LockBit 2.0 Ransomware: Analysis of infection, persistence, prevention mechanism

Eliando*[1], Yunianto Purnomo[2]
[1,2]Universitas Matana; ARA Center,
Jl. CBD Barat Kav. 1. Gading Serpong, Tangerang - 15810, Indonesia,
Telp 021-29232999
[3]Program Studi Sistem Informasi, FSTEM, Universitas Matana
e-mail: ***[1]eliando@matanauniversity.ac.id**, [2]yunianto@matanauniversity.ac.id

Abstract

This research was carried out due to the prevalence of ransomware attacks, especially in Indonesia against data located at Endpoints, in early 2022 ransomware was enough to horrify the news in cyberspace and one of the ransomware that is quite worrying in Indonesia is LockBit 2.0 ransomware, so research is needed against the ransomware. The method used to research the ransomware is static analysis and dynamic analysis which will show the infection and persistence of the LockBit 2.0 ransomware, the static analysis method is used by reverse engineering the portable executable (PE) file and the dynamic analysis method is carried out by running the ransomware. then look at the operating activities, the resources used, and including the network activities carried out by the ransomware and its impact on the affected operating system, so that a scenario for prevention methods can be made, where in this study we can see the real impact of the attacks carried out by the LockBit 2.0 ransomware which is also part of ransomware-as-a-services (Raas), as well as 5 steps that can be taken to avoid it and can make anyone aware with ransomware attacks that's why create artificial intelligence that accommodates such vigilance is important.

Keywords—Ransomware, LockBit 2.0, Infection, Persistence, Prevention

1. INTRODUCTION

In the current era of digitalization, computer security is very important, because every data has important information in it. When talking about computer security compared to seven years ago, attack techniques and threat techniques to computer security have changed a lot like never seen before, in the modern world of cybersecurity attacks, attack patterns have changed from the former attacking directly to the intended target, for example server of a company or organization, in the modern world of cybersecurity attack, innocent users can be the target of the attack by using malicious software (Malware) as a tool for the next purpose [1]. Malware is often used to facilitate cybercrimes with various purposes such as causing the device to be locked or unused, stealing, erasing or encrypting data, taking control of your device to attack other organizations or companies, obtaining credentials that allow access to the organization's or company's systems or services. that you use and use these services to spend your money, but among all these purposes there is malware that is often used to encrypt your data and ask for a ransom to decrypt the data or commonly known as Ransomware [2]. Ransomware often also has the ability to spread very quickly and perform discovery of the surrounding network and enter computers on the network and immediately encrypt the computer, and not only that Ransomware is often used as a tool to hide malware that acts as a backdoors, or Trojans, so that users are only diverted to data that has been encrypted without caring about anything including other activities carried out by the Ransomware [3].

Based on the 2021 Cyber Security Monitoring Annual Report published by the National

Cyber and Crypto Agency (BSSN) in March 2022, as seen in figure 1 below, that Ransomware is a type of attack that is reported quite a lot in Indonesia, this shows that very many computers or endpoints that were affected by the ransomware attack, BSSN also reports that of the 206,185 ransomware submissions that have been recorded by Emsisoft, the agency that publishes reports and statistics [4] regarding ransomware, it states that as many as 13.80% of submissions are submissions originating from Indonesia. , the large number of submissions puts Indonesia in the category of the top 10 countries reporting ransomware incidents. In particular, the Directorate of Cybersecurity Operations BSSN through its search on the dark web site managed to find that from January 1, 2021 to December 31, 2021, there had been 15 incidents of ransomware attacks accompanied by extortion by threat actors in a number of agencies from various sectors such as Government, Finance, Technology, Education, Agriculture, Food Industry, to insurance in Indonesia.

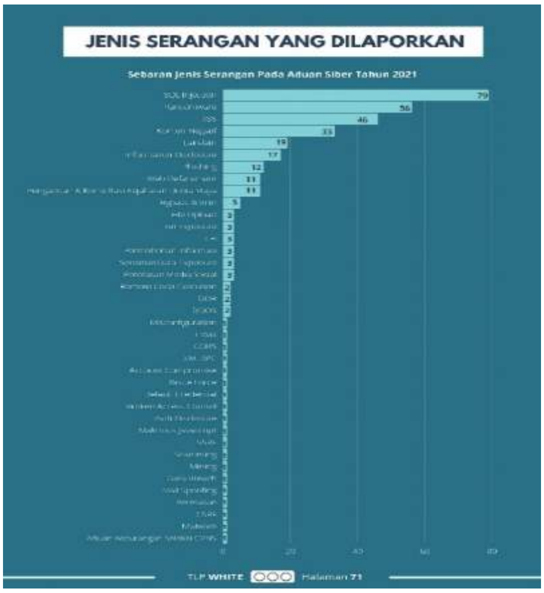


Figure 1 BSSN Report Page 71

One of the ransomware attacks that is quite worrying as seen in the image below which shows the BSSN report on ransomware trends, that from existing reports regarding ransomware attacks, Conti and Avaddon occupy the top positions of ransomware attacks that occurred in Indonesia, but which is no less worrying which occupies the second position of the ransomware attack in Indonesia, namely LockBit ransomware, based on the cases handled by the Directorate of Cybersecurity Operations BSSN [5], Lockbit 2.0 publishes victim data through the Lockbit 2.0 dark website which can be accessed via The Onion Router (TOR). Lockbit 2.0 exploits vulnerabilities found in Fortinet devices, namely FortiOS and FortiProxy contained in CVE-2018-13379. Lockbit 2.0 will scan the network to get domain control from the victim so that it can be used for lateral movement. Lockbit 2.0 was detected using mimikatz which is stored in the C:\\TEMP\mimikatz.exe folder. Mimikatz used Lockbit 2.0 to perform credential dumping. Lockbit 2.0 also performs defense evasion by disabling antivirus and windows defender using “bat_av.bat” and “bat.bat”” files which are executed using PsExec.exe [6] .

