Learning the Basic Structure of Several Ransomwares Using Static Analysis Technique

Amiruddin Amiruddin*, Candra Kurniawan, Eka Hero Ramadhani, Julio Rinaldi
Cyber Security Engineering Study Program
Politeknik Siber dan Sandi Negara

* amir@poltekssn.ac.id

Abstract. The ransomware can encrypt the files on the victim's device and then offer a keyword to decrypt them with a ransom of money. Information about the basic structure of ransomware is needed so that an antivirus can detect its presence. To find out the structure of ransomware, static and/or dynamic analysis can be done. In this study, ransomware analysis was performed using static techniques. The choice of static techniques was based on the ease of doing the analysis and also it does not need to run the malware sample being analyzed. The result of the research shows that of the six ransomware samples analyzed, it is known that all of the samples used almost the same structure in the form of imphash, ssdeep, and library and even samples come from the same family of ransomware.

1. Introduction

In this increasingly advanced digital age, ransomware is becoming a frightening attack because it can cause huge financial losses. The effects of ransomware attacks range from minor intrusions with relatively quick recovery to severe disruptions that can affect business operations [1][2]. Ransomware blackmalls computer users by locking access to their computers (called lockscreen ransomware) or data owners by locking access to their data by encryption (called encryption ransomware, crypto ransomware or cryptoware) [3]. With the ransom from the victim to pay for the decryption key, of course the attacker gets abundant financial benefits. Even if a ransom has been paid, the data is not guaranteed to be recovered [4]. This is inline with the Midyear Cybersecurity Report released by Cisco Systems in 2016 which states that the cryptoware, a type of ransomware, is recognized as the most beneficial malware in history for its creators [5] and it is estimated that hundreds of millions of dollars have been successfully obtained by the makers from the results of squeezing the victim within one year [6].

Ransomware threats targeting home user, companies, and even critical telecommunication [7]. Ransomware attacks data or files on the victim's computer even though the data is a valuable asset for the success of a business and organization [8]. Data is part of the information that must be guaranteed availability so that it can be accessed by users to be used as intended [9]. therefore, data must be avoided from ransomware coverage.

Researchers offer ways to prevent ransomware from updating vaccination systems [10], access control [11], to static and dynamic analysis [12][13] to recognize the characteristics of ransomware. In this study we focus to prevent ransomware attacks through malware analysis. This aims to provide information in response to intrusion of computers or networks and determine what happens to ensure a computer is exposed to malware or not. Malware analysis can be done with two basic approaches namely static and dynamic. Static analysis is done by testing the executable file without running the file. Static analysis can show whether a file is malware and provide information about the functionality of the malware. In contrast to static analysis, dynamic analysis is carried out by running malware and analyzing its behavior using an isolated system. However, dynamic analysis requires a new environment to run malware so
that it does not have a negative impact on resources that are around or connected to the analysis environment. This necessity requires more memory resources [14][15]. Meanwhile, malware detection continues to be a challenge because malware makers continue to try to avoid and distort malware detection methods. Most antivirus software uses signature-based detection namely unique identification for binary files, which is created by analyzing binary files using static analysis methods [15][16]. Therefore, in this study static analysis of ransomware is carried out which aims to find out its basic structure, so that in the future it can be used to detect the presence of ransomware on the device used.

2. Method and materials

2.1. Sample preparation

To do the analysis, we first prepared some malware samples as given in Table 1. All these files will be explored using static analysis method to learn their basic structure.

| Malware sample # | Original name       |
|------------------|---------------------|
| Sample 1         | smb-b_8ti77.bin     |
| Sample 2         | smb-5ebgzza0.tmp    |
| Sample 3         | smb-7teux2sm.exe    |
| Sample 4         | smb-onil0o36.bin    |
| Sample 5         | smb-ts5zof3r.tmp    |
| Sample 6         | smb-zxck4paa.tmp    |

2.2. Method

In this study, the method used for analysis the samples of ransomware are scanning using Virustotal, investigation using PEStudio, and analysis of the obtained results, which is explained as follows. 1. Scanning with virustotal. The first step is to upload the file to Virustotal, an online scanner that uses antivirus databases throughout the world. By using virustotal data obtained by any antivirus that can detect the file as malware or even detect it as ransomware, and even vice versa i.e. it cannot detect the file as malware. In addition to that, Virustotal was also found to be associated with fingerprints, file types, and other names of uploaded malware. 2. Investigation with PEStudio. PEStudio is an application used to find out strings, libraries, and signatures. The results obtained from virustotal and PEStudio applications are almost the same, but they support each other. 3. Analysis of the results obtained. The next step is to look for similarity of the two samples tested on Virustotal and PEStudio to determine the structure of the underlying ransomware.

