Ransomware Detection and Prevention through Strategically Hidden Decoy File

Yung-She Lin and Chin-Feng Lee
(Corresponding author: Chin-Feng Lee)

Department of Information Management, Chaoyang University of Technology
Taichung 41349, Taiwan, ROC
Email: asirlin@gmail.com; lcf@cyut.edu.tw

(Received Aug. 15, 2022; Revised and Accepted Jan. 28, 2023; First Online Feb. 17, 2023)
The Special Issue on Trusted ICT Technologies on the Smart Society and Secure Multimedia Applications
Special Editor: Prof. Chin-Feng Lee (Chaoyang University of Technology)

Abstract

Today's antivirus software has various methods to detect new and unknown malware, offering a very high detection rate and protection ability for virus-type malware. However, this detection rate is significantly reduced or even provides no protection capability for ransomware good at hiding, which is a highly severe threat to the computer files stored by users. Current antivirus software uses machine or deep learning mechanisms to effectively improve the detection rate of new and unknown malware. However, the news still reports ransomware incidents from enterprises or government units. This study implements a honeypot technique, a secret pot mechanism, where decoys are placed in the computer to detect ransomware. The detection program monitors the decoy files used at any time. Once the file is damaged by ransomware, the protection mechanism is triggered immediately, forcing the computer to shut down, preventing the ransomware from encrypting and destroying the files, which can protect the user's files and minimize losses.

Keywords: Cyberattack; Honeypot; Ransomware Detection and Prevention

1 Introduction

One of the required applications for computers are antivirus software, which is used to prevent malicious software (such as computer viruses, trojans, and ransomware) from invading our devices. The advancements of information technology enable hackers to use new technologies and methods that keep pace with the times to develop malicious software or even find weaknesses in antivirus software, break through its detection and protection, and cause computer damage through poison or invasion. This problem is a highly significant information security threat for enterprises.

In 1989, Joseph Popp developed the first ransomware AIDS Trojan in human history [2]. He distributed 20,000 posters labeled "AIDS Information–Introductory Diskettes" to attendees at the World Health Organization (WHO) AIDS Conference. The disks were infected with the AIDS Trojan, which replaces the AUTOEXEC.BAT file and uses it to count computer boot times. Once the boot count reaches 90, the AIDS Trojan hides the directory and encrypts all file names on the hard drive C, making the computer unbootable. Then, a screen appears asking the user to pay ($189 to a PO Box in Panama).

Ransomware has been developed for over 25 years, and the encryption technology used by ransomware is also constantly improving. Today's ransomware uses asymmetric encryption technology that is difficult to crack.

In addition to stealing the confidential information in the user's computer, ransomware also encrypts the computer files such that the user cannot obtain access. Then, the user is asked to pay a certain amount of Canadian currency as a ransom to obtain the decryption key. If the user fails to pay the ransom according to the hacker's instructions, the latter does not provide the decryption key to the user. Without the correct decryption key, the file cannot be restored. In several cases, even when the user has paid the ransom according to the hacker's instructions, the hacker still did not provide the decryption key. Cases of repeated extortion by the same ransomware have also occurred.

Today's antivirus software has good detection rate and protection against known ransomware, but most are almost powerless against new and unknown ransomware. Antivirus software can become useless because ransomware has multiple ways to evade detection. This is also the reason why users install antivirus software and often update the latest virus patterns, but they are still unable to escape malicious ransomware. Four types of ransomware incidents have been reported:

1) In March 2021, Acer was attacked by ransomware,

which stole company files and encrypted them. Hackers extorted $50 million from Acer [5]. In July 2021, Kaseya Software suffered a ransomware attack during the National Day holiday in the United States, which affected about 1,500 companies around the world, compromised more than 1 million computers, and was extorted $70 million [6]. Occurred in August 2021 Gigabyte was attacked by hackers, it was confirmed that confidential files were stolen, and the hackers demanded a ransom in cryptocurrency [7].

2) Cause network interruption and leakage of customer data. In 2021, Insurance giant CNA reports data breach after ransomware attack [8], and Fimmick ransomware attack puts over 35,000 people's data at risk [11].

3) Attack cloud infrastructure. In 2021, Python ransomware script targets ESXi server for encryption [13]. In 2022 ASUSTOR NAS been hit by Deadbolt Ransomware [14].

4) Create national security problems such as in 2021, the Colonial Pipeline cyberattack [15] shuts down pipeline that supply 45% of East Coast's fuel.