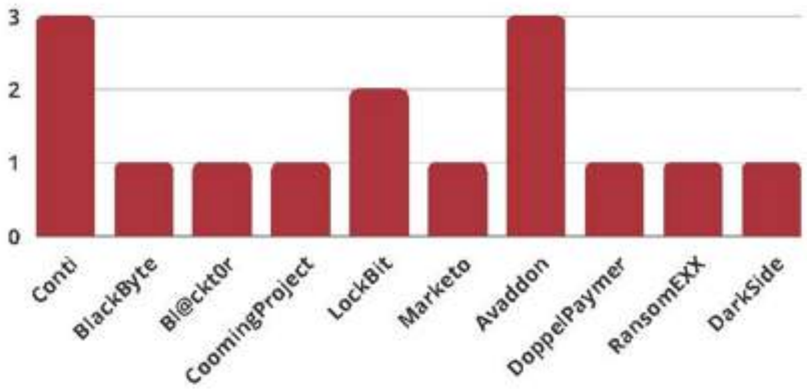
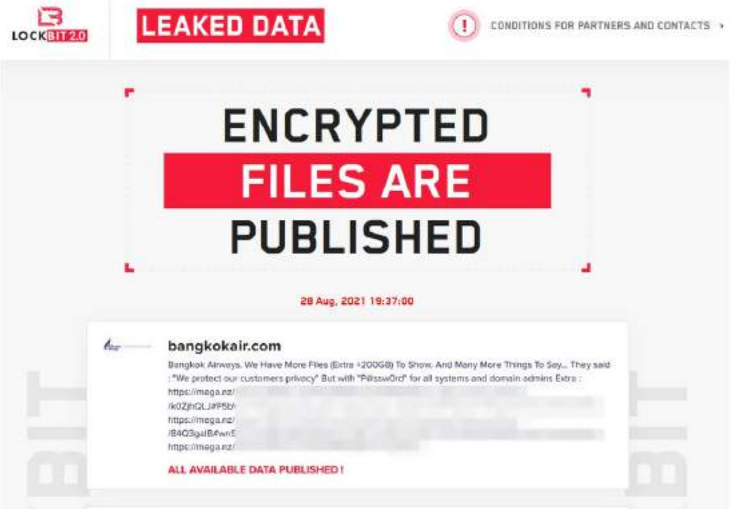


Figure 2 BSSN Report Page 150 Ransomware Trend

LockBit 2.0 Ransomware leaked more than 200GB of data from one of the largest companies in Thailand, namely Bangkok Airways, as reported by the BleepingComputer website, not only that, even a company as big as Accenture which is the largest IT consultancy company, was affected by the LockBit 2.0 attack and the hacker group. demanded a ransom of $50 million to stop the leak of data that had reached 6TB.



LOCKBIT 2.0

LEAKED DATA

CONDITIONS FOR PARTNERS AND CONTACTS ›

ENCRYPTED FILES ARE PUBLISHED

28 Aug, 2021 19:37:00

bangkokair.com

Bangkok Airways. We Have More Files (Extra +200GB) To Show. And Many More Things To Say... They said : "We protect our customers privacy" But with "P@ssw0rd" for all systems and domain admins Extra :
https://mega.nz/ [redacted]
/k0ZjhQLJ#P5b [redacted]
https://mega.nz/ [redacted]
/B4Q3gaIB#wn5 [redacted]
https://mega.nz/ [redacted]

ALL AVAILABLE DATA PUBLISHED !

Figure 3 Source BleepingComputer

Of the many attacks that have been successfully carried out by the LockBit 2.0 ransomware, and no more in-depth research has been carried out on the LockBit 2.0 ransomware, in this paper an in-depth analysis of LockBit 2.0 is carried out to at least prevent or even stop immediately before the LockBit 2.0 ransomware spreads.

2. RESEARCH METHOD

In this section, the methods used to analyze Malicious Software (Malware) can also be used to analyze LockBit 2.0 ransomware. The sample used in this study was obtained from MalwareBazaar with detailed hash information as follows:

Table 1 LockBit 2.0 Components

	Mutation LockBit 2.0 Components
MD5	8B58D80D6650CEA98B5DC6374A47E16E

SHA1	C1EEA96AF2E60D2328DCADE8BEEC7C8ACD47AB39
SHA256	66C817095A95ADE8B25DC3C53C1F4DA5714B3D3F5A72922E73B476D8F17B1703
File Type	Portable Executable for 80386
Size	959KB
	Encryption Components
MD5	84866FCA8A5CEB187BCA8E257E4F875A
SHA1	038BC02C0997770A1E764D0203303EF8FCAD11FB
SHA256	ACAD2D9B291B5A9662AA1469F96995DC547A45E391AF9C7FA24F5921B0128B2C
File Type	Portable Executable for 80386
Size	959KB

As shown in the image below, the method used in this study to obtain the results of infection analysis, persistence and mechanisms for preventing LockBit 2.0 ransomware can be divided into 2 methods, namely Static Analysis and Dynamic Analysis.

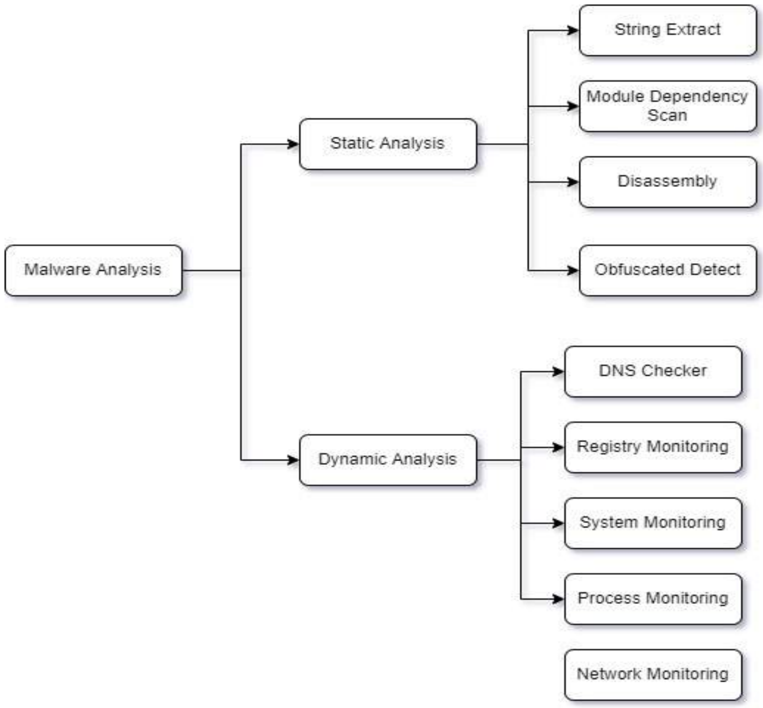


Figure 4 Malware Analysis

2.1 Static Analysis

The first method used is Static Analysis, this technique is used as the initial process for determining the file suspected of being malware so that an analysis determination is obtained that the suspected file is a file that has malicious code and can be categorized as malware. At this stage, several things are carried out, such as the following [7] :