3. Results and discussion

In this study, there are six samples of ransomware have been analyzed as given in Table 1, according to the stages previously described, i.e. scanning with Virustotal, investigating with PEStudio, and analyzing the results. However, the discussion of the results of the analysis is sorted by samples as follows.
Sample 1

The first ransomware sample is a file with the name smb-b_8ti77_.bin. Based on the results obtained using Virustotal there were 53 of 66 antiviruses that detect this sample file as malware as shown in Figure 1. Based on Table 2, it is known that this file is a Portable Executable (PE) file. However, of the 53, only 11 antiviruses that detect it as ransomware, while others are only able to detect as a trojan. This shows that there are still many antiviruses that have not been able to detect ransomware. Some antiviruses that do not detect this malware are Avira, Baidu, Cyren, Kingsoft, TotalDefense, ViRobot, Avast-Mobile, Babable, Bkav, F-Secure, SUPERAntiSpyware, Trustlook, and Zoner. This ransomware has several names which are obtained when scanning using Virustotal.

Figure 1. Scanning sample 1 using Virustotal

Figure 2. Aliases of sample 1

A malware will usually disguise itself with various aliases. Sample 1 has the alias name as given in Figure 2. Besides information about the detection of the antivirus, we also gained basic parameters such as MD5, SHA-1, SHA-256, autentihash, imphash, SSDEEP, file type, target, and file size of sample 1, as summarized in Table 2. Apart from Virustotal, PEStudio application is also used in this study. PEStudio gives almost the same results as Virustotal. The following results use the PEStudio application.
Table 2. Other basic parameters of sample 1

| Parameter     | Value                                                                 |
|---------------|----------------------------------------------------------------------|
| MD5           | 43115dc539f8b8c8fd8b47b2b88e409a88                                  |
| SHA-1         | 5a78a4e6d8eefb4a4f1e6ed35544c961d2d2b89e9939d                       |
| SHA-256       | 9ce6f363f8d4daaaaa437cbf97c0d0f97293b0d6f87ac30bf3b2a8aca09353      |
| Imphash       | 6dad54c96d96295e9eca1e7cc2ce681652                                  |
| SSDEEP        | 536:RgHRJ3E6kIMW6XbdTkYHrlTc4m4G5Qy9WcFe-CHRJ3d6kEW0h9L8ttV        |
| File Type     | Win32 EXE                                                             |
| Target        | PE32 executable for MS Windows(GUI) Intel 80386 32-bit              |
| File Size     | 288 KB (294912 bytes)                                               |

In Figure 3, first-bytes-hex (line 1) shows 4D 5A and first-bytes-text shows MZ (line 2). This indicates that the file is portable executable. Then there is also information about the signature and compiler-stamp that indicate that the ransomware was made on March 22, 2017 using the Microsoft Visual C++ v6.0. In addition, library information is also used to run the malware. A malware has a small size because it will utilize the existing library on a PC or device by using the call function [17]. The libraries that this ransomware use to run are given in Figure 4 where the first three libraries are blacklisted, and the file description is as follows. W2-32.dll is a windows socket, kernel32.dll is a Windows NT base API client dll., user32.dll is a multi-user, advapi32.dll is an advanced Windows 32, and msvcr.dll is a Windows NT CRT DLL.

![Figure 3. Scanning result using PEStudio](image)

![Figure 4. Libraries used by sample 1](image)

Sample 2

The ransomware sample 2 was analyzed in similar manner to sample 1. Sample 2 has the file name smb-5ebzzza0.tmp and the original file name is 60b377c3d9e087273a5824b70-54839f1b307e6ad3b7def71d2a4ca9e8ed110581.bin. This file is indicated as ransomware based on the results of a scan using Virustotal. 56 antiviruses are able to detect this file as malware, 21 antiviruses are able to detect it as ransomware, and the remaining antiviruses only detect it as a trojan or a malicious application. In addition, there are also well-known antiviruses but not able
to detect this malware for example Avast, Baidu, and others. Some antiviruses which are unable to detect this malware are Avast-Mobile, Baidu, F-Secure, The Hacker, Trustlook, ViRobot, Avira, Kingsoft, Bkav, F-Secure, TotalDefense, and Zoner. It is known that sample 2 is a portable executable file type. Then an analysis was performed using the PEStudio and the result, as in Figure 5, showed that sample 2 is Portable Executable file. Libraries used by sample 2 are ws2_32.dll, netapi32.dll, mpr.dll, kernel32.dll, advapi32.dll, msvcr.dll, where the first three libraries are blacklisted.