In recent years, due to its great progress, artificial intelligence-related technologies, such as machine or deep learning, have been used to effectively improve the detection rate of new computer viruses and malware. According to Poudyal and Dasgupta, the detection rate of ransomware can reach 99.54% by using artificial intelligence-related technologies [17]. Adamov and Carlsson applied a Reinforcement Learning approach to anti-ransomware testing, and helps to improve weaknesses in anti-ransomware defenses and fixes them before a real attack occurs [19].

A deception strategy commonly used to detect network intrusion is the honeypot mechanism, which lures hackers or malicious software to attack the honeypot server. This method has shown good performance and can effectively reduce or prevent the server from being attacked. Pascariu and Barbu use Honeypot solution designed to detect a ransomware infection identify the ransomware family [9]. Moore [3] deployed a Honeypot server on the network to detect any ransomware activity.

In the present study, we refer to the deception strategy of the honeypot mechanism commonly used in network intrusion detection. According to the characteristics of the Windows operating system, a decoy file is planted to detect the ransomware. Once the honeypot file used as bait has been damaged by ransomware, it shuts down the computer immediately to prevent the ransomware from encrypting and destroying files, which can protect the user's data to the greatest extent and minimize losses.

This paper is divided into five parts. The first section briefly introduces the research background and the current ransomware threats. The second section mainly discusses the honeypot mechanism used to lure the enemy. The third section presents how we strategically use a hidden decoy file to detect and prevent the ransomware attack. The fourth section describes the results and the comparison of the protection effect of antivirus software commonly used by users against new and unknown ransomware. The fifth section presents the conclusion.

2 Literature Review

Honeypot is a deception strategy mechanism used to lure attackers. The purpose of honeypot is not to prevent or mitigate attacks, but rather to pretend to be a real environment, deceive attackers, and lure them into exhibiting aggressive behavior. When the attacker appears, they are caught and dealt with later.

A good example of a honeypot is proposed by Pascariu and Barbu, who used Raspberry Pi to disguise an SMB server secret jar to lure and catch ransomware attacks on the Internet. This method has a good effect when the ransomware is intended to destroy the files on the server in the network [9]. Moore deployed a honeypot server by creating a secret can folder on the server and monitoring the activities related to the files to detect any ransomware activity on the network [3]. Venkatesh *et al.* established a sealed container environment for file servers to test and analyze any malicious network behavior or file destruction [1]. However, the methods of detecting ransomware by the encrypted server deployed on the Internet cannot identify when the ransomware starts to destroy the files. The sabotage of servers by ransomware is not detected until the files on the secret can are encrypted.

Zhuravchak *et al.* used an file symbolic linking honeypots to detect and prevent ransomware attacks in Linux operating systems [4]. A honeypot archive is deployed to monitor ransomware encryption activity on the file, and deploying one or more symbolic links pointing to the sealed and monitored can file in the folder. Thus, the file encryption activities of the ransomware on the Linux operating system can be completely and effectively monitored.

Fan *et al.* deployed a high-efficiency canister system to block various attacks from the network [12]. According to different network security requirements, Eliot *et al.* proposed a flexible network security laboratory environment that uses Raspberry Pi and VMWare virtual machines as honeypot deployment to effectively detect and prevent intrusions and attacks from the Internet [10]. Fan et al mentioned an intrusion prevention system (IPS) integrated with a honeypot can used to detect and block attacks from internal or external networks [16]. Lee *et al.* [18] suggested that when a malicious program has successfully invaded a computer system and gotten administrator privileges, the hidden interface is used to implement file-based Phantom FS spoofing technology to provide simulation and camouflage and hide real files, maximizing the chance of successfully deceiving malware into corrupt file.

The above cases show that the honeypot mechanism

used to deceive and lure hackers or malicious software to attack itself has various setting methods according to different baiting requirements. The secret can server has shown good protection on the server and the network.

3 Proposed Method

With a focus on the behavior pattern of ransomware encrypting files, this study refers to the method of deceiving the enemy that is commonly used in network intrusion detection. The encrypted canister file is set as a bait in the computer with the Windows operating system to attract and deceive ransomware. Once the file is damaged by ransomware, the protection mechanism is triggered immediately, forcing the computer to shut down and preventing the ransomware from encrypting and destroying files, which can protect the user's data and minimize losses.