1. In static analysis, the file to be analyzed will be disassembled, the file will be unpacked and seen in comparison, whether the file is classified as a benign file or malware.
2. Hexadecimal analysis is used to determine the type of file to be analyzed. The executable file has a hexadecimal code or 4D 5A signature or can be categorized as a Windows or

DOS executable that has a Part Executable (PE) file. To analyze the file, tools are needed to assist the analysis, such as IDAPro Free and PEid [8].

3. Analysis with the static in method aims to obtain the identity of a file, where CRC32 is an identifier of a file that has experienced data transmission from the origin of the file to the destination of the file, and this is one of the hash functions developed to detect data corruption in the process transmission or storage [9].

2.2 Dynamic Analysis

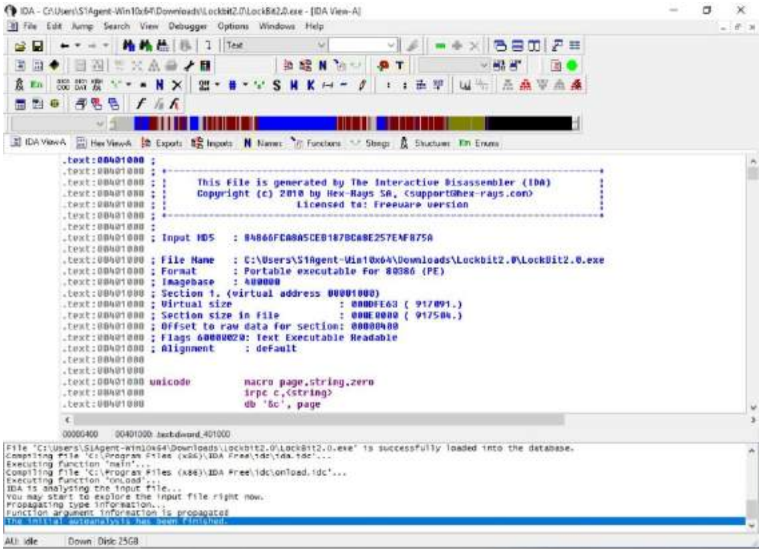
The second method used is dynamic analysis, this technique is carried out by analyzing the infected virtual system network, and monitoring the network, operating system, and process activities carried out by malware that has infected a system, in the hope of seeing the deployment method carried out. by the malware or ransomware and the activities it creates. To analyze this, tools are needed to help, such as Process Hacker, Process Monitor, Wireshark and others [10].

3. RESULTS AND DISCUSSION

To get the results of this study, several tools were used in conducting the analysis, each tool has characteristics in the test so that minimal results are obtained and can be correlated with one another to get more detailed information on the LockBit 2.0 ransomware attack.

3.1 PE LockBit 2.0 Ransomware

This research begins by first conducting a static analysis of the sample file by disassembling it using IDA Pro tools with information as shown in the image below.


IDA - C:\Users\S1Agent-Win10x64\Downloads\Lockbit2.0\LockBit2.0.exe - [IDA View-A]
File Edit Jump Search View Debugger Options Windows Help
IDA View-A Hex View-A Exports Imports Names Functions Strings Structures Enums

```
.text:00401000 ;
.text:00401000 ; +-------------------------------------------------------------+
.text:00401000 ; |      This file is generated by The Interactive Disassembler (IDA)      |
.text:00401000 ; |      Copyright (c) 2010 by Hex-Rays SA, <support@hex-rays.com>       |
.text:00401000 ; |                    Licensed to: Freeware version                     |
.text:00401000 ; +-------------------------------------------------------------+
.text:00401000 ;
.text:00401000 ; Input MD5   : 84866FCA8A5CEB187BCA8E257EAF875A
.text:00401000
.text:00401000 ; File Name   : C:\Users\S1Agent-Win10x64\Downloads\Lockbit2.0\LockBit2.0.exe
.text:00401000 ; Format      : Portable executable for 80386 (PE)
.text:00401000 ; Imagebase   : 400000
.text:00401000 ; Section 1. (virtual address 00001000)
.text:00401000 ; Virtual size                  : 000DFE63 ( 917091.)
.text:00401000 ; Section size in file          : 000E0000 ( 917504.)
.text:00401000 ; Offset to raw data for section: 00000400
.text:00401000 ; Flags 60000020: Text Executable Readable
.text:00401000 ; Alignment     : default
.text:00401000
.text:00401000
.text:00401000 unicode         macro page,string,zero
.text:00401000                 irpc c,<string>
.text:00401000                 db '&c', page
```

00000400 00401000: .text:dword_401000

```
File 'C:\Users\S1Agent-Win10x64\Downloads\Lockbit2.0\LockBit2.0.exe' is successfully loaded into the database.
Compiling file 'C:\Program Files (x86)\IDA Free\idc\ida.idc'...
Executing function 'main'...
Compiling file 'C:\Program Files (x86)\IDA Free\idc\onload.idc'...
Executing function 'OnLoad'...
IDA is analysing the input file...
You may start to explore the input file right now.
Propagating type information...
Function argument information is propagated
The initial autoanalysis has been finished.
```

