Available online at https://journal.rescollacomm.com/index.php/ijqrm/index

International Journal of Quantitative Research and Modeling

e-ISSN 2721-477X
p-ISSN 2722-5046

Vol. 5, No. 2, pp. 140-147, 2024

Comparative Analysis of the Effectiveness Between Malwarebytes and BitDefender to Prevent Malware Attacks

Mohammad Zidan Yohanza[1*], Muhammad Giat[2], Muhammad Iksan Fadhilah[3], Mohammad Sulaeman[4], Ibrahim Dafi Iskandar[5], Varian Avila Faldi[6], Yuyun Hidayat[7]

[1,2,3,4,5,6] *Informatics Engineering, Universitas Padjadjaran West Java, Sumedang, Indonesia*
[7] *Statistics study program, Universitas Padjadjaran West Java, Sumedang, Indonesia*

**Corresponding author email: mohammad21005@mail.unpad.ac.id*

Abstract

Malware is the largest type of cyber-attack case in Indonesia. With the number of cases of malware occurring, many emerging software that provides services to ward off malware attacks. It takes the most effective anti-malware software to ward off malware attacks, so research is carried out. This study tested the detection and removal power of two anti-malware software (BitDefender and Malwarebytes). The initial research method used is to make a Pilot test which is a prefix in malware testing. In the Pilot test, the initial testing process for anti-malware software is carried out. Software that tested in the Pilot test include Malwarebytes, BitDefender, Avast, Cybereason, AVG, Avira. In the Pilot test, as many as 30 malwares were tested to determine which two software had the highest percentage of detection and removal tests. Furthermore, the data from the previous test got analyzed using the proportion of two populations test to determine the most effective software. With the tests of 500 malwares, it was found that the proportion of detection and removal of the BitDefender software is better than the Malwarebytes software. Therefore, it can be concluded that the BitDefender software is more effective than the Malwarebytes software as seen from the results of the test of the proportion of malware detection and removal.

Keywords: Cyber Attack, malware, anti-malware software, effectiveness, malwarebytes, bitdefender.

1. Introduction

1.1. Research Background

In the era of technology that is growing rapidly today, computers are used to facilitate human work, in operating computers there is software that runs on the operating system and plays an important role in performing the tasks performed by users. It is through this software that a computer can execute commands to assist users in completing their work (Akdemir and Lawless, 2020). Internet users both in the world and in Indonesia are increasing every year, of course, there is a positive side to a high internet network, but on a negative side, the internet or information technology is a new tool used by criminals to harm others (Delaney, 2020).

Throughout January-July 2021, cyber-attacks continued to increase drastically. This increase will undoubtedly cause even greater losses. In Southeast Asia, the Deloitte Cyber Smart: Enabling APAC businesses research report stated that the estimated cost for cybersecurity by companies is to reach USD 5.5 billion by 2025. Director of the Center of Economic and Law Studies (CELIOS), Arundati Swastika Waranggani (2022), explained that Indonesia's position was ranked 83 out of 160 based on rankings from the National Cyber Security Index (NCSI). This means that the quality of cyber security in Indonesia still requires significant improvement.

In 2020, as many as 316,167,753 cyber-attack cases were recorded by the National Cyber Security Operations Center of the National Cyber and Crypto Agency (BSSN) (Honeynet, 2022). Among all these cyber-attacks, 217,781 were cases of malware attacks. According to Cindy Mutia Annur (2021), 7 types of cyber-attacks that occurred in Indonesia at the end of 2021 were very diverse. Such as: Malware (85%), Phishing (70%), DNS Tunneling (68%), Denial of service (64%), SQL Injection (62%), Man-in-The-Middle attacks (61%), and Zero-day exploits (60%). Based on these data, malware is the largest type of cyber-attack case in Indonesia.

In general, malware is created to damage or break into software or operating system through an undisclosed script, which means that it is hidden by an attacker. The rapid development of malware requires computer users to be more vigilant so that personal information or important files are not taken by unauthorized people. Malware cases that are increasingly prevalent have resulted in many software providing services to ward off malware attacks by detecting and removing malware that comes from malware cases.

