LockBit Black Ransomware On Reverse Shell: Analysis of Infection

Ransomware LockBit Black di Dalam Reverse Shell: Analisis Infeksi

Eliando*[1], Ary Budi Warsito[2]
[1,2]Universitas Matana; ARA Center,
Jl. CBD Barat Kav. 1. Gading Serpong, Tangerang - 15810, Indonesia,
Telp 021-29232999
[3]Teknik Informatika, FSTEM, Universitas Matana
e-mail: *[1]eliando@matanauniversity.ac.id, [2]ary@matanauniversity.ac.id

Abstract

This research was conducted due to the widespread occurrence of ransomware attacks, especially in Indonesia, against data that is at the endpoint and has even reached the banking sector, to estimate the likelihood of future ransomware infections. LockBit 3 ransomware aka LockBit Black is ransomware that has penetrated one of the banks in Indonesia, along with a reverse shell which is an infection method that cannot be recognized by every protection so that when combined it can penetrate all sides of protection. The method used to research the combination of ransomware and reverse shell is a hybrid analysis with a combination of static and dynamic analysis, to see every capability that can be carried out by the LockBit Black ransomware and channeled through the reverse shell. In this research, we can see the real impact of the attack and estimate protection in the future from the results of this analysis so that variant ransomware attacks from LockBit can be overcome.

Keywords—Ransomware, LockBit Black, Reverse, Shell, Infection

Abstrak

Penelitian ini dilakukan dikarenakan cukup maraknya serangan ransomware khususnya di Negara Indonesia terhadap data-data yang berada di Endpoint bahkan sudah sampai ke sektor perbankan, sistem keamanan yang cukup ternyata belum menjadi jaminan keamanan terhadap di dalam lingkungan, untuk itu analisa terhadap kemampuan infeksi harus terus dilakukan untuk memperkirakan kemungkinan terjadinya infeksi ransomware di kemudian hari. Ransomware LockBit 3 alias LockBit Black merupakan ransomware yang sempat menembus salah satu perbankan di Indonesia, beserta reverse shell yang merupakan metode infeksi yang tidak dapat dikenali oleh setia perlindungan sehingga apabila digabungkan memiliki kemungkinan untuk dapat menembus semua sisi perlindungan. Metode yang digunakan untuk meneliti kombinasi ransomware dan reverse shell adalah hybrid analysis dengan kombinasi static dan dynamic analysis, untuk melihat setiap kemampuan yang dapat dilakukan oleh ransomware LockBit Black dan disalurkan melalui reverse shell.Di dalam penelitian ini kita dapat melihat dampak real dari serangan tersebut dan memperkirakan proteksi di kemudian hari dari hasil analisa ini sehingga serangan ransomware variant dari LockBit dapat di atasi.

Kata kunci—Ransomware, LockBit Black, Reverse, Shell, Infeksi

1. INTRODUCTION

Cyber security will never stop right here and right now there will always be something new about it, including one of the malicious software that asks for ransom or commonly known as ransomware, many people when facing a ransomware attack only focus on the name of the ransomware and try to look for information even when someone developed a decryptor on the Internet, without realizing it, the ransomware attack managed to enter the system environment due to the success of other malicious software that went undetected like Trojan horses malware. These weapons of malware are often used to disguise real attacks and this technique of hiding attacks is very effective, especially in malicious software attacks, especially detonating ransomware. The techniques used in trojans can be used as tools or can be said to be operators in running various kinds of malware actions, even in some studies there are trojan horses that can be used in the form of hardware or trojan horse hardware, which essentially hides very dangerous malware attack activities [1].

Every organization at this time has used technology quite a lot as a tool to expand its business, be it private or public industry, therefore every organization will not be spared from cyber attacks, including financial services organizations where banking is the target of various kinds of attacks both traditional attacks such as robberies and cyber attacks where these attacks are used to take advantage of cybercriminals [2]. Reasonably everyone in Indonesia was shocked by the news that one of the banks in Indonesia was hit by a LockBit 3.0 attack, aka LockBit Black, as seen in Figure 1, and all the data has been successfully retrieved and ready to be sold on the dark web, after previously in early 2022, Indonesia was shocked by the news that the Bank of Indonesia hit by conti ransomware attack.