AU: idle Down Disk: 25GB

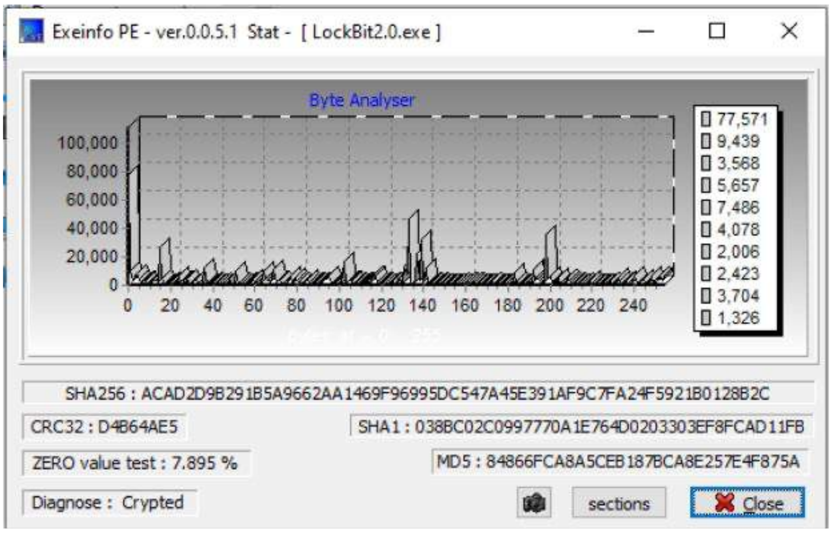
Figure 5 IDA Pro

By using IDA Pro, we can read each source code from reverse engineering one by one, for example as seen from the OpCode below that one of the .dll files, namely ole32.dll, was imported and the dword value changed and configured the server and proxy performed by the file which indicates that there was an attempt to bypass the protection against communications from the Command and Control Server [11].

```
; Imports from ole32.dll
;
```

```
; HRESULT __stdcall CoCreateInstance(const CLSID *const
rclsid,LPUNKNOWN pUnkOuter,DWORD dwClsContext,const IID *const
riid,LPVOID *ppv)
extrn CoCreateInstance:dword
; HRESULT __stdcall CoSetProxyBlanket(IUnknown *pProxy,DWORD
dwAuthnSvc,DWORD dwAuthzSvc,OLECHAR *pServerPrincName,DWORD
dwAuthnLevel,DWORD dwImpLevel,RPC_AUTH_IDENTITY_HANDLE pAuthInfo,DWORD
dwCapabilities)
extrn CoSetProxyBlanket:dword
```

It can be seen in the picture that the input hash is MD5 and the file format used in this research sample, it is also seen that this portable executable format file has several sections in raw and virtual form with flags which are readable text executables to run commands on the system. operation, using the Byte Analyzer from Exeinfo PE as in figure 6, it can be seen that from the diagnosis that the file is Crypted with a zero value test of 7.895% which shows that the file is a pure file in the form of LockBit 2.0 ransomware.