In research conducted by Kurniawati and Ardiansyah (2020), the study used a performance measurement methodology to detect and remove malware. In this study using antivirus such as Trend Micro Worry-Free Services and Kaspersky Endpoint Security antivirus. In the results of the study, both antiviruses have their respective advantages and disadvantages, but from this the research concludes that Kaspersky Endpoint Security Antivirus is the best performing antivirus. Even so in the detection and removal there are still drawbacks. Therefore, this study aims to improve the study, by testing several antivirus software that is more specific to malware.

1.2. Formulation of The Problem

Based on data from Honeynet Report, there was a very significant increase in cyber-attacks in 2019 and 2020 (Honeyet, 2022):

a. In 2019 , there were 98,243,896 attacks, 22,750 of which were malware attacks.
b. In 2020 , there were 316,167,753 attacks, 217,781 of which were malware attacks.

The Interpol Cyber Assessment Report 2021 reported that there were around 2.7 million ransomware attacks detected in Southeast Asian countries for the January-September 2020 period. Of that number, Indonesia was in the top rank with 1.3 million cases (INTERPOL, 2022).

Data from Cisco shows that as much as 85%, Malware often occurs in Indonesia by the end of 2021 (DISCO, 2021).

1.3. Research Purposes

The purpose of this research is to find the most effective malware prevention software for detecting and removing malware.

1.4. Research Contribution

The contribution of this research is to minimize or reduce malware attacks that are now spreading very widely in today's digital world.

2. Literature Review

2.1. Cyber Attack

According to Wilson, cyber-attack is any activity carried out using equipment, computer networks, or computer code that has destructive properties that can be used to modify, disrupt, close access, reduce performance, or damage computer files, computer networks, or computers and computer networks. itself is done intentionally and against the law.

2.2. Malware

Malware is software that is explicitly designed to carry out malicious activities or destroy other software such as Trojans, Viruses, Spyware, and Exploits (Kramer and Bradfield, 2010) .

2.3. Software anti-malware

In preventing malware attacks, anti-malware/anti-virus software is needed. Anti-malware software is a type of software that is installed directly on the computer to fend off, detect, and actively remove malware from existing systems. Some examples of anti-malware software include BitDefender and Malwarebytes.

2.4. Software BitDefender

Bitdefender software is a software that provides cybersecurity solutions with leading security efficacy and the best solution in warding off viruses, especially malware (Garba et al., 2021).

2.5. Software Malwarebytes

Malwarebytes software is software released by the Malwarebytes company which functions to eradicate or eliminate malware viruses effectively (Goldman, 2019).

2.6. Effectiveness

Effectiveness in general shows how far a predetermined goal has been reached (Rahadhitya and Darsono, 2015). Therefore, effectiveness emphasizes how the desired results are achieved according to a predetermined plan.

2.7. Proportion Hypothesis Test

Based on the book "Uji Hipotesis Statistik" by Mustofa (2013), the proportion hypothesis test is a test of two populations that aims to compare whether the first population is greater/equal/smaller than the second population.

a. Hypothesis
   The one-way proportion test hypothesis is used to compare 2 populations of larger or smaller proportions.
   $$H_0: P_1 \leq P_2$$
   P_1 is the proportion in population 1
   P_2 is the proportion in population 2
b. Level of Confidence
   The level of confidence used in this test is 90 percent or $(1-\alpha) = 0{,}90$ and $\alpha = 0{,}10$.
c. Proportion Test Statistical Formula

$$z = \frac{\widehat{p_1} - \widehat{p_2}}{\sqrt{\bar{p}(1-\bar{p})\left(\frac{1}{n_1} + \frac{1}{n_2}\right)}}$$

Where :

$$\widehat{p_1} = \frac{x_1}{n_1}$$
$$\widehat{p_2} = \frac{x_2}{n_2}$$
$$\bar{p} = \frac{x_1 + x_2}{n_1 + n_2}$$

Description:
$\hat{p}_1$ is the proportion in the sample 1
$\hat{p}_2$ is the proportion in the sample 1
$\bar{p}$ is the composite proportion
x_1 is the number of successes on sample 1
x_2 is the number of successes on sample 2
n_1 is the number of samples 1
n_2 is the number of samples 1

d. Critical Region
   The critical region is the area that rejects the first hypothesis. The critical point for one direction is Z_α for H_0 : $P_1 \leq P_2$.
e. Decision
   The decision rule for the one-way test is that the right-side rejects H_o if $z > Z_\alpha$.

