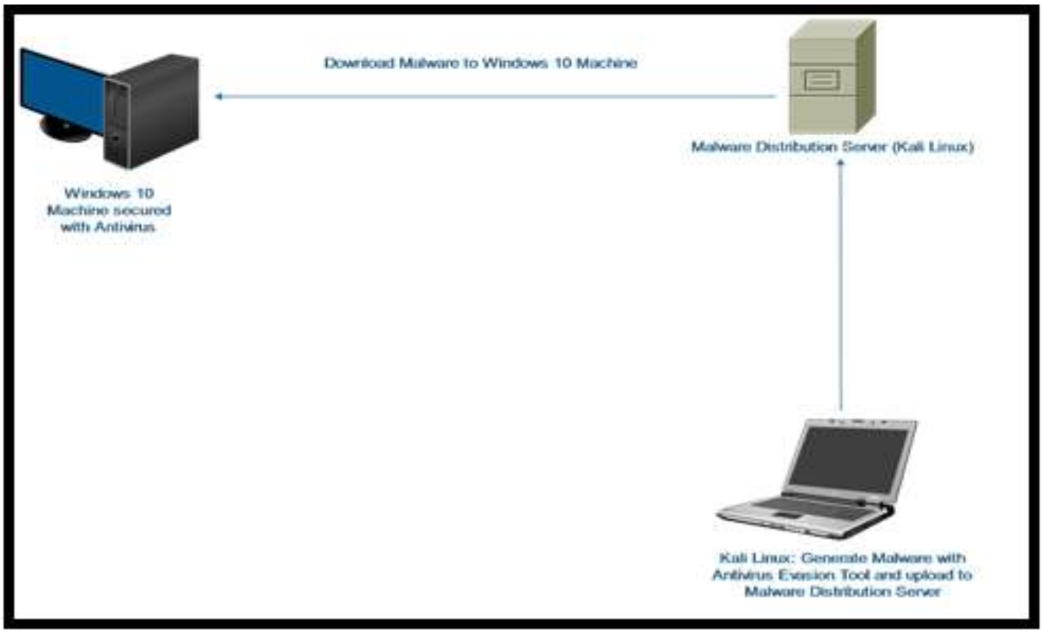
Download Malware to Windows 10 Machine
Windows 10
Machine secured
with Antivirus
Malware Distribution Server (Kali Linux)
Kali Linux: Generate Malware with
Antivirus Evasion Tool and upload to
Malware Distribution Server

Fig 2: Laboratory System Architecture

The antivirus solutions were also installed one at a time, tested with a malware generated from one of the evasion tools. Afterward, the tests continued until all selected AV software products were tested. During the evaluation, if the antivirus software detected the malware, a score of 1 is awarded to the antivirus; otherwise, it is awarded a score of 0. Henceforth, the evasion tool is awarded a score of 1 point if it was able to bypass the antivirus and a score of 0 otherwise. Finally, the antivirus software with the highest detection scores was awarded the most efficient. Also, the evasion tool with the highest score was awarded the best antivirus evasion tool in this study. Then, test results were recorded and compared with the recent work of Kalogranis (2018).

RESULTS AND DISCUSSION

The popular Metasploit window reverses TCP metepreter was used in this paper, to encrypt the payload. According to Beer and Hornat (2006), Metasploit is designed and easy to use, for penetration testing purposes. It was also mentioned that; Metasploit framework can be used to exploit any target in the system or network infrastructures.

The Tables listed below displayed the scores recorded to each antivirus software and AV evasion tools used in this study.