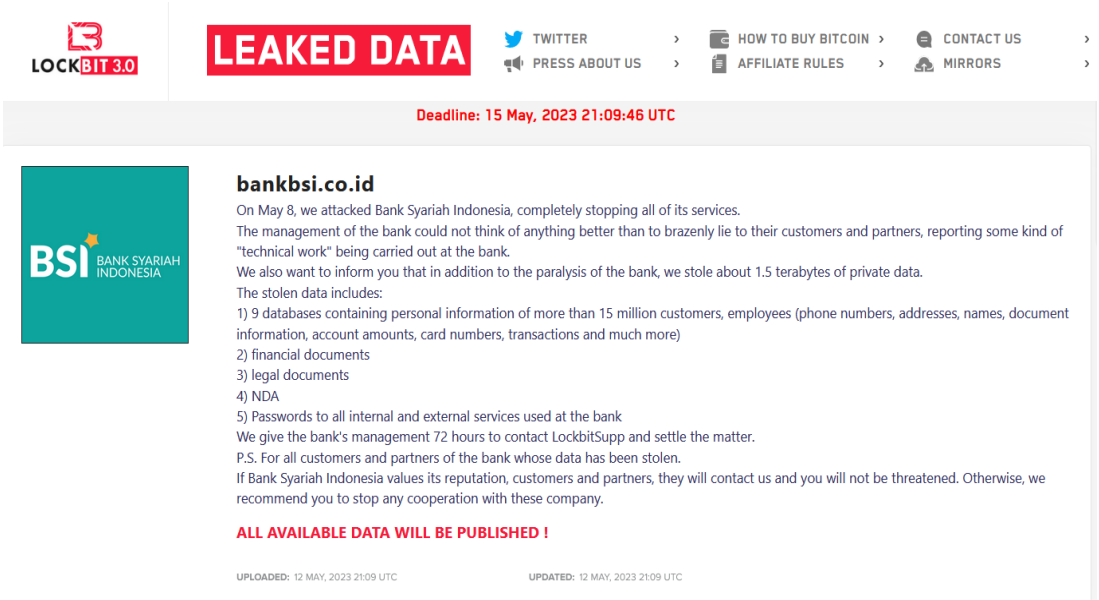

Figure 1 LockBit 3.0 Ransomware
(Source:https://tekno.kompas.com/read/2023/05/15/12450037/mengenal-ransomware-LockBit-30-yang-diduga-serang-bsi-dan-cara-kerjanya?)

This means that ransomware attacks have been very massive in Indonesia and it is necessary to carry out routine analysis of each of these ransomware. The analysis carried out aims to see the impact of the ransomware attack and also see all the possibilities that exist for the emergence of the latest variant of ransomware, considering that now everyone familiar with the concept of ransomware as a service, where ransomware is used as a service, and this is a cybercrime business model, where a ransomware operator writes another software and its affiliates or using operators

person with a revenue sharing system to launch an attack using that software and embed the ransomware in a company [3].

Based on the monthly monitoring report conducted by the National Cyber and Crypto Agency or BSSN, as of December 2022, as shown in Figure 2, malware is still developing very significantly, more than fifteen thousand attack anomalies in Indonesia in December 2022 were caused by Malware, one of which is ransomware, and LockBit 3 aka LockBit Black is one of them and this threat must be taken seriously, but things that need to be concern is why ransomware that has been known before by making the latest variant but every computer security devices that have existed before in banking cannot deal with it and produce an attack that has a very dangerous impact.

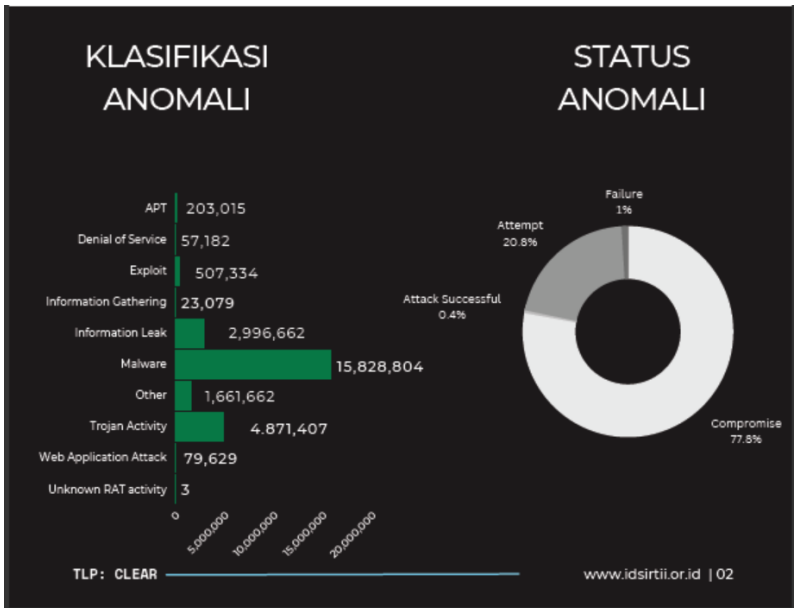

Figure 2 BSSN Monthly Monitoring Report December 2022 Page 3

Even according to the bleeping computer, the LockBit 3.0 attack still ranks second, which occurred in February 2023, as seen in Figure 3

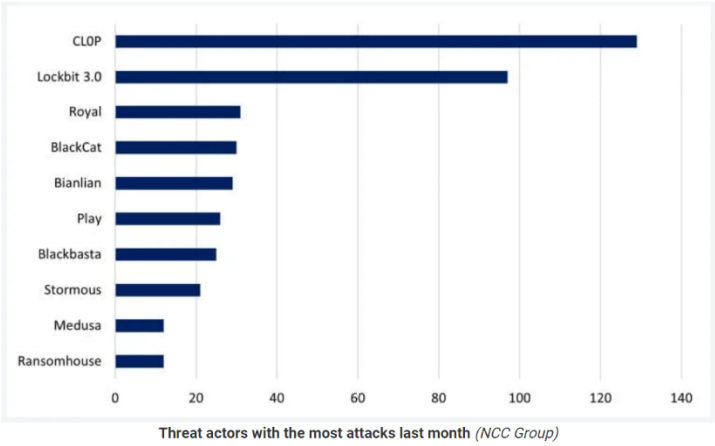

Figure 3 Top Ten Ransomware Most Attack

(Source: https://www.bleepingcomputer.com/news/security/march-2023-broke-ransomware-attack-records-with-459-incidents/)