3. Methods

3.1. Pilot Test

The pilot test is the initial method of performing malware testing. The malware collection used for testing was collected from the virussign.com site. To test the anti-malware software on the Pilot test, it takes as many as 30 malwares. After the malware has been collected, a pilot test is carried out on the anti-malware software. The software tested in the pilot test included Malwarebytes, BitDefender, Avast, Cybereason, AVG, Avira. In the pilot test to determine 2 software that has the highest percentage of detection and deletion tests.

Table 1: Pilot test detection results

	Number of malwares detected	Percentage
Anti-Malware	28	93%
BitDefender	29	97%
Cybereason	24	80%
AVG	26	87%
Avast	25	83%
Avira	25	83%

Table 2: Test results delete test pilot

Anti-Malware	Number of malware delected	Percentage
Malwarebytes	26	87%
BitDefender	27	90%
Cybereason	21	70%
AVG	25	83%
Avast	22	73%
Avira	23	77%

Table 1 and Table 2 are data obtained from the pilot test. Produced 2 software that has the highest percentage of detection and deletion tests, namely BitDefender and Malwarebytes. Data from the pilot test is also used to determine the initial hypothesis in testing the effectiveness of 2 anti-malware software.

3.2. Two Software Detection Test

The detection test method was carried out after collecting 500 malware obtained from the virussign.com site. The first test is to do a scanning process to detect malware. Malware detected by anti-malware software is marked according to the name of the detected malware, while undetected malware is marked with "undetected".

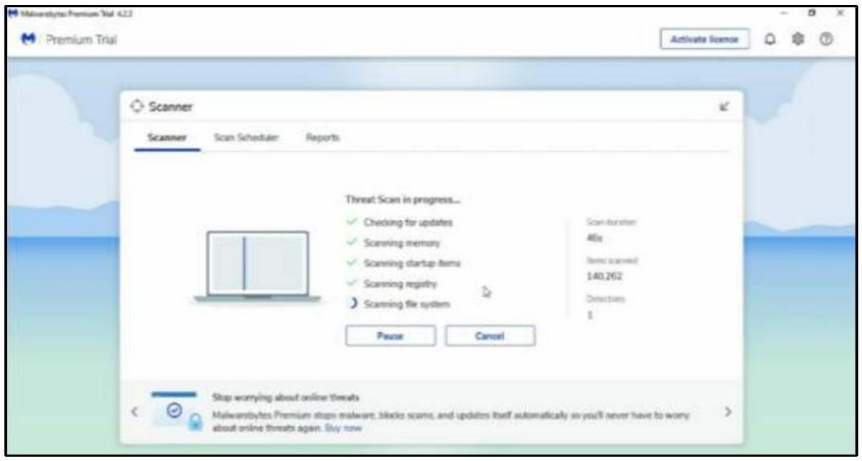

Figure 1: Malwarebytes scan process

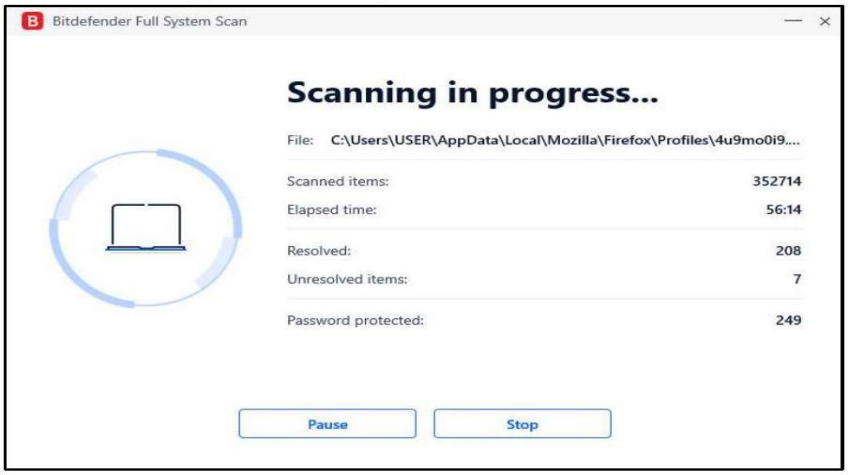

Figure 2: Bitdefender scan process

Figures 1 and 2 are views in the scanning process to detect malware. Figure 1 shows the scanning process using Malwarebytes software and the detection results are in the detections section, while Figure 2 shows the scanning process using BitDefender software and the detection results are in the resolved section.