3.1 Behavior Patterns of Ransomware

This study has repeatedly verified the behavior of several kinds of ransomware on file encryption and has confirmed its behavior mode. The ransomware found in the Windows system, when encrypting the files of the compromised computer, starts looking for the files from the root directory of drive C: to encrypt and destroy. Then, the ransomware repeatedly searches for the files in its lower subfolders. In encrypting and destroying files, ransomware uses an ascending order by file name. Ransomware does not destroy the normal operations of the computer system, and does not encrypt executable files including exe, com, dll, and sys. Rather, the main targets for encryption are the following file types:

1) Document File: txt, doc, docx, pdf, xls, xlsx, ppt, pptx, htm, html, ...
2) Video files: mp3, wav, mp4, dat, avi, ...
3) Program source code files: c, cpp, java, js, css, ...
4) Graphic files: bmp, jpg, gif, dwg, ...
5) Database files: dbf, mdf, mdb, accdb, db, sql, xml, json, ...

This study finds that the ransomware may process the file names of the encrypted files in the following three modes: (1) The file name remains unchanged after encryption; (2) After encryption, a specific file name is added to the file name, varying with different ransomware. For example, assuming that the original file name is A.txt, the encrypted file name becoms A.txt.xxx; (3) After encryption, the file name is changed to a random English + numeric string file name. Suppose the original file name is A.txt, the encrypted file name may become Asdcifksmc.xk354.

Given the difficulties to obtain new and unknown ransomware, all of the obtained ransomware are known and can be effectively identified and protected by antivirus software. However, the protective effect on new and unknown ransomware is impossible to measure. To simulate the new and unknown ransomware, we refer to the behavior patterns of three different types of ransomwares and develop three simulation programs to simulate new and unknown ransomware. Then, these three simulation programs are used to test the proposed method and the common antivirus software in the market for purposes of comparison. When facing new unknown ransomware, the proposed method and each antivirus software can effectively protect computer files.

The ransomware processing for encrypting files is a complex and hard-to-break asymmetric encryption algorithm. In this study, the ransomware simulation program only mimics the effect of encrypting files, and does not use a high-strength asymmetric encryption algorithm. Instead, a simple symmetric encryption algorithm is used to simulate the effect of ransomware encrypting and breaking files. Table 1 shows the software and hardware of the development environment where Microsoft Visual Studio 2019 and Microsoft Visual C# are used to develop a simulated ransomware.

Table 1: The software and hardware configuration of development environment

CPU	Intel i7-8750H
RAM	DDR4 16GB
HDD	SSD 256GB
Operating System	Microsoft Windows 10 Home
Development Tools	Microsoft Visual Studio 2019
Programming Language	Microsoft Visual C#

3.2 The Protection Mechanism

This study addresses the behavior patterns of ransomware encrypted files, with reference to the honeypot method of deceiving the enemy commonly used in the network intrusion detection. The proposed method proposed sets up a monitoring program in Windows OS and a honeypot file in the computer as bait to lure and deceive ransomware attacks. If the monitoring program finds that the honeypot file used as bait is encrypted by ransomware, it triggers emergency protection, forcing the computer to shut down and stop working, to prevent the ransomware from encrypting other files and thereby protect the data. Figure 1 shows the proposed protection architecture diagram.

Figure 2 shows the proposed protection workflow chart. The monitoring program first checks whether the bait honeypot file exists, given that ransomware may change the file name synchronously during encryption. If the monitoring program does not find the bait honeypot file, then it assumes that the ransomware has invaded the computer, changed the file name of the decoy file, and has

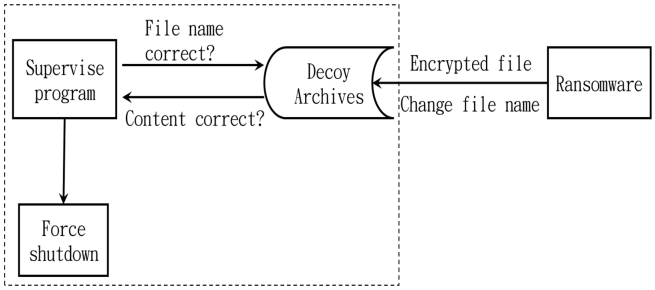

Figure 1: The proposed protection architecture diagram.