Even on March 16, 2023 joint Cybersecurity Advisory (CSA) which is a combination of The

Federal Bureau of Investigation (FBI), the Cybersecurity and Infrastructure Security Agency (CISA), and the Multi-State Information Sharing & Analysis Center (MS-ISAC), has issued an analysis guide regarding the ransomware, this shows that many cybersecurity platforms are aware of LockBit 3 aka LockBit Black as seen in Figure 3, so this research will provide technical reasons or methods so that LockBit 3 aka LockBit Black ransomware is not recognized by all cybersecurity tools [4]. One possible method that ransomware can use to gain authorization from an operating system that has been protected by an anti-virus or endpoint protection device is to use a reverse shell, in which the attacker can gain control through the victim's operating system and can execute any command by generating an interactive shell, or even run a pre-prepared script which could be ransomware [5].

Figure 4 LockBit 3 aka LockBit Black

Of the many attacks that have been successfully carried out by the LockBit 3.0 ransomware in the last few months and almost a year for example in Figure 4, LockBit 3.0 aka LockBit Black attacks are still rampant, and there has been no in-depth research conducted on the LockBit 3.0 ransomware in the form of scientific publications, so in this paper at least do an in-depth analysis of LockBit 3.0 to prevent or even stop it immediately before the LockBit 3.0 ransomware spreads or even makes its variants[6], this research is needed so that many people also know that to deal with ransomware attacks is not only closing access to the ransomware either through the network or anti-virus but also looking at all the possibilities that exist, one way to spread this ransomware is by using a reverse shell as an exploit [7].

2. RESEARCH METHOD

In this research method section, researchers will show how it is possible that LockBit 3.0, aka LockBit Black, can infect one of them by using what we know as a reverse shell, the method that will be applied is shown in Figure 5.

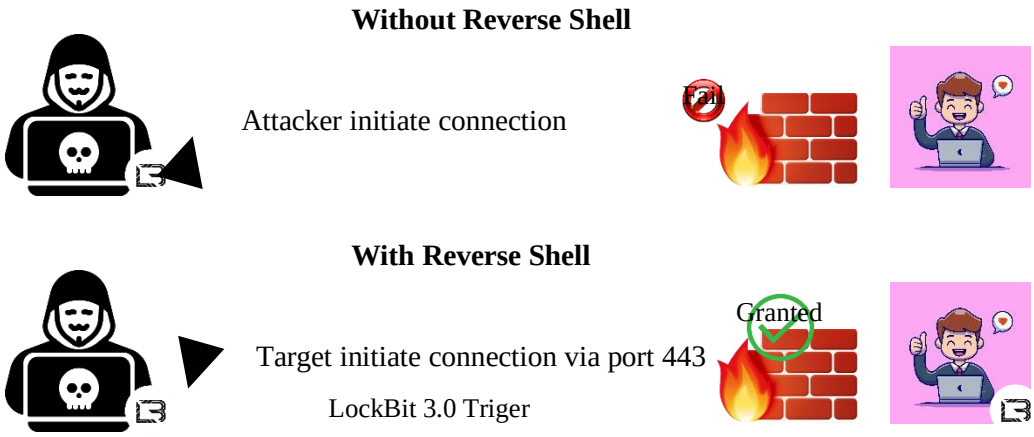

Figure 5. Reverse Shell

This research uses a reverse or known as a connect-back shell method. This method is often used to bypass the existing anti-virus on each device or the AntiMalware Scan Interface (AMSI) Signature on each device [8], which is a versatile interface standard that allows applications and services to integrate with any existing antimalware product on the machine, this method is being developed by several ransomware including LockBit which will spawn a new type variant with the same method, by using a reverse shell, the operating system will think that the shell that was sent was based on a request from itself so that the connection will be ignored by the operating system protection, which we know as anti-virus [9]. In this research, the reverse shell or connect-back shell that will be used as an example is the reverse shell which is currently being widely used, namely hoax-shell where with LockBit 3.0 ransomware infection aka LockBit Black using hoax-shell like in Figure 6, that will avoid detection from protection at each endpoint. In the following picture we can see that the reverse shell tried to generate a command in the powershell to make the target initiate to allow the attacker or hacker to attack or detonate LockBit 3.0 ransomware aka LockBit Black.

Figure 6 Example of Reverse Shell

In this research study, the anti-virus from the Windows operating system, which is Windows Defender, is activated, with an up-to-date antivirus database and real-time blocking capabilities and protection against ransomware is turned on, as seen in Figure 7

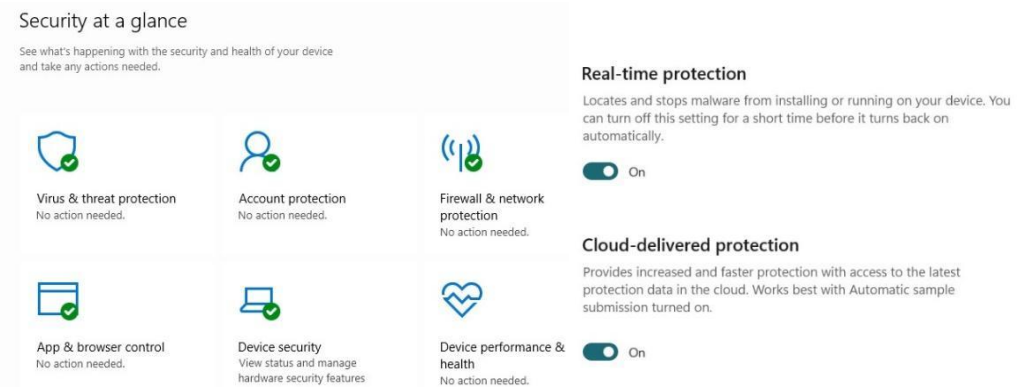

Figure 7 Windows Defender Active

The sample used this time consists of LockBit 3.0 and LockBit 3.1 files with hashes and details shown in Table 1