Sample 3
The analyzed ransomware 3 sample has the name smb-7teux2sm.exe and the original name of the file is 7b2f8c43b4ec92f2b2add9fceu264e92668dace2530493c51c5d6b45dc7b64e208ed.bin. Based on the results of a scan using Virustotal it is known that 59 of 68 antiviruses are able to detect this file as malware, while the remaining 9 antiviruses do not detect this file as a malicious file. Based on analysis using the PEStudio application, it is known that this malware uses five libraries that are used as call functions namely ws2_32dll, kernel32.dll, user32.dll, advapi32.dll, and msvcr.dll, where library ws2_32.dll is blacklisted.

Sample 4
The analyzed ransomware 4 sample has the name smb-onil0o36.bin and the original file name is e906e8c65d9d42582ea3874bc0a388936dbbe4bc4fc89432db01c0995146c18d2.bin. Based on the results of a scan using Virustotal, it is known that 60 of 69 antiviruses are able to detect this file as malware, while 10 other antiviruses cannot detect that this file is dangerous. This sample used five libraries, known from the scanning using the PEStudio application, namely ws2_32.dll, kernel32.dll, user32.dll, advapi32.dll, and msvcr.dll, where the first library is blacklisted.

Sample 5
The analyzed ransomware 5 sample has the name smb-ts5zof3r.tmp and has the original name 31ddc7fe6adb62938b2d021cc9d557f0293fe4fd0c225c2368d8d98a4da119d.bin. Based on the results of the scan using Virustotal, it is known that from 55 out of 65 antiviruses can detect this file as malware, while 15 other antiviruses cannot detect files as dangerous files. There are six libraries in this sample, namely, ws2_32.dll, netapi32.dll, mpr.dll, kernel32.dll, advapi32.dll, and msvcr.dll, where the first three libraries are blacklisted.

Sample 6
This sample has the file name smb-zxck4paa.tmp and this malware also has the same original name, smb-zxck4paa.tmp. Based on Virustotal it is known that from 58 of 68 antiviruses can detect this file as malware while 10 other antiviruses cannot detect this file as a malicious file. This sample has five libraries namely, ws2_32.dll, kernel32.dll, user32.dll, advapi32.dll, msvcr.dll where only ws2_32.dll is blacklisted.

Samples comparison
To see the difference or similarity in the basic structure of all the samples that have been studied, the comparison of parameters of all samples is given in Table 3, where tick sign (√) means the ransomware sample uses the corresponding parameters.
Table 3. Samples comparison

| Parameter | Value | Sample |
|-----------|-------|--------|
|           |       | 1      | 2      | 3      | 4      | 5      | 6      |
| Imphash   |       | ✓      | -      | -      | -      | -      | -      |
|           | a49ad1d64126f3ac266ed2f5f4e2219 | -      | ✓      | -      | -      | ✓      | -      |
|           | 2b018f96d7cdaf0b915d2c1dcb16595c4 | -      | -      | ✓      | -      | -      | -      |
|           | 64db760a6cfba3323cae0d6629a80725a | -      | -      | -      | -      | -      | -      |
| SSDEEP    | 1536:RgHRJs3EU6kifMWOxTjk (shortened) | ✓      | -      | -      | -      | -      | -      |
|           | 24576:BX13b5RFB9HevDYv8v871 (shortened) | -      | ✓      | -      | -      | ✓      | -      |
|           | 768:1W8+9FisiTNdzkHLCLTXn (shortened) | -      | -      | ✓      | ✓      | -      | -      |
|           | 384:N73vq0yEXDBAFVPd3leq (shortened) | -      | -      | ✓      | ✓      | -      | ✓      |
| Library   | ws2_32.dll (blacklist) | ✓      | ✓      | ✓      | ✓      | ✓      | ✓      |
|           | netapi32.dll (blacklist) | ✓      | ✓      | -      | -      | ✓      | -      |
|           | mpr32.dll (blacklist) | ✓      | ✓      | -      | -      | -      | -      |
|           | kernel32.dll | ✓      | ✓      | ✓      | ✓      | ✓      | ✓      |
|           | advapi32.dll | ✓      | ✓      | ✓      | ✓      | ✓      | ✓      |
|           | msvcrt.dll | ✓      | ✓      | ✓      | ✓      | ✓      | ✓      |
|           | user32.dll | -      | ✓      | -      | ✓      | ✓      | ✓      |

Based on the Table 3, it is known that samples 2 and 5 as well as samples 3 and 4 have the same values for all compared parameters, whereas sample 1 as well as sample 6 has the different value. This shows that the two samples have the same structure, but there are different attributes that cause the MD5 and SHA hash values to be different or change. Therefore, we can state that there are four different family of ransomware found in this study e.g. fam1 (sample 1), fam2 (sample 2 and 5), fam3 (sample 3 and 4) and fam4 (sample 6). In addition, in library parameter, library ws2_32.dll is blacklisted in all samples. Blacklist library is an API function from Windows that can be used to run potentially dangerous files and to that end, all the analysed samples use the library ws2_32.dll to run the ransomware. The two other blacklisted libraries should be considered potential for running the ransomware.