SHA256 : ACAD2D9B291B5A9662AA1469F96995DC547A45E391AF9C7FA24F5921B0128B2C

CRC32 : D4B64AE5

SHA1 : 038BC02C0997770A1E764D0203303EF8FCAD11FB

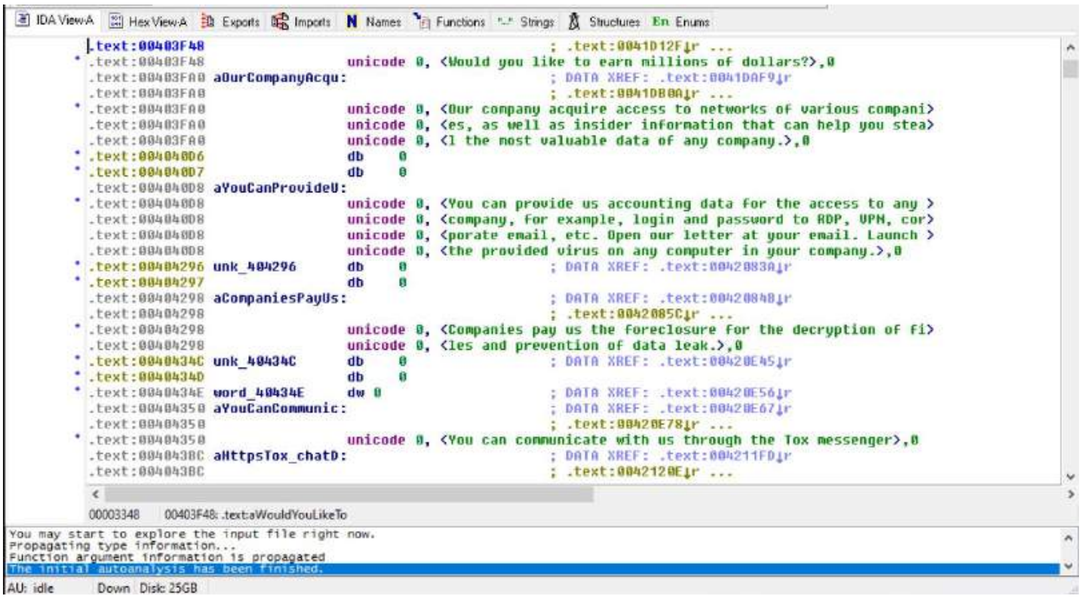
ZERO value test : 7.895 %

MD5 : 84866FCA8A5CEB187BCA8E257E4F875A

Diagnose : Crypted

Figure 6 Byte Analyser

In using Exeinfo PE we can see how the portable executable file acts so that the process of finding a way to go back to back by doing recovery is very possible to do [12]. However, the file also includes several notes, which means that the creators of the LockBit 2.0 ransomware know that the files they create will be reverse engineered as an analysis to find out how it works, and the unique message that is inserted is an invitation to cooperate by providing data in the form of access to companies such as logins and passwords for RDP, VPN, corporate email and others and running LockBit 2.0 into the company, and they mention also communicating with them can be done via Tox messenger, the messages are embedded in the bundle executable file, so only people with reverse engineering capabilities that can see the hidden message as shown in the image below,



```
.text:00403F48                                  ; .text:0041D12F↓r ...
.text:00403F48                 unicode 0, <Would you like to earn millions of dollars?>,0
.text:00403FA0 aOurCompanyAcqu:                 ; DATA XREF: .text:0041DAF9↓r
.text:00403FA0                                  ; .text:0041DB0A↓r ...
.text:00403FA0                 unicode 0, <Our company acquire access to networks of various compani>
.text:00403FA0                 unicode 0, <es, as well as insider information that can help you stea>
.text:00403FA0                 unicode 0, <l the most valuable data of any company.>,0
.text:004040D6                 db    0
.text:004040D7                 db    0
.text:004040D8 aYouCanProvideU:
.text:004040D8                 unicode 0, <You can provide us accounting data for the access to any >
.text:004040D8                 unicode 0, <company, for example, login and password to RDP, VPN, cor>
.text:004040D8                 unicode 0, <porate email, etc. Open our letter at your email. Launch >
.text:004040D8                 unicode 0, <the provided virus on any computer in your company.>,0
.text:00404296 unk_404296      db    0          ; DATA XREF: .text:0042083A↓r
.text:00404297                 db    0
.text:00404298 aCompaniesPayUs:                 ; DATA XREF: .text:0042084B↓r
.text:00404298                                  ; .text:0042085C↓r ...
.text:00404298                 unicode 0, <Companies pay us the foreclosure for the decryption of fi>
.text:00404298                 unicode 0, <les and prevention of data leak.>,0
.text:0040434C unk_40434C      db    0          ; DATA XREF: .text:00420E45↓r
.text:0040434D                 db    0
.text:0040434E word_40434E     dw 0             ; DATA XREF: .text:00420E56↓r
.text:00404350 aYouCanCommunic:                 ; DATA XREF: .text:00420E67↓r
.text:00404350                                  ; .text:00420E78↓r ...
.text:00404350                 unicode 0, <You can communicate with us through the Tox messenger>,0
.text:0040438C aHttpsTox_chatD:                 ; DATA XREF: .text:004211FD↓r
.text:0040438C                                  ; .text:0042120E↓r ...
```

00003348   00403F48: .text:aWouldYouLikeTo

```
You may start to explore the input file right now.
Propagating type information...
Function argument information is propagated
The initial autoanalysis has been finished.
```

AU: idle   Down   Disk: 25GB

Figure 6 Hiding Message

This shows that the LockBit 2.0 Ransomware is a Ransomware-as-a-services (Raas) which is a service that allows anyone who does not have expertise in making ransomware even to carry out attacks and target anyone with Ransomware [13]. Raas providers facilitate anyone to become cyber criminals from the packages or services already provided in the Raas, from this it can be seen that LockBit 2.0 ransomware is not an easy type of ransomware to analyze.

3.2 Libraries and Function

To get the libraries and functions of the LockBit 2.0 ransomware, a tool called PEstudio is used as shown in the table Libraries of Encryption and table Function of Encryption below

Table 2 Libraries of Encryption

Libraries	Description
shlwapi.dll	Shell Light-weight Utility Library
activeds.dll	Active Directory Router Layer
kernel32.dll	Windows NT BASE API Client DLL
advapi32.dll	Advanced Windows 32 Base API
ole32.dll	Microsoft OLE for Windows

Table 3 Function of Encrytion

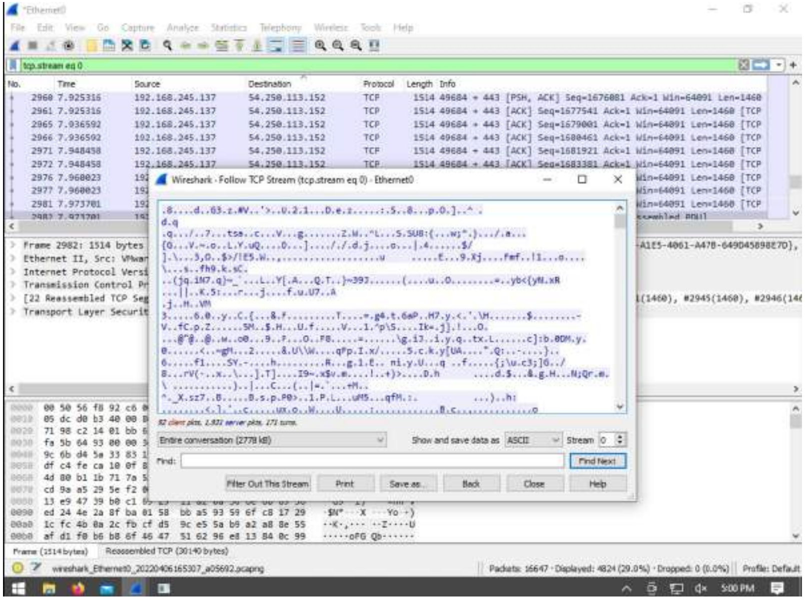
Libraries	Function
activeds.dll	9 (ADsOpenObject)
activeds.dll	15 (FreeADsMem)
kernel32.dll	CreateProcessW
advapi32.dll	CheckTokenMembership
advapi32.dll	CreateWellKnownSid
shlwapi.dll	PathAppendW
kernel32.dll	GetSystemTime

kernel32.dll	lstrlenW
kernel32.dll	LocalFree
ole32.dll	CoCreateInstance
ole32.dll	CoSetProxyBlanket

From these libraries and functions, it can be seen how the LockBit 2.0 ransomware uses activeds.dll to deploy and several other libraries are used to perform persistence, whereas if viewed from the existing functions, for example advapi32.dll is used as a function to generate keys for encryption, run and control. services, obtaining Token Privileges, and other functions that aid the persistence and infection of the LockBit 2.0 ransomware.

3.3 Interaction and Persistense Mechanism

By using a combination of Static and Dynamic Analysis, as an example as shown in the image below using the Wireshark and Process Hacker tools