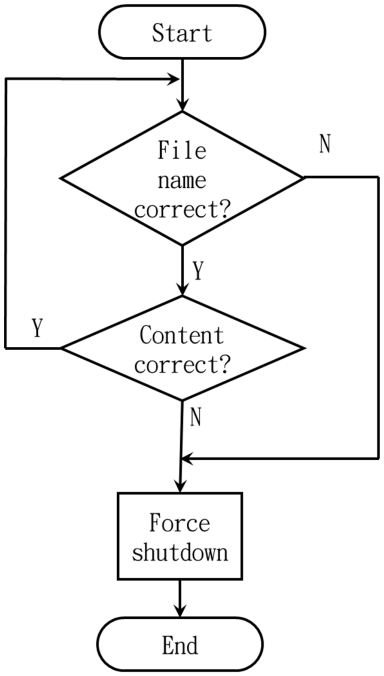

Figure 2: The proposed protection workflow chart.

begun to destroy files. At this point, the monitoring program triggers the protection mechanism to force the computer to shut down, and thus that the ransomware cannot work, preventing the continuous destruction of files. Thus, To further determine if there is any ransomware intrusion, the monitoring program opens the honeypot file and reads its content for comparison. If the read content is the correct preset identification key, then the computer has not been corrupted by ransomware and remains safe at this time. To avoid occupying system resources, the monitoring program enters the sleep mode (60 seconds by default), and restarts the detection after resting.

3.3 The Testing Method

This study adopts the ransomware behavior model to implement new and unknown simulated ransomware to test the proposed methods and antivirus software regarding the detection and protection capabilities of

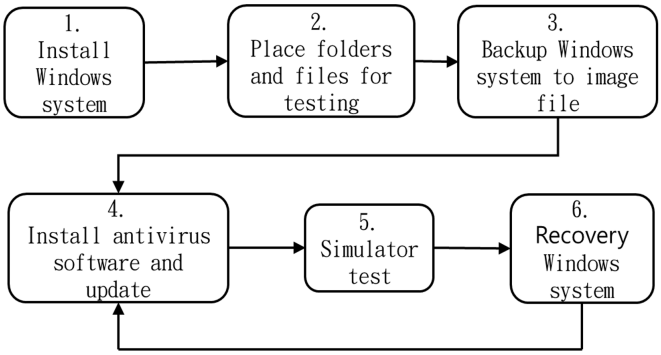

Figure 3: The flowchart of this test assignment.

new and unknown ransomware.
A desktop computer is used for testing and verification. Table 2 shows the software and hardware specifications of the test computer.

Table 2: The software and hardware specifications of the test computer.

CPU	AMD Ryzen R7-3700X
RAM	DDR4 16GB
Motherboard	ASUS B450M-A
HDD	SSD 256GB
Operating System	Microsoft Windows 10 Home
Development Tools	Microsoft Visual Studio 2019

The test proceeds as follows: Step 1 installs Windows 10. Step 2 simulates general users storing folders and files in the disk drive, with a total of 850 files. Step 3 backs up the hard disk as an image file. Step 4 reboots and installs the antivirus software for testing, and updates the antivirus software version and virus pattern to the latest version. Step 5 executes simulated ransomware to test the antivirus software the detection and protection capabilities. Step 6 restores the image file to this hard disk and returns to step 4 for the next test. Figure 3 shows the flowchart of this test assignment.

We prepared commonly used 10 files, including document files (.doc, .docx, xlsx, ods, ppt, pdf, odt, txt), video files (.mp4), compression files (.zip), as shown in Table 3. In Table 4, we create 8 different folders, each of which contains a different number of files, for a total of 850 files.

4 Research Results

Facing the ever-evolving ransomware, ensuring that the computer files are not damaged is a problem for enterprises and government units. Although everyone knows that file backup is the best method to deal with ransomware, such operation is often not performed due to human negligence, equipment problems, or network is-

Table 3: 10 different file type.

Item	File	File type
1	01.jpg	Image file
2	02.mp4	Video file
3	03.dot	Document file
4	04.doc	Document file
5	05.xlsx	Spreadsheet file
6	06.ods	Spreadsheet file
7	07.ppt	Presentation file
8	08.pdf	Document file
9	09.txt	Plain text file
10	10.zip	Compressed file

Table 4: 8 different folders, each of which contains a different number of files, for a total of 850 files.

Item	Folder	File count
1	C:\	10
2	C:\TEST	120
3	C:\Users\User\Desktop	120
4	C:\Users\User\Documents	120
5	C:\Users\User\Download	120
6	C:\Users\User\Music	120
7	C:\Users\User\Pictures	120
8	C:\Users\User\Videos	120
Total files		850

Figure 4: Screenshot of the original content of “a.txt” file.