Table 3: Test results for Veil Antivirus Evasion

Antivirus Solution	Veil Score	Antivirus Score
Avira	0	1
Bitdefender	0	1
Avast	0	1
Kaspersky	0	1
AVG	0	1
Panda	0	1

Table 4: Test results for Pe.Cloak.py Antivirus Evasion

Antivirus Solution	Pe.Cloak.py Score	Antivirus Score
Avira	1	0
Bitdefender	0	1
Avast	1	0
Kaspersky	0	1
AVG	1	0
Panda	1	0

Table 5: Test results for Shellter Antivirus Evasion

Antivirus Solution	Shellter Score	Antivirus Score
Avira	0	1
Bitdefender	0	1
Avast	0	1
Kaspersky	0	1
AVG	0	1
Panda	0	1

Table 6: Test results for AVET Antivirus Evasion

Antivirus Solution	Avet Score	Antivirus Score
Avira	1	0
Bitdefender	1	0
Avast	1	0
Kaspersky	0	1
AVG	1	0
Panda	1	0

Table 7: Test results for Fat Rat Antivirus Evasion

Antivirus Solution	The Fat Rat Score	Antivirus Score
Avira	0	1
Bitdefender	1	0
Avast	0	1
Kaspersky	0	1
AVG	0	1
Panda	0	1

Table 8: Test results summary of the Antivirus evasion tools

S/N	AV Evasion Tools	Antivirus Free Avira	Bitdefender	Avast	Kaspersky	AVG	Panda	Total Evasion tools Scores
1.	Veil 3.0	0	0	0	0	0	0	**0**
2.	PeCloak.py	1	0	1	0	1	1	**4**
3.	Shellter	0	0	0	0	0	0	**0**
4.	Avet	1	1	1	0	1	1	**5**
5.	Fat Rat	0	1	0	0	0	0	**1**

The evasion ratios among antivirus evasion tools are compared here. In this research study, the evasion ratios (AVs evaded/Total Number of Selected AVs) were from 0% to 83%. PeCoak.py Evasion was observed with a 67% evasion ratio, Avet reported the highest evasion ratio of 83%, while Fatrat with 15%, the lowest 0% for both Veil and Shellter, as depicted in Figure 3.

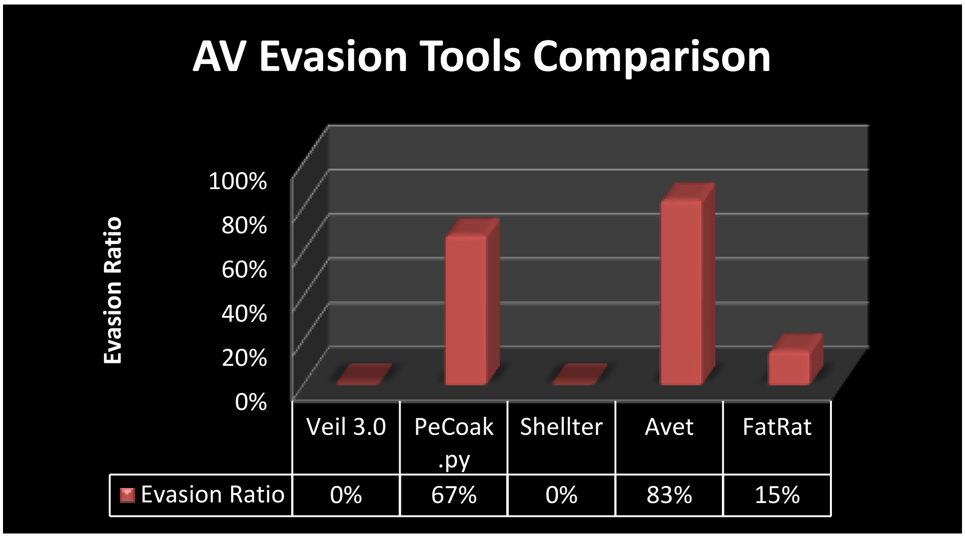

Figure 3: AV Evasion Tools Comparison

The results in Table 8 revealed that **Avet** evasion tools reported the best performance evasion tool, the technique used in Avet evaded 5 out of 6 Anti-virus suites. Avet includes two tools, avet.exe and AV evasion technique to avoid sandboxing and emulation. Avet.exe compiles the preconfigured binary file and is capable of loading ASCII encoded shellcode from textfile or from a webserver. While **peCloak.py** evasion tools became second for bypassing 4 out of 6 AVs**. Fat rat** evasion tool only able to evade 1 out of 6 AVs. Hence, none of the AVs was able to be bypassed by **shelter** and **Veil 3.0** evasion tool. For Veil 3.0 failures, there is need the script to be re-run to install any additional package and update the common configuration files. And in the case of Shellter, currently 32-bit apps only available, at the time of this study, while the laboratory system used pose 64-bits window application. This disparity also can yield an ineffective result for Shellter evasion tool. Shellter is capable of taking any of 32-bits Window application and embedding shellcode, either by custom payload or one available from

.