*Ethernet0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Wireshark · Follow TCP Stream (tcp.stream eq 0) · Ethernet0
Filter Out This Stream
Print
Save as...
Back
Close
Help
Find Next

```
tcp.stream eq 0

No.     Time        Source            Destination      Protocol  Length Info
2960 7.925316  192.168.245.137  54.250.113.152  TCP  1514 49684 → 443 [PSH, ACK] Seq=1676081 Ack=1 Win=64091 Len=1460
2961 7.925316  192.168.245.137  54.250.113.152  TCP  1514 49684 → 443 [ACK] Seq=1677541 Ack=1 Win=64091 Len=1460 [TCP
2965 7.936592  192.168.245.137  54.250.113.152  TCP  1514 49684 → 443 [ACK] Seq=1679001 Ack=1 Win=64091 Len=1460 [TCP
2966 7.936592  192.168.245.137  54.250.113.152  TCP  1514 49684 → 443 [ACK] Seq=1680461 Ack=1 Win=64091 Len=1460 [TCP
2971 7.948458  192.168.245.137  54.250.113.152  TCP  1514 49684 → 443 [ACK] Seq=1681921 Ack=1 Win=64091 Len=1460 [TCP
2972 7.948458  192.168.245.137  54.250.113.152  TCP  1514 49684 → 443 [ACK] Seq=1683381 Ack=1 Win=64091 Len=1460 [TCP
2976 7.960023  192                                                            Win=64091 Len=1460 [TCP
2977 7.960023  192                                                            Win=64091 Len=1460 [TCP
2981 7.973701  192                                                            Win=64091 Len=1460 [TCP

> Frame 2982: 1514 bytes                                              -A1E5-4061-A478-649D45898E7D},
> Ethernet II, Src: VMwar
> Internet Protocol Versi
> Transmission Control Pr
> [22 Reassembled TCP Seg                                             1(1460), #2945(1460), #2946(146
> Transport Layer Securit

0090  ed 24 4e 2a 8f ba 01 58  bb a5 93 59 6f c8 17 29   ·$N*···X ···Yo··)
00a0  1c fc 4b 0a 2c fb cf d5  9c e5 5a b9 a2 a8 8e 55   ··K·,··· ··Z····U
00b0  af d1 f0 b6 b8 6f 46 47  51 62 96 e8 13 84 0c 99   ·····oFG Qb······

Frame (1514 bytes)   Reassembled TCP (30140 bytes)
wireshark_Ethernet0_20220406165307_a05692.pcapng    Packets: 16647 · Displayed: 4824 (29.0%) · Dropped: 0 (0.0%)   Profile: Default
```

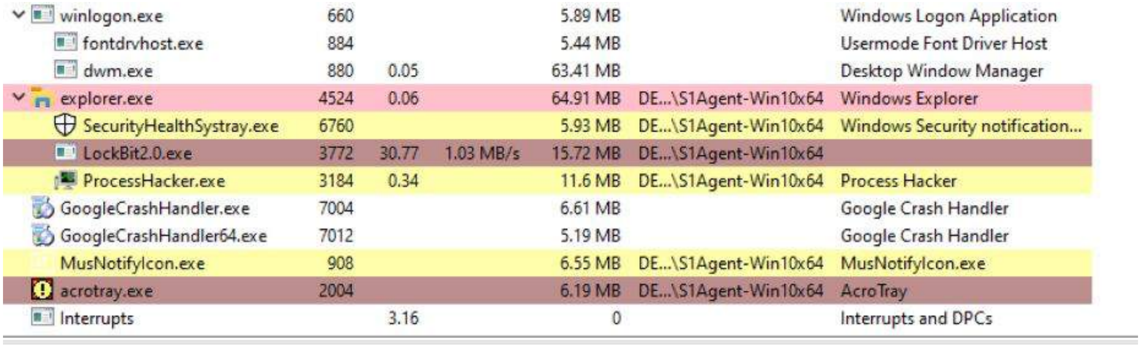
92 client pkts, 1,931 server pkts, 171 turns.

Entire conversation (2778 kB)   Show and save data as: ASCII   Stream: 0

Find:

Figure 7 Wireshark TCP Stream

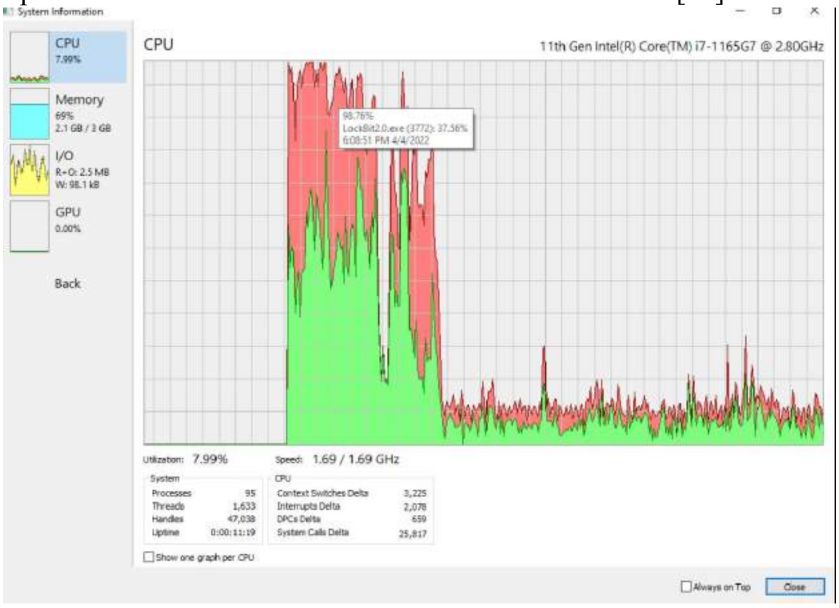
By looking at the TCP Stream from Wireshark as a tool for dynamic analysis, we can see activities or communications hidden in passing packets so that we can analyze IP addresses and incoming files and communicate both from inbound and outbound. [14]



winlogon.exe	660			5.89 MB		Windows Logon Application
fontdrvhost.exe	884			5.44 MB		Usermode Font Driver Host
dwm.exe	880	0.05		63.41 MB		Desktop Window Manager
explorer.exe	4524	0.06		64.91 MB	DE...\S1Agent-Win10x64	Windows Explorer
SecurityHealthSystray.exe	6760			5.93 MB	DE...\S1Agent-Win10x64	Windows Security notification...
LockBit2.0.exe	3772	30.77	1.03 MB/s	15.72 MB	DE...\S1Agent-Win10x64	
ProcessHacker.exe	3184	0.34		11.6 MB	DE...\S1Agent-Win10x64	Process Hacker
GoogleCrashHandler.exe	7004			6.61 MB		Google Crash Handler
GoogleCrashHandler64.exe	7012			5.19 MB		Google Crash Handler
MusNotifyIcon.exe	908			6.55 MB	DE...\S1Agent-Win10x64	MusNotifyIcon.exe
acrotray.exe	2004			6.19 MB	DE...\S1Agent-Win10x64	AcroTray
Interrupts		3.16		0		Interrupts and DPCs

Figure 8 Process Hacker

By looking at the process activities running using the Process Hacker tool in the Windows operating system, we can see various hidden process activities and with the operating system idle, anomaly activity can be found and we can see the process tree so that it can be known dynamically each analysis. processes related to the LockBit 2.0 ransomware attack [15]