Table 1 LockBit 3.0 Components

	LockBit 3.1 Components
MD5	A8E0D56F8C67F1F7B6E592C12D87ACAB
SHA1	ED555F0162EA6EC5B8B8BADA743CFC628D376274
SHA256	C690148B6BAEC765C65FE91EA9F282D6A411AE90C08D74D600515B3E075E21B2
File Type	Portable Executable for 80386
Size	162816 Bytes
	Encryption LockBit 3.0 Components
MD5	7FB11398C5BE61445BEE1EFA7C9CAA31
SHA1	CED1C9FABFE7E187DD809E77C9CA28EA2E165FA8
SHA256	F9B9D45339DB9164A3861BF61758B7F41E6BCFB5BC93404E296E2918E52CCC10
File Type	Portable Executable for 80386
Size	166400 Bytes

This research method that uses is by seeing every movement of infection from LockBit 3.0 ransomware aka LockBit Black using a hybrid model by combining static analysis and dynamic analysis, from each of these analysis techniques several things can be found that allow predictions to be made about what the next malware infection model will look like, this method can be used to prevent things that will happen in the future, especially to explain how the method used by malicious software, in this case, ransomware, infects the computer device that is being used.

2.1 Static Analysis

The first method used is static analysis, this static analysis method is a method that is more or less similar to signature-based analysis or statistical-based analysis, in this technique what you want to look for are typical behaviors and statistical indications on most malware or ransomware, which use forensics clues so that programs like antivirus can detect whether this is malware or not. To do this static analysis, you must have a file to analyze and the file does not need to be run, the file will be analyzed to see how the opcode sequences and also the control flow graphs are, so that we can estimate whether it is similar to the Malware or ransomware being studied, including the string Extraction of executable files is the usual method for viewing

suspicious programs, viewing their signatures and obfuscated packages, viewing libraries used by functions and so on, even in static analysis techniques the file is dissected or disassembled every code used so that it can be reverse engineering is carried out by looking at the structure, function and sequence of processes in the code [10].

2.2 Dynamic Analysis

In the second method, namely dynamic analysis, then the program that is suspicious or dangerous is run, but to carry out dynamic analysis it must be run in a safe environment, such as a sandboxing environment that is isolated from various devices on the network, virtualization is usually used with a network that is not connected anywhere or isolated, which will not affect the actual system, with this dynamic analysis technique it is an improvement over the static analysis technique, but it is also difficult to do, for example it is very difficult to see obfuscate code after it is executed compared to static binary-code, all changes in the system can be carried out by the malicious software so that the analysis tends to be more difficult, what can be seen is monitoring any changes caused by the malware or ransomware along with the possibility of encryption used, but sophisticated malware can hide every activity so it is much more difficult to monitor, so it needs to be done static analysis first to determine whether the file will run on the operating system or not [11].

2.3 Hybrid Analysis

Hybrid analysis is a combination of the two methods, namely static analysis and dynamic analysis, which in principle both static and dynamic analysis must be carried out on the same file or activity to get accurate results and estimate what infection method might be used next [12], as shown in the figure 8