3.3. Deletion test

Furthermore, the data from the detection test results, a second test is carried out, namely the removal of malware viruses that have been detected, if malware is not detected in the test, it is not delected and is marked as unprocessed. If the malware was successfully removed by the anti-malware software it is marked as removed, while malware that was not successfully removed is marked as unremoved.

Figure 3: Detection test and removal test table

Figure 3 is an overview of the results of the detection and removal tests for malware. There is malware data that has been detected and the information can be delected or not. For the full table, see Attachment 1.

4. Results and Discussion

4.1. Analysis Test Detection and Remove

Attachment 1 , there are the results of the detection and deletion test data that were previously detected using two Malwarebytes and BitDefender software, then an analysis of the data was carried out.

The first data to be analyzed is the detection test data. Of the 500 malware tested, the detection test results can be seen in Table 3 .

Table 3: Detection test analysis results

Anti-Malware	Total

BitDefender	483
Malwarebytes	444

Table 3 shows the results of the detection test on both software. In BitDefender software there are 483 malware that can be detected from 500 malware. While the Malwarebytes software can detect 444 malware out of 500 malware.

Table 4: Removal test analysis results

Anti-Malware	Number of malware detected	Number of malware delected
BitDefender	483	475
Malwarebytes	444	421

Table 4 shows the malware that can be removed from the malware that has been detected by the two software used previously. In table 4, it can be seen that the BitDefender software from 483 detected malware can remove 475 detected malware. Meanwhile, Malwarebytes software was able to remove 421 malware from 444 detected malware.

4.2. Proportion Test Analysis

a. Test proportion of detection test

$$z = \frac{\widehat{p_1} - \widehat{p_2}}{\sqrt{\bar{p}(1-\bar{p})\left(\frac{1}{n_1} + \frac{1}{n_2}\right)}}$$

Hypothesis:

$$\mathrm{H}_0 : P_1 \leq P_2$$

Description:

Research confidence level is 90%.
$\widehat{p_1}$ is the proportion of malware that BitDefender detects
$\widehat{p_2}$ is the proportion of malware detected by Malwarebytes
H_0 is the first hypothesis

b. Z Test Detection Proportion

$$z = \frac{0{,}966 - 0{,}888}{\sqrt{0{,}927(1-0{,}063)\left(\frac{1}{500} + \frac{1}{500}\right)}}$$

Table 5: Z test results proportion detection

Description	Result
$\widehat{p_1}$	0,966
$\widehat{p_2}$	0,888
$\bar{p}$	0,927
z	4,74

1) Critical area
   The level of confidence in this study is 90%, so $= 0.1$ so that the Result Z0.1 is 1.28 .
2) Decision
   The $z = 4.74$ test is obtained, then the arena $z >$ Z0,1 so that the decision is to reject H_0.
3) Result
   Based on the detection proportion test data, z was found to be 4.74 which was greater than $Z0.1 = 1.28$. This proves that the second hypothesis is correct, namely BitDefender is more effective in detecting malware than Malwarebytes.

c. Proportion test of deletion test

$$z = \frac{\widehat{p_1} - \widehat{p_2}}{\sqrt{\bar{p}(1-\bar{p})\left(\frac{1}{n_1} + \frac{1}{n_2}\right)}}$$

Hypothesis:

$$\mathrm{H}_0: P_1 \leq P_2$$

Description:
Research confidence level is 90%.
$\widehat{p_1}$ is the proportion of malware that BitDefender detects.
$\widehat{p_2}$ is the proportion of malware detected by Malwarebytes.
H_0 is the first hypothesis.