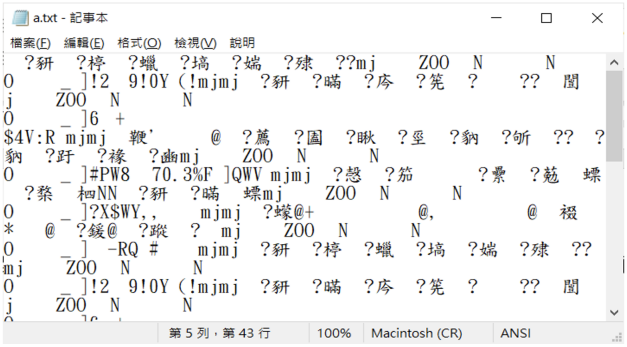

Figure 5: Screenshot of encrypted content of a.txt

sues. This lack of backup is the main cause of huge losses for businesses when faced with ransomware attacks.

Antivirus software has a good protection effect against general computer viruses, but can it effectively protect computer files from new and unknown ransomware? This issue deserves attention. Therefore, well-known antivirus software on the market are selected and compared to test the detection and defense capabilities of each method against various ransomware attacks.

This study prevents the continuous destruction of archives from three different types of ransomware threats. The protection rate of stored files is 98.82%. If the user does not place the file in C:\, then the protection rate can reach 100%, which is an excellent performance.

4.1 Simulate and Verify the Behavior of Ransomware

The behavior patterns of three different ransomware types are imitated in simulations A, B, and C to represent three new and unknown ransomwares for testing purposes. In addition, we create a plain text file named ”a.txt” to illustrate the file changes after going through different types of ransomware emulators. Figure 4. Screenshot of the original content of “a.txt” file.

Simulation A does NOT change file names or extensions but only encrypts the file contents. Figure 5 presents the encrypted content of “a.txt” file. After encryption,

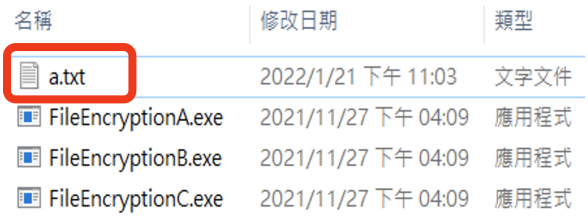

Figure 6: Screenshot of the file list after simulation program A is executed

Figure 7: Screenshot of the file list after simulation program B is executed

the file name has not been changed. Figure 6 shows the screenshot of the file list after simulation A. In simulation B, which encrypts files and appends the encrypted filename with ".xxx." Thus, the "a.txt" file is be renamed as "a.txt.xxx," as shown in Figure 7. Simulation C not only encrypts file contents but also renames file name by using random English + numeric strings, as shown in Figure 8.

4.2 Method to Prevent Ransomware from Continuously Destroying Files and Their Protective Effects

We proposes a method to prevent ransomware from continuously destroying files. Table 5 shows the results of attack tests from three different types of ransomware simulators. The numbers represent the files that were attacked, with 0 indicating that no files in that folder were attacked by the ransomware simulation. Faced with three different types of ransomware threats, the proposed method garners a protection rate of 98.82% for the computer files. If the user does not place the file in C:\, then the protection rate can reach 100%, which is an excellent performance.

Figure 8: Screenshot of the file list after the execution of the Type C emulator

Table 5: The results of attack tests from three different types of ransomware simulators.

Folder	A simulation program	B simulation program	C simulation program
C:\	10	10	10
C:\TEST	0	0	0
C:\Users\User\Desktop	0	0	0
C:\Users\User\Documents	0	0	0
C:\Users\User\Download	0	0	0
C:\Users\User\Music	0	0	0
C:\Users\User\Pictures	0	0	0
C:\Users\User\Videos	0	0	0
Total damage	10	10	10
Total not destroyed	840	840	840
Destruction rate	1.18%	1.18%	1.18%
Protection rate	98.82%	98.82%	98.82%
Stop time	< 60 second	< 60 second	< 60 second
	Force shutdown	Force shutdown	Force shutdown

4.3 Comparison Between the Proposed Method and Other Well-known Antivirus Software for Ransomware Protection

Antivirus software has a good protection effect against general computer viruses, but can it effectively protect computer files in the face of new and unknown ransomware? This issue deserves attention. Therefore, this study selects 16 commonly used sets of antivirus software in the market, as shown in the list of antivirus software to be tested in Table 6. All antivirus software is tested using the most common installation defaults for general users. Among them, the four sets of antivirus software (Avast Free Antivirus, Comodo Free Antivirus, Microsoft Defender, and Tinder Security) have anti-ransomware or advanced protection functions in their setting items, which need to be manually turned on. This study also manually starts the following settings and tests for these four sets of antivirus software, as follows: Avast Free Antivirus opens the default protected folder; Comodo Free Antivirus opens the Container; Microsoft Defender turns on controlled folder access; and Tinder Security - Turn on ransomware trapping.