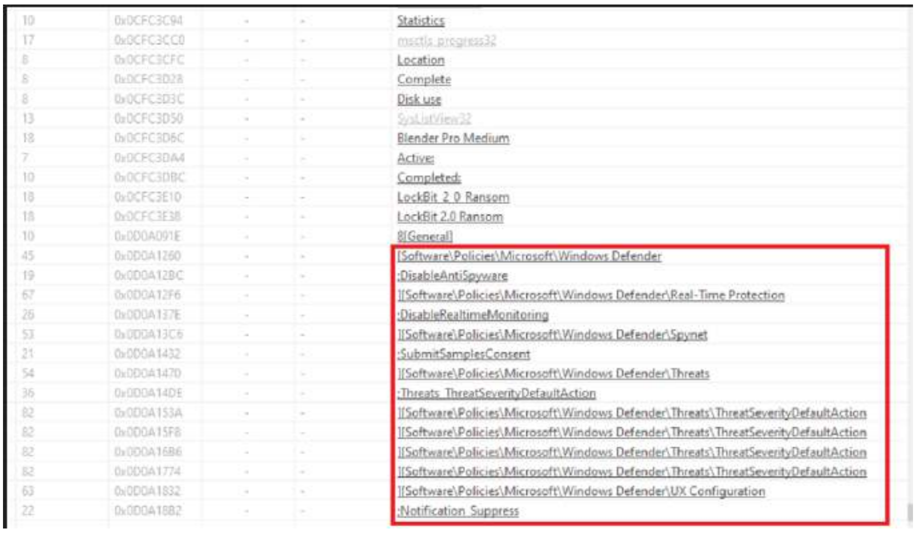
Utilization: 7.99%
Speed: 1.69 / 1.69 GHz

System		CPU	
Processes	95	Context Switches Delta	3,225
Threads	1,633	Interrupts Delta	2,078
Handles	47,038	DPCs Delta	659
Uptime	0:00:11:19	System Calls Delta	25,817

□ Show one graph per CPU

Figure 9 System Information

It can be seen in Figures 7, 8 and 9 that the LockBit 2.0 ransomware activity once running can be seen quite a change, especially the CPU movement, as well as the network activity carried out by the ransomware, seeing the significant activity on the network, it can be seen that the antivirus embedded in the operating system has difficulty To protect, this is because the LockBit 2.0 ransomware tries to disable Windows Defender or other currently active antiviruses as shown in Figure 10 below. Windows Defender is protection software provided by Microsoft as a provider of the Windows Operating System, the software functions as an anti-malicious software where the smart screen which is a feature of Windows Defender provides real time protection, but if it is successfully disabled, the operating system in case of this windows will have no protection [16].

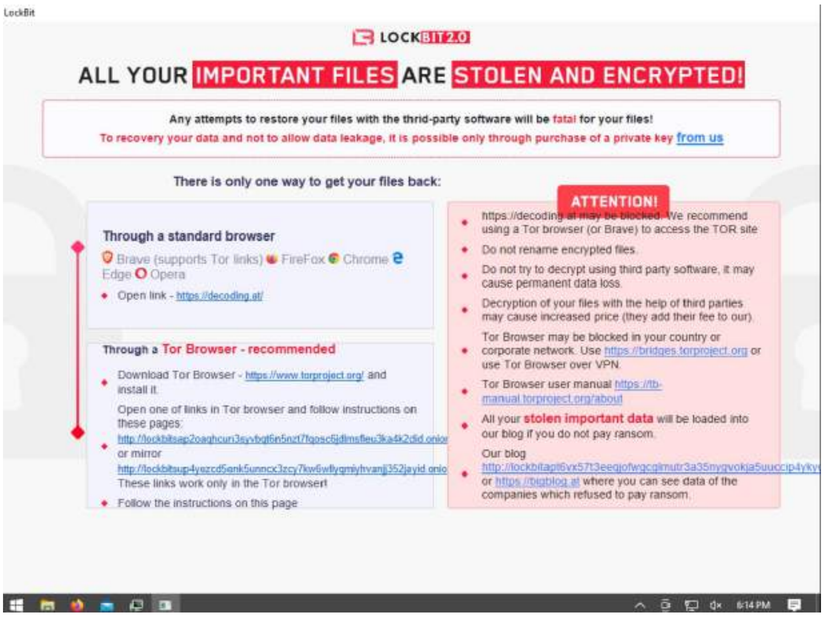


10	0x0CFC3C94	-	-	Statistics
17	0x0CFC3CC0	-	-	msctls_progress32
8	0x0CFC3CFC	-	-	Location
8	0x0CFC3D28	-	-	Complete
8	0x0CFC3D3C	-	-	Disk use
13	0x0CFC3D50	-	-	SysListView32
18	0x0CFC3D6C	-	-	Blender Pro Medium
7	0x0CFC3DA4	-	-	Active:
10	0x0CFC3DBC	-	-	Completed:
18	0x0CFC3E10	-	-	LockBit_2_0_Ransom
18	0x0CFC3E38	-	-	LockBit 2.0 Ransom
10	0x0D0A091E	-	-	8[General]
45	0x0D0A1260	-	-	[Software\Policies\Microsoft\Windows Defender
19	0x0D0A12BC	-	-	:DisableAntiSpyware
67	0x0D0A12F6	-	-	][Software\Policies\Microsoft\Windows Defender\Real-Time Protection
26	0x0D0A137E	-	-	:DisableRealtimeMonitoring
53	0x0D0A13C6	-	-	][Software\Policies\Microsoft\Windows Defender\Spynet
21	0x0D0A1432	-	-	:SubmitSamplesConsent
54	0x0D0A1470	-	-	][Software\Policies\Microsoft\Windows Defender\Threats
36	0x0D0A14DE	-	-	:Threats_ThreatSeverityDefaultAction
82	0x0D0A153A	-	-	][Software\Policies\Microsoft\Windows Defender\Threats\ThreatSeverityDefaultAction
82	0x0D0A15F8	-	-	][Software\Policies\Microsoft\Windows Defender\Threats\ThreatSeverityDefaultAction
82	0x0D0A16B6	-	-	][Software\Policies\Microsoft\Windows Defender\Threats\ThreatSeverityDefaultAction
82	0x0D0A1774	-	-	][Software\Policies\Microsoft\Windows Defender\Threats\ThreatSeverityDefaultAction
63	0x0D0A1832	-	-	][Software\Policies\Microsoft\Windows Defender\UX Configuration
22	0x0D0A18B2	-	-	:Notification_Suppress