Metasploit framework as used in this study, in a way that is very often undetectable by AV software. If 32-bits application was used, you can create almost an infinite number of signatures making it nearly impossible for AV software to detect

Some of the results obtained in this study differ from the findings of Kalogranis (2018) whose evasion ratio (AVs evaded/Total number of selected AVs) was from 40% to 60%, while 0% to 83% is noticed in this present research.

In this study, Veil 3.0 evasion tool failed to bypass all the used antivirus software protection, while in the work of Kalogranis it was 60%, PeCloak.py acquires 67% rate of evasion, while 40% in the work of Kalogranis (2018). Shellter also got the weakest evasion ratio, in this research work, while shellter reported a 40% evasion ratio in the work of Kalogranis (2018). In both works, Avet maintained a high evasion ratio while 60% in Kalogranis's (2018) study as displayed in Figure 4

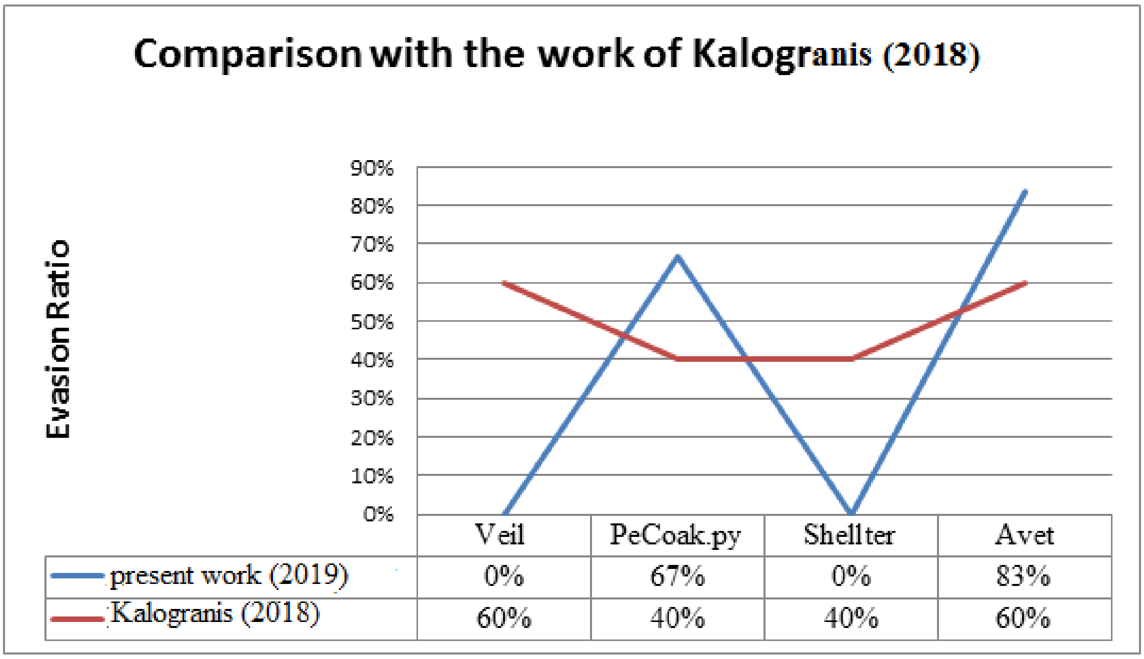

Figure 4: Comparison of Kalogranis (2018) and Present study

The results of the two study compared in Figure 4 varies; this is because anti-malware software designers improve their effort, enhance the detection accuracy by updating the signatures files of the software protection products, while some designers upgrade from traditional signature-based detection techniques to behaviour-based detection techniques. In addition, the malicious sample file, (Portable Executable) generated by the Evasion tools used in this study are predefined payloads. They created using popular frameworks and no any custom payloads injected. While in Kalogrnis (2018) study, most of the best efforts obtained from the Evasion tools are with the custom payloads. And the work of Chua and Balachandran (2018) only considered obfuscation as an evading technique and no known tool has been identified. The study also differs from this research since the researchers' target window platform, not android.