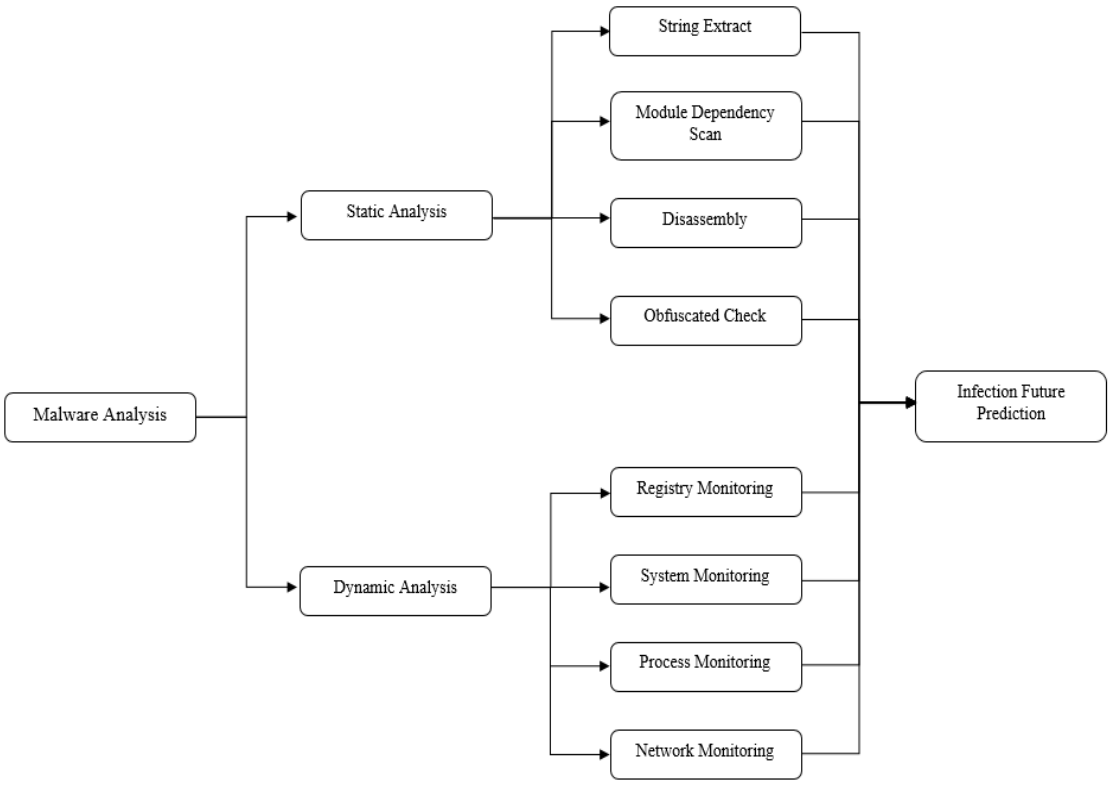

Figure 8 Malware Infection Analysis

3. RESULT AND DISCUSSION

To get the results from this research, many tools are needed to analyze everything, the tools that will be used in this research are standard analysis tools such as IDA Pro, PEStudio, Process Hacker, etc., which will later be used to see the correlation between LockBit Black Ransomware and see what infection methods were used and the possibility in the future [13].

3.1 PE LockBit 3.0 Ransomware

The first time this research used IDA Pro to disassemble Portable Executable files from LockBit Black with information as shown in the image below

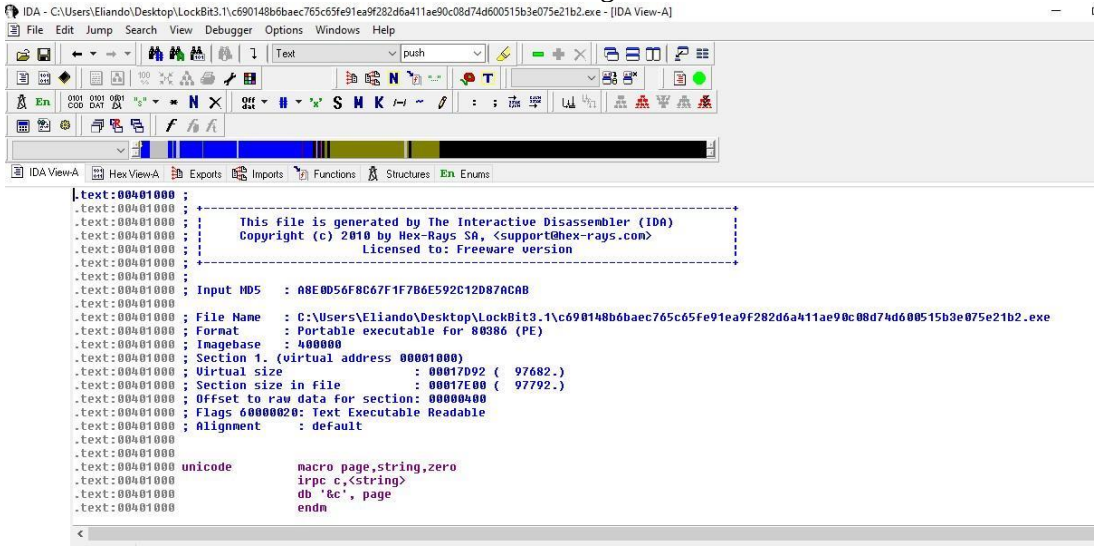

Figure 9 IDA Pro

By using the IDA Pro tools for disassembly the malware like on Figure 9, we can reverse engineer each OpCode, so that you can see everything that the executable file does before it is run, for example, as shown in the command line below, there is an OpCode using kernel32.dll which is imported for change the dword value in the registry, even run the command line and provide error information that will be requested to be handled by the operating system for the error message [14].

```
; Imports from KERNEL32.dll
; Segment type: Externs
; _idata
; HMODULE __stdcall GetModuleHandleW(LPCWSTR lpModuleName)
                extrn GetModuleHandleW:dword ; DATA XREF:
.text:00418D6Er
 ; void __stdcall SetLastError(DWORD dwErrCode)
                 extrn SetLastError:dword ; DATA XREF: .text:00418D8Cr
 ; HMODULE __stdcall LoadLibraryW(LPCWSTR lpLibFileName)
                 extrn LoadLibraryW:dword ; DATA XREF: .text:00418D86r
 ; HMODULE __stdcall LoadLibraryExA(LPCSTR lpLibFileName,HANDLE
hFile,DWORD dwFlags)
                 extrn LoadLibraryExA:dword ; DATA XREF:
.text:00418D80r
 ; DWORD GetTickCount(void)
                 extrn GetTickCount:dword ; DATA XREF: .text:00418D7Ar
 ; FARPROC __stdcall GetProcAddress(HMODULE hModule,LPCSTR lpProcName)
                 extrn GetProcAddress:dword ; DATA XREF:
.text:00418D74r
```

```
 ; HMODULE __stdcall GetModuleHandleA(LPCSTR lpModuleName)
                 extrn GetModuleHandleA:dword ; DATA XREF:
.text:00418D68r
 ; DWORD GetLastError(void)
                 extrn GetLastError:dword ; DATA XREF: .text:00418D62r
 ; DWORD __stdcall GetFileAttributesW(LPCWSTR lpFileName)
                 extrn GetFileAttributesW:dword ; DATA XREF:
.text:00418D5Cr
 ; LPWSTR GetCommandLineW(void)
                 extrn GetCommandLineW:dword ; DATA XREF:
.text:00418D56r
 ; UINT __stdcall GetAtomNameW(ATOM nAtom,LPWSTR lpBuffer,int nSize)
                 extrn GetAtomNameW:dword ; DATA XREF: .text:00418D50r
```