1) Z Test Removal Proportion

$$z = \frac{0{,}98 - 0{,}95}{\sqrt{0{,}97(1-0{,}03)\left(\frac{1}{483} + \frac{1}{421}\right)}}$$

Table 6: Z test results proportion removal

Description	Result
$\widehat{p_1}$	0,98
$\widehat{p_2}$	0,95
$\bar{p}$	0,97
z	2,98

2) Critical area
The level of confidence in this study is 90%, so $= 0.1$ so that the Result Z0.1 is 1.28 .
3) Decision
It was found that the test $z = 2.98$, then the arena $z >$ Z0,1 so the decision was to reject H_0.
4) Result
Based on the test data for the proportion of deletions, it was found that z of 2.98 was greater than Z0,1 = 1.28. This proves that the second hypothesis is correct, namely BitDefender is more effective in removing malware than Malwarebytes.

5. Conclussion and Recommendation

5.1. Conclusion

Based on the data from the tests that have been carried out, it can be concluded that the BitDefender software is more effective in detecting and removing malware than the Malwarebytes software.

5.2. Recommendation

In this study, there are several suggestions or recommendations given, namely:
1) In detecting and removing malware, it is recommended to use BitDefender software because it is able to detect malware (96%) and remove malware (98%).
2) In future research, conduct research using anti-malware software that can detect and remove all malware and test its effectiveness using other, more complex methods.

6. Attachment

Link : bit.ly/DataUjiDeteksiDanUjiHapus

References

Cindy Mutia Annur. (2021, Oktober 23). *Serangan Malware Banyak Mengintai UMKM di Masa Pandemi*. Katadata.co.id. https://katadata.co.id/teknologi-telekomunikasi/serangan-malware-banyak-mengintai-umkm-di-masa-pandemi

Kramer, S., & Bradfield, J. C. (2010). A general definition of malware. *Journal in computer virology*, *6*, 105-114.

Kurniawati, A., & Ardiansyah, A. (2020). Analisis Performa Perangkat Lunak Antivirus Dengan Menggunakan Metodologi Pengukuran Performance. *Jurnal Ilmiah Matrik*, *22*(1), 43-54.

Mustofa, A. (2013). *Uji hipotesis statistik*. Gapura Publishing. com.

Rahadhitya, R., & Darsono, D. (2015). *Faktor-Faktor Yang Berpengaruh Terhadap Efektivitas Audit Internal (Studi Pada Inspektorat Provinsi Jawa Tengah)* (Doctoral dissertation, Fakultas Ekonomika dan Bisnis).

Wilson, C. (2003). Computer attack and cyber terrorism: Vulnerabilities and policy issues for congress. *Focus on Terrorism*, *9*(1), 1-42.

Garba, F. A., Yarima, F. U., Kunya, K. I., Abdullahi, F. U., Bello, A. A., Abba, A., & Musa, A. L. (2021). Evaluating Antivirus Evasion Tools Against Bitdefender Antivirus. In *Proceedings of the International Conference on FINTECH Opportunities and Challenges, Karachi, Pakistan* (Vol. 18, pp. 1-6).

Goldman, E. (2019). Amicus Brief of Cybersecurity Law Professors in Enigma Software v. Malwarebytes. *Santa Clara Univ. Legal Studies Research Paper*.

INTERPOL. (2021*). INTERPOL report charts top cyberthreats in Southeast Asia.* Diakses pada 5 Juni 2022, dari https://www.interpol.int/News-and-Events/News/2021/INTERPOL-report-charts-top-cyberthreats-in-Southeast-Asia

Akdemir, N., & Lawless, C. J. (2020). Exploring the human factor in cyber-enabled and cyber-dependent crime victimisation: A lifestyle routine activities approach. *Internet Research*, *30*(6), 1665-1687.

Delaney, J. (2020). *The effectiveness of antivirus software* (Master's thesis, Utica College).

Arundati Swastika Waranggani. (2022, Juni 15). NCSI : Keamanan Siber Indonesia Peringkat 83 dari 160 Negara. Cloud Computing Indonesia. https://cloudcomputing.id/berita/ncsi-keamanan-siber-indonesia-peringkat-83-dari-160-negara/

CISCO. (2021, September). Cybersecurity for SMBs: Asia Pacific Businesses Prepare for Digital Defense.

Honeynet. (2022). *(2022). Informasi Serangan Cyber.* Diakses 5 Juni 2022, dari https://honeynet.bssn.go.id/