Table 6: Antivirus software to be tested.

Item	Antivirus software
1	Avast Free Antivirus
2	AVG Antivirus Free
3	Avira Antivirus
4	Bitdefender
5	BullGuard Antivirus
6	Comodo Free Antivirus
7	F-Secure Safe
8	Kasperskey Free
9	McAfee Total Protection
10	Microsoft Defender
11	Panda Free Antivirus
12	PC-Cillin 2022
13	Vipre Advanced Security
14	Kinstnui
15	360 Total Security
16	Sysdiag

In the proposed method, 16 sets of antivirus software presets and four sets of antivirus software are set to manually open ransomware or advanced protection mode. Table 7 shows the test results of three different types of new and unknown ransomware simulation, and compares the protection rates of the proposed method and other well-known antivirus software.

In the results, 0% indicates that when the antivirus software faces ransomware emulators, all test files are encrypted and have no protection at all. According to the test results, 12 sets of antivirus software had no protection effect when faced with three different types of ransomware simulation. A set of antivirus software achieves no protection even when the advanced protection setting function is manually turned on. However, a different set of antivirus software shows a good protection effect against the attacks in simulations A or B, but has no protection against the attack in simulation C. Another set of antivirus software manually activates the ransomware trapping function, which has a good protection effect from attacks in simulations B and C, but has no protection against the attack in simulation A.

Meanwhile, the "Comodo Free Antivirus" software can completely block the attacks from three different types of ransomware simulations after manually enabling the Container function, yielding an impressive 100% protection rate for files. The proposed method and two other sets of antivirus software, Bitdefender and BullGuard Antivirus, achieve a protection rate of 98.82% when faced with the attacks from the three different types of ransomware simulation. Despite a very small number of test files loss, the abovementioned antivirus software also shows a good protection level.

Given the many antivirus software with no protection for the three different types of simulations, they cannot

Table 7: The test results of three different types of new and unknown ransomware simulation.

Item	Antivirus software	A simulation program	B simulation program	C simulation program
1	The proposed method	98.82%	98.82%	98.82%
2	Avast Free Antivirus default value	0%	0%	0%
3	Avast Free Antivirus enable default protected folder	0%	0%	0%
4	AVG Antivirus Free	0%	0%	0%
5	Avira Antivirus	0%	0%	0%
6	Bitdefender	98.82%	98.82%	98.82%
7	BullGuard Antivirus	98.82%	98.82%	98.82%
8	Comodo Free Antivirus default value	0%	0%	0%
9	Comodo Free Antivirus enable Container	100%	100%	100%
10	F-Secure Safe	0%	0%	0%
11	Kasperskey Free	0%	0%	0%
12	McAfee Total Protection	0%	0%	0%
13	Microsoft Defender	0%	0%	0%
14	Microsoft Defender enable Controlled Folder Access	56.47%	56.47%	56.47%
15	Panda Free Antivirus	0%	0%	0%
16	PC-Cillin 2022	70.59%	70.59%	70.59%
17	Vipre Advanced Security	98.82%	98.82%	0%
18	Kinstnui	0%	0%	0%
19	360 Total Security	0%	0%	0%
20	Sysdiag default value	0%	0%	0%
21	Sysdiag enable Ransomware lure	0%	98.82%	98.82%