Meanwhile, as seen in figure 10, each hash of the executable file be it MD5, SHA1, SHA256 can be seen clearly using the exeinfo PE tool to see the Byte Analyzer for the executable file, in this tool it can also be seen that this executable file is encrypted and has a function hash to detect errors and any changes between the data source and target data, namely crc32, but this file still has a Zero value test of 9.5691% so that it shows that it is not like LockBit 3.0 in general which is a strong package that requires a passcode to run the executable file [15].

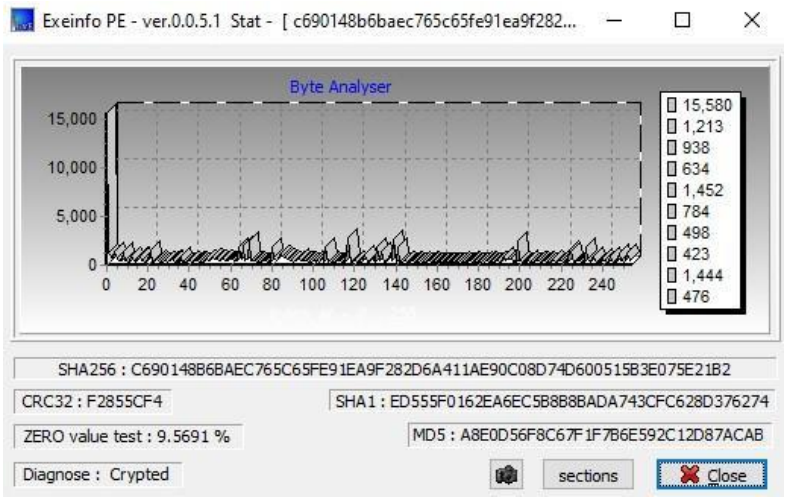

Figure 10 Byte Analyser

By using exeinfo PE, it can also be seen that the encoded data is done using base 64, but because the creators of the ransomware have prepared anti-analysis techniques so that a lot of information cannot be obtained that is clear and clear, unlike other LockBit ransomware which are its predecessors, such as seen in the libraries below all the information found is very limited [16].

3.2 Libraries and Function

To get Libraries from LockBit Black ransomware, you need PE Studio tools, but because the file ransomware uses anti-analysis techniques, only 3 libraries can be found, namely:

Table 2 Libraries of Encryption

Libraries	Description
Gdi32.dll	Graphics Device Interface
User32.dll	Windows USER component
kernel32.dll	Windows NT BASE API Client DLL

From these libraries it can only be seen that the executable file bypasses the user, in this case it is definitely the administrator user, and it only looks at handling errors and trying to close the display of the executable file, little information can be obtained because the executable file uses an anti-corruption technique. -analysis to prevent reverse engineering [17].

3.3 Interaction Mechanism

To see the mechanism of interaction in the operating system, the executable file needs to be run or this is a technique called dynamic analysis, simultaneously when the executable file is executed then with process hackers and wireshark like on Figure 11 we see some suspicious things [18].