Figure 10 Disable Windows Defender

From every analysis carried out using both static analysis and dynamic analysis, it can be seen that the LockBit 2.0 ransomware is a very dangerous ransomware, plus if it has succeeded in infecting the operating system then the data contained in it will be difficult to recover, and create a decryptor from ransomware attacks. LockBit 2.0 requires a short amount of time due to its unique encryption type, so precautions are needed so that the operating system is not infected by the LockBit 2.0 ransomware attack. Based on the infection method and persistence method used by LockBit 2.0 ransomware, what can be done to prevent the operating system from being affected. It can be seen in the image below which is the Endpoint used to run the LockBit 2.0

Ransomware



LockBit

LOCKBIT 2.0

ALL YOUR IMPORTANT FILES ARE STOLEN AND ENCRYPTED!

Any attempts to restore your files with the thrid-party software will be fatal for your files!
To recovery your data and not to allow data leakage, it is possible only through purchase of a private key from us

There is only one way to get your files back:

Through a standard browser

Brave (supports Tor links) FireFox Chrome Edge Opera

- Open link - https://decoding.at/

Through a Tor Browser - recommended

- Download Tor Browser - https://www.torproject.org/ and install it
- Open one of links in Tor browser and follow instructions on these pages: http://lockbitsap2oaghcun3syvbqt6n5nzt7fqosc6jdlmsfleu3ka4k2did.onion or mirror http://lockbitsup4yezcd5enk5unncx3zcy7kw6wllyqmiyhvanjj352jayid.onio These links work only in the Tor browser!
- Follow the instructions on this page

ATTENTION!

- https://decoding.at may be blocked. We recommend using a Tor browser (or Brave) to access the TOR site
- Do not rename encrypted files.
- Do not try to decrypt using third party software, it may cause permanent data loss.
- Decryption of your files with the help of third parties may cause increased price (they add their fee to our).
- Tor Browser may be blocked in your country or corporate network. Use https://bridges.torproject.org or use Tor Browser over VPN.
- Tor Browser user manual https://tb-manual.torproject.org/about
- All your stolen important data will be loaded into our blog if you do not pay ransom.
- Our blog http://lockbitapt6vx57t3eeqjofwgcglmutr3a35nygvokja5uuccip4ykyd or https://bigblog.at where you can see data of the companies which refused to pay ransom.

Figure 11 Ransomware LockBit 2.0 on windows

4. CONCLUSION

From the results of the research conducted this time on the LockBit 2.0 ransonware by looking at the infection techniques and persistence techniques carried out by the LockBit 2.0 ransomware, the prevention mechanisms that can be carried out are as follows:

1. To protect dll files like those in table 2 and table 3 to enhanced security levels [17], what you have to do is always Monitor Registry for any changes when running keys that do not correlate with known software, patch cycles, etc. Also do Monitor initial folder for additions or changes. Tools like Sysinternals Autoruns can also be used to detect system changes that could be persistent attempts, including listing the Registry location and the run key startup folder. The execution of any suspicious program as a startup program may appear as a never-before-seen outlier process when compared to historical data.
2. To protect files from being encrypted by ransomware by using the command line as shown in figure 11, not only on Linux [18] but also on others operating system the actions that must be taken are monitor command line activity and catchable scripts through proper logging of process execution with command line arguments. This information can be useful in gaining additional insight into enemy actions through how they use native processes or special tools. Also monitor the loading of modules related to a particular language.

3. To avoid ransomware taking action to disable antivirus and windows defender as shown in figure 9, using the capability of The Security Account Manager (SAM) [19] the actions that must be taken are enable Windows Group Policy "Do Not Allow Anonymous Enumeration of SAM Accounts and Shares" security setting to limit users who can enumerate network shares.
4. To avoid a file being executed and calling the ransomware program or running commands to encrypt existing files, especially on Windows 10 which has the autorun feature, the thing to do is enable cloud-delivered protection and Attack Surface Reduction (ASR) that as part f hardening operating system [20] rules to block the execution of files that resemble ransomware if there is virtual machine using snapshot is one of best practise.
5. If the ransomware has already attacked and there is nothing more that can be done, then what must be done before a ransomware disaster occurs is consider implementing IT disaster recovery plans that contain procedures for regularly taking and testing data backups that can be used to restore organizational data [21]. Ensure backups are stored off system and is protected from common methods adversaries may use to gain access and destroy the backups to prevent recovery. Consider enabling versioning in cloud environments to maintain backup copies of storage objects.

5. FUTURE STUDIES

The evaluation of the results of this study is that a development method of machine learning with artificial intelligence is needed in the future to deal with this type of ransomware attack, because if detection and prevention measures fail and the ransomware successfully enters the operating system, recovery will be difficult to do.

REFERENCES

[1] M. J. Haber and B. Hibbert, “Ransomware,” in *Privileged Attack Vectors*, 2018.

[2] NCSC, “Mitigating malware and ransomware attacks,” *Natl. Cyber Secur. Cent.*, 2020.

[3] H. Alshaikh, N. Ramadan, and H. Ahmed, “Ransomware Prevention and Mitigation Techniques,” *Int. J. Comput. Appl.*, vol. 177, no. 40, 2020, doi: 10.5120/ijca2020919899.

[4] EMSISoft, *The State of Ransomware in the US: Report and Statistics 2019*. 2019.

[5] M. A. R. Dewi, I. A. Putra, and S. Sulistyo, “DESIGN INTEGRATED HONEYPOT UNTUK DETEKSI DAN IDENTIFIKASI SERANGAN SIBER,” *J. IT*, vol. 10, no. 3, 2020, doi: 10.37639/jti.v10i3.141.

[6] J. Mulder, “Mimikatz Overview, Defenses and Detection,” 2019.

[7] S. Gadhiya, K. Bhavsar, and P. D. Student, “Techniques for Malware Analysis,” *Int. J. Adv. Res