CONCLUSION

In conclusion, the results obtained in this research work, proved Avet and PeCloak.py AV evasion tools as the best having bypassed most of the selected antivirus by 83% and 67% respectively. On the other hand, Kaspersky and Bitdefender antivirus appeared to be the best performing software protection to detect the malware evasions tricks.

Also, based on the comparison made between this present study and Kalogranis (2018), indicated that it is better to write custom payloads and keep them simple to be away from AV detection rather than creating payloads using popular frameworks. Notwithstanding, the results gathered may still change as the AV products continuously updating the AV products signature files.

Finally, the computer system users are recommended to use the antivirus software protection indicated in this study, for the best system protection. In addition, Avet and PecCloak.py AV Evasion Tools are recommended for penetration testing activities.

REFERENCES

Allen, J. (2019) Eight (8) of the Best Free Antivirus Software Options. Retrieved from:

https://mashable.com/roundup/best-free-antivirus/. Accessed: June 2019.

Beer, D. D., Hornat, C. (2006). Penetration Testing with Metasploit. Retrieved from

http://www.scribd.com/doc/48616896/MSF-final, 2006. (Accessed: August 2019).

Chua, Balachandran (2018) Evaluated the Effectiveness of Android Obfuscation on EvadingAnti-malware. Retrieved from:
http//www.researchgate.net/publication/323786257_Effectiveness_of_AndroidObfuscation_on_Evading_Anti-malware. Accessed: June 2019.

Chen, W. (2018) Encapsulating Antivirus (AV) Evasion Techniques in Metasploit Framework. Rapid 7, 2018.

Fisher, T. (2019) The 10 Best Free Antivirus Software of 2019. Retrieved from:

https://www.lifewire.com/best-free-antivirus-software-4151895. Accessed on 02, July 2019.

Johnston, Roger, G., Garcia, A. R. (2002) Vulnerability Assessment of Security Seals. Technical report LA- UR-96-3672. Alamos National Lab.

Kalogranis, C. (2018) AntiVirus Software Evasion: An Evaluation Of The AV Evasion Tools. University of Piraeus, 2018.

Orphanides, K. G. (2019) Best Free Antivirus 2019: 6 tried and tested ways to stay safe. Retrieved from: https://www.trustedreviews.com/best/best-freeantivirus-3633595. Accessed on 28, June 2019

Ogeto, V. M. K. (2004). A survey of Computer-Based Information Systems Security Implemented by Large Private Manufacturing Companies in Kenya.MBA Thesis. University of Nairobi 2004.

Rubenking, J. N. (2019) The Best Free Antivirus Protection for 2019. Retrieved from: https://www.pcmag.com/roundup/267984/the-bestfree-antivirus-protection. Accessed on June 2019.

Shrestha, N. (2012) Security Assessment via Penetration Testing: A Network and System Administrator’s Approach. University Of Oslo, June 4, 2012.

Sukwong, O., Kim, H. S. (2011) Commercial Antivirus Software Effectiveness: An Empirical Study, IEEE Computer Society, pp. 63-70.

Techopedia, (2019) Malware – Payload Behavior. Available at www.technopedia.comAccessed: June 2019.

Themelis, N. (2018) A Tool for Antivirus Evasion: pyRAT. The University of Piraeus, Available: https://github.com/govolution/avet. Accessed in July 2019.

Wagenseil, P. (2019) Best Free Antivirus Software 2019. Retrieved from: https://www.tomsguide.com/us/best-freeantivirus, review-6003.html. Accessed: July 2019.

Yoo, S. G., Barriga, J. J. (2017) Malware Detection and Evasion with Machine Learning Techniques: A Survey.International Journal of Applied Engineering Research, Vol. ISSN 0973-4562 Volume 12, pp. 7207-7214, 2017.