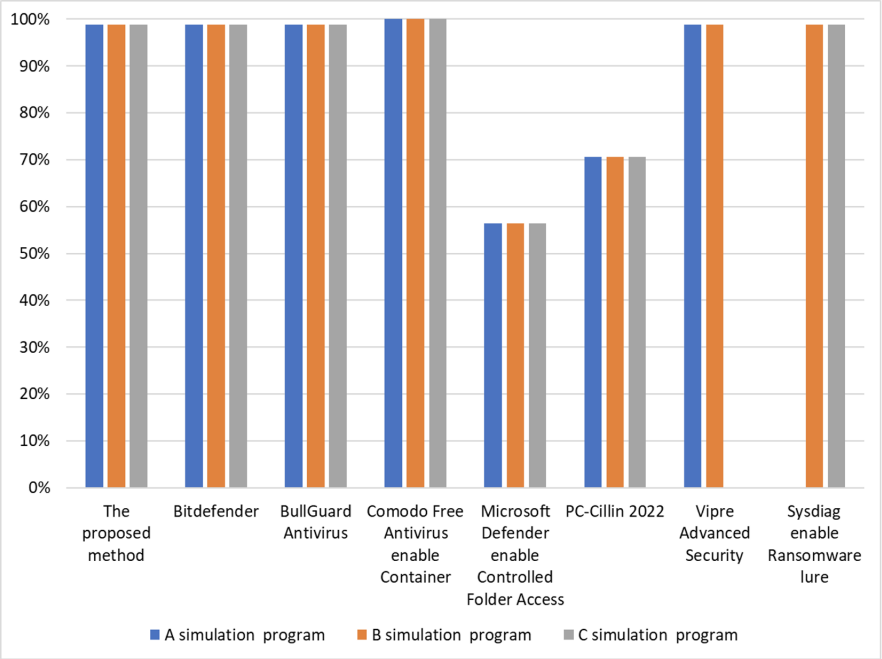

Figure 9: Comparison chart of the proposed method and other well-known antivirus software against ransomware protection (protection rate)

be clearly displayed in the comparison chart, and are thus removed. Figure 9 clearly shows the protection effect of antivirus software on new ransomware. The proposed method is comparable to well-known antivirus software in terms of protection against new and unknown ransomware.

The results of test experiments in Figure 9 present that the proposed method can effectively monitor and prevent ransomware from encrypting files. When faced with the threat of three different types of ransomware such as simulated programs A, B, and C, the method we proposed can effectively protect computer files, and the protection rate is 98.82% which is same with the methods of Bitdefender and BullGuard Antivirus. The Comodo Free Antivirus enable Container has the highest protection rate 0f 100%. However, if the files are not placed on the disk drive C:\, then this proposed method can detect ransomware and protect the files in time with the protection rate of 100%.

5 Conclusions

The results of the test experiments prove that the proposed method can effectively monitor and prevent file encryption from ransomware. When facing the threat of three different types of ransomwares, the proposed method can protect the computer files with a rate of 98.82%. If the files are not placed in C:\, then the protection rate can reach 100%, which shows excellent performance.

The test also reveals that when the antivirus software commonly used by users face new and unknown ransomware, only a few antivirus software have protective effects. Thus, the computer clearly has antivirus software installed, so why is it still infected with ransomware or computer virus? The current testing is limited to new and unknown ransomware threats, and thus may not be fair to antivirus software, which may have other good protection effects.

The proposed method can indeed protect computer files from the threat of ransomware. Thus, this method has high value, especially for users and enterprises with no file backup. This study focuses on the behavior pattern of ransomware as a method to detect and prevent it from encrypting and destroying files. The effect is the same for new and unknown ransomware. However, the proposed method does not have the functions of antivirus software and cannot replace its protection. The purpose of this study is to strengthen the existing antivirus software that cannot effectively detect and prevent computer files from being encrypted and damaged by new or unknown ransomware. The proposed method can work together with antivirus software to enable better protection effect for users' computer files.

Acknowledgments

This research was partially supported by the Ministry of Science and Technology, Taiwan, Republic of China under the Grant[MOST 111-2221-E-324-019-MY2]. The authors also gratefully acknowledge the helpful comments and suggestions of the reviewers, which have improved the quality.

References

[1] L. Abrams, "Computer giant acer hit by $50 million ransomware attack," Jan. 28, 2023. (https://www.bleepingcomputer.com/news/security/computer-giant-acer-hit-by-50-million-ransomware-attack)

[2] A. Adamov, A. Carlsson, "Reinforcement learning for anti-ransomware testing," in *Proceedings of 2020 IEEE East-West Design & Test Symposium (EWDTS'20)*, pp. 1–5, Sept. 2020.