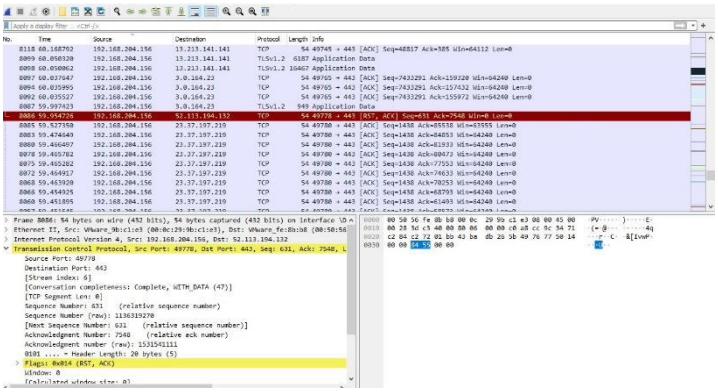

Figure 11 Suspicious IP reset on wireshark

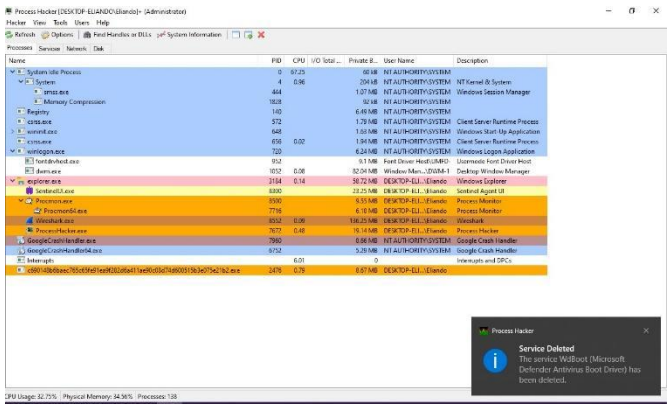

Figure 12 Malicious Activity on Process Hacker

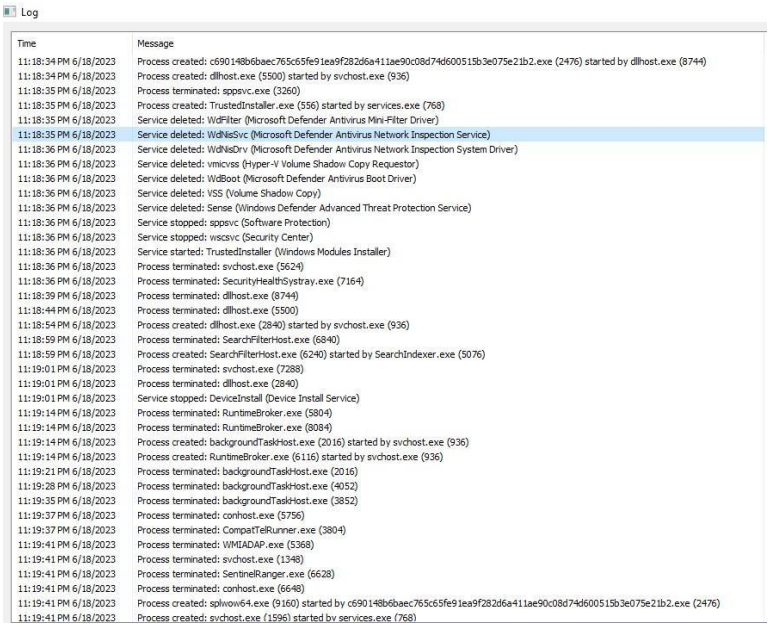

Figure 13 Log Process Hacker

From what is seen in the three pictures above, namely the Figure 12 and Figure 13, it can be seen that the LockBit Black ransomware communicates with several IPs that have been Blacklisted, along with turning off several services owned by the operating system as seen in the hacker process log, one of which turned off is windows defender as protection and all software protection and windows updates, along with LockBit Black deletes either system restore on the windows operating system by deleting the volume shadow copy service and removing the event log in the operating system to remove traces of the ransomware [19].

3.4 The combination

Looking at the ability to infect and bypass all protections that are in operation of attack computer, it is very possible for the shell that modification of the reverse shell in metasploit [20] to be combined with LockBit 3.0 aka LockBit Black with an example as shown in the Figure 14

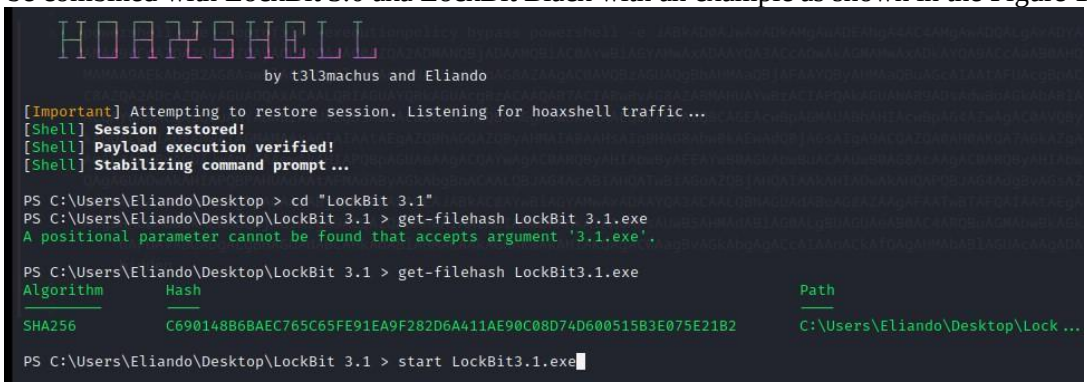

Figure 14 Reverse Shell On LockBit Black

The ability of LockBit 3 aka LockBit Black in infecting and disabling every protection in the operating system and eliminating traces in the operating system as well as performing anti-analysis techniques so that it makes it difficult to carry out both static and dynamic analysis, with the ability to reverse shell or connect back shell to ensure attacker communication is not detected allowing LockBit 3 aka LockBit Black to be quite a powerful weapon and when the antivirus realizes by looking at the binary in the encrypted file and then reverse shell will help LockBit Black hide itself while waiting for commands from the attacker to communicate again.

4. CONCLUSION

The conclusion from the results of this study is that LockBit 3.0 aka LockBit Black will continue to experience development in view of its capabilities which until now have contributed to science, especially the coding abilities of program makers and make every malware analysis expert must continue to look for ways to counter the ability of anti-malware techniques. -the analysis, until now the anti-analysis technique of LockBit 3 aka LockBit Black is not something that is easy to solve, reverse engineering which is easy at first becomes difficult when dealing with ransomware like this, coupled with the ability of a reverse shell that every protection from anti it is impossible for a virus to distinguish which is a false positive or a true positive from the connect-back shell, so machine learning and artificial intelligence are expected to help humans find solutions quickly.