Conclusion

Ransomware has a basic structure that shows its existence. In general, malware uses the library as a function call to run on infected systems. In the analyzed ransomware samples, samples 1, 2, and 5 have six libraries and samples 3, 4, and 6 have five libraries. There are four libraries used generally by all samples, namely ws2_32.dll, kernel32.dll, advapi32.dll, msvcrt.dll. Also, there are 3 blacklisted libraries e.g. ws2_32.dll, netapi32.dll, and mpr32.dll which are very likely to be potential to run dangerous files. Of all the samples, there are 2 samples come from the same family of ransomware since they have the same imphash and ssdeep values. Therefore, the basic structure of ransomware in the form of imphash, ssdeep, and library values can be used to make an Indication of Compromise (IoC) for ransomware detection or to be an update recommendation for antivirus that cannot detect the type of ransomware.

References

[1] L. Y. Connolly, D. S. Wall, The rise of crypto-ransomware in a changing cybercrime landscape: Taxonomising countermeasures, Computers & Security, Volume 87, 2019, pp. 1-17
[2] P.B. Pathak, Y.M. Nanded, A dangerous trend of cybercrime: ransomware growing challenge. Int. J. Adv. Res. Comput. Eng. Technol. 5 (2), 2016, pp. 371–373
[3] D. Morato, E. Berrueta, E. Magaña, and M. Izal, “Ransomware early detection by the analysis of file sharing traffic,” J. Netw. Comput. Appl., vol. 124, 2018, pp. 14–32
[4] Ferdiansyah, “Analisis Aktivitas dan Pola Jaringan Terhadap Eternal Blue & Wannacry Ransomware,” JUSINFO, vol. 4, 2018, pp. 37-48
[5] Cisco, “Midyear Cybersecurity Report,” Cisco Systems, 2006.
[6] Symantec, “Ransomware and Businesses 2016,” Tech. Rep Symantec Corporation, 2006.
[7] M. Akbanov, V.G. Vassilakis, & M.D. Logothetis, “WannaCry Ransomware: Analysis of Infection, Persistence, Recovery Prevention and Propagation Mechanisms,” Journal of Telecommunications and Information Technology, 1, 113-124, 2019.
[8] Z. Faheem et al., “Trustworthy Data: A Survey, Taxonomy and future trends of Secure Provenance Schemes,” J. Netw. Comput. Appl.
[9] M.E. Whitman, and J. M. Herbert, Principles of Information Security, 4th edition. KY: Cengage: Independence, 2009
[10] A. Saxena, H.K. Soni, Strategies for ransomware removal and prevention. 4th International Conference on Advances in Electrical, Electronics, Information, Communication and Bio-Informatics 27-28 February 2018
[11] S. Parkinson, Use of access control to minimize ransomware impact. Netw. Secur. (7), 2017, pp. 5–8
[12] I. Kara and M. Aydos, "Static and Dynamic Analysis of Third Generation Cerber Ransomware," 2018 International Congress on Big Data, Deep Learning and Fighting Cyber Terrorism (IBIGDELFT), ANKARA, Turkey, 2018, pp. 12-17.
[13] S. Hsiao and D. Kao, "The static analysis of WannaCry ransomware," 2018 20th International Conference on Advanced Communication Technology (ICACT), Chuncheon-si Gangwon-do, Korea (South), 2018, pp. 153-158.
[14] M. Sikorski and A. Honig, Practical malware analysis: the hands-on guide to dissecting malicious software. San Francisco: No Starch Press, 2012.
[15] T.A. Cahyanto, V. Wahanggara, and D. Ramadana, “Analisis dan Deteksi Malware Menggunakan Metode Malware Analisis Dinamis dan Malware Analisis Statis,” JUStINDO, vol. 2, 2018, pp. 19–30.
[16] P. Shijo and A. Salim, “Integrated Static and Dynamic Analysis for Malware Detection,” Procedia Comput. Sci., vol. 46, 2015, pp. 804–811
[17] Anonymous, “Process Library,” ProcessLibrary, 2004 [online] available at https://www.processlibrary.com/en/