[3] A. Brandt, "Python ransomware script targets esxi server for encryption," Jan. 28, 2023. (https://news.sophos.com/en-us/2021/10/05/python-ransomware-script-targets-esxi-server-for-encryption)

[4] M. Clark, "Hackers reportedly threaten to leak data from gigabyte ransomware attack," Jan. 28, 2023. (https://www.theverge.com/2021/8/9/22616882/gigabyte-technologies-ransomware-attack-data-leak-112-gb-ransomexx)

[5] L. Dignan, "Colonial pipeline cyberattack shuts down pipeline that supplies 45% of east coast's fuel," Jan. 28, 2023. (https://www.zdnet.com/article/colonial-pipeline-cyberattack-shuts-down-pipeline-that-supplies-45-of-east-coasts-fuel)

[6] N. Eliot, D. Kendall, and M. Brockway, "A flexible laboratory environment supporting honeypot deployment for teaching real-world cybersecurity skills," *IEEE Access*, vol. 6, pp. 34884–34895, 2018.

[7] W. Fan, Z. Du, D. Fernández, and V. A. Villagrá, "Enabling an anatomic view to investigate honeypot systems: A survey," *IEEE Systems Journal*, vol. 12, pp. 3906–3919, 2018.

[8] W. Fan, Z. Du, M. Smith-Creasey, and D. Fernández, "Honeydoc: An efficient honeypot architecture enabling all-round design," *IEEE Journal on Selected Areas in Communications*, vol. 37, pp. 683–697, 2019.

[9] ASUSTOR Community Forum, "Deadbolt ransomware," Jan. 28, 2023. (https://forum.asustor.com/viewtopic.php?f=45&t=12630)

[10] S. Gatlan, "Insurance giant cna reports data breach after ransomware attack," Jan. 28, 2023. (https://www.bleepingcomputer.com/news/security/insurance-giant-cna-reports-data-breach-after-ransomware-attack)

[11] J. Lee, J. Choi, G. Lee, S. W. Shim, and T. Kim, "Phantomfs: File-based deception technology for thwarting malicious users," *IEEE Access*, vol. 8, pp. 32203–32214, 2020.

[12] R. McMillan, "Ransomware hackers demand $70 million to unlock computers in widespread attack," Jan. 28, 2023. (https://www.wsj.com/articles/ransomware-hackers-demand-70-million-to-unlock-computer-in-widespread-attack-11625524076)

[13] C. Moore, "Reinforcement learning for anti-ransomware testing," in *Proceedings of 2016 Cybersecurity and Cyberforensics Conference(CCC'16)*, pp. 77–81, 2016.

[14] C. Pascariu, I. D. Barbu, "Ransomware honeypot - honeypot solution designed to detect a ransomware infection identify the ransomware family," in *Proceedings of the 11th International Conference on ELECTRONICS, COMPUTERS and ARTIFICIAL INTELLIGENCE (ECAI'19)*, pp. 1–4, 2019.

[15] S. Poudyal, D. Dasgupta, "Analysis of crypto-ransomware using ml-based multi-level profiling," *IEEE Access*, vol. 9, pp. 122532–122547, 2021.

[16] The Standard, "Fimmick ransomware attack puts over 35,000 people's data at risk," Jan. 28, 2023. (https://www.thestandard.com.hk/breaking-news/section/4/181793/Fimmick-ransomware-attack-puts-over-35,000-people%27s-data-at-risk)

[17] J. Venkatesh, V. Vetriselvi, Ranjani Parthasarathi, and G. Subrahmanya V.R.K. Rao, "Identification and isolation of crypto ransomware using honeypot," in *Proceedings of Fourteenth International Conference on Information Processing (ICINPRO'18)*, pp. 1–6, 2018.

[18] Wikipedia, "Aids (trojan horse)," Jan. 28, 2023. (https://en.wikipedia.org/wiki/AIDS_(Trojan_horse)

[19] D. Zhuravchak, T. Ustyianovych, V. Dudykevych, B. Vennyk, and K. Ruda, "Ransomware prevention system design based on file symbolic linking honeypots," in *Proceedings of 11th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS'21)*, vol. 1, pp. 284–287, 2021.

Biography

Yung-She Lin received his Master degree in Information Management from Chaoyang University of Technology, Taiwan. Currently He is a PhD. Candidate in the department of Information Management, Chaoyang University of Technology. His research interests include cryptography and information hiding.

Chin-Feng Lee received her Ph.D. in Computer Science and Information Engineering from National Chung Cheng University, Taiwan in 1998. She is currently a professor of Information Management at Chaoyang University of Technology, Taiwan. Her research interests include steganography, image processing, information retrieval and data mining.