5. FUTURE STUDIES

Evaluation of the results of this study is that it is necessary to develop machine learning methods with artificial intelligence to deal with various types of ransomware attacks, because it is felt that the knowledge of the weaknesses of a system and analysis techniques is faster, so if the detection and prevention measures fail and the ransomware succeeds in entering the operating system, recovery will be impossible to do.

REFERENCES

[1] F. Almeida, M. Imran, J. Raik, and S. Pagliarini, "Ransomware Attack as Hardware Trojan: A Feasibility and Demonstration Study," *IEEE Access*, vol. 10, 2022, doi: 10.1109/ACCESS.2022.3168991.

[2] M. Locatelli, "How financial services firms can mitigate the next wave of attacks," *Netw. Secur.*, vol. 2021, no. 10, 2021, doi: 10.1016/S1353-4858(21)00117-3.

[3] H. Athir, M. Puat, A. A. Rahman, K. Jalil, and M. Lumpur, "RANSOMWARE AS A SERVICE AND PUBLIC AWARENESS," *PalArch's J. Archaeol. Egypt / Egyptol.*, vol. 17, no. 7, 2020.

[4] M. McMurrough, A. Fein, and C. Skeath, "CISA Issues Joint Cybersecurity Advisory on Ransomware Trends and Recommendations," *Bank. Law J.*, vol. 139, no. 5, 2022.

[5] "A novel approach to generate a reverse shell: Exploitation and Prevention," *Int. J. Intell. Commun. Comput. Networks*, vol. 2, no. 2, 2021, doi: 10.51735/ijiccn/001/33.

[6] M. Humayun, N. Z. Jhanjhi, A. Alsayat, and V. Ponnusamy, "Internet of things and ransomware: Evolution, mitigation and prevention," *Egyptian Informatics Journal*, vol. 22, no. 1. 2021, doi: 10.1016/j.eij.2020.05.003.

[7] D. Arnold, C. David, and J. Saniie, "PowerShell Malware Analysis Using a Novel Malware Rating System," in *IEEE International Conference on Electro Information Technology*, 2022, vol. 2022-May, doi: 10.1109/eIT53891.2022.9813771.

[8] A. Johnson and R. J. Haddad, "Evading signature-based antivirus software using custom reverse shell exploit," in *Conference Proceedings - IEEE SOUTHEASTCON*, 2021, vol. 2021-March, doi: 10.1109/SoutheastCon45413.2021.9401881.

[9] D. Hendler, S. Kels, and A. Rubin, "AMSI-Based Detection of Malicious PowerShell Code Using Contextual Embeddings," 2020, doi: 10.1145/3320269.3384742.

[10] D. Vidyarthi, S. P. Choudhary, S. Rakshit, and C. R. S. Kumar, "Malware detection by static checking and dynamic analysis of executables," *Int. J. Inf. Secur. Priv.*, vol. 11, no. 3, 2017, doi: 10.4018/IJISP.2017070103.

[11] U. Urooj, B. A. S. Al-Rimy, A. Zainal, F. A. Ghaleb, and M. A. Rassam, "Ransomware Detection Using the Dynamic Analysis and Machine Learning: A Survey and Research Directions," *Appl. Sci.*, vol. 12, no. 1, 2022, doi: 10.3390/app12010172.

[12] A. Damodaran, F. Di Troia, C. A. Visaggio, T. H. Austin, and M. Stamp, "A comparison of static, dynamic, and hybrid analysis for malware detection," *J. Comput. Virol. Hacking Tech.*, vol. 13, no. 1, 2017, doi: 10.1007/s11416-015-0261-z.

[13] A. Kapoor, A. Gupta, R. Gupta, S. Tanwar, G. Sharma, and I. E. Davidson, "Ransomware detection, avoidance, and mitigation scheme: A review and future directions," *Sustainability (Switzerland)*, vol. 14, no. 1. 2022, doi: 10.3390/su14010008.

[14] C. Eagle, *The IDA Pro Book*, vol. 91, no. 5. 2012.

[15] D. Zhang, Z. Zhang, B. Jiang, and T. H. Tse, "The Impact of Lightweight Disassembler on Malware Detection: An Empirical Study," in *Proceedings - International Computer Software and Applications Conference*, 2018, vol. 1, doi: 10.1109/COMPSAC.2018.00094.

[16] T. McIntosh, A. S. M. Kayes, Y. P. P. Chen, A. Ng, and P. Watters, "Ransomware Mitigation in the Modern Era: A Comprehensive Review, Research Challenges, and Future Directions," *ACM Computing Surveys*, vol. 54, no. 9. 2022, doi: 10.1145/3479393.

[17] K. Acici and G. Ugurlu, "A Reverse Engineering Tool that Directly Injects Shellcodes to the Code Caves in Portable Executable Files," 2022, doi: 10.1109/ICTACSE50438.2022.10009732.

[18] R. Umar, I. Riadi, and R. S. Kusuma, "Analysis of Conti Ransomware Attack on Computer Network with Live Forensic Method," *IJID (International J. Informatics Dev.*, vol. 10, no. 1, 2021, doi: 10.14421/ijid.2021.2423.

[19] I. Kara and M. Aydos, "The rise of ransomware: Forensic analysis for windows based ransomware attacks," *Expert Syst. Appl.*, vol. 190, 2022, doi: 10.1016/j.eswa.2021.116198.

[20] Willcox Grant, "How to use a reverse shell in Metasploit · rapid7/metasploit-framework Wiki," *GitHub*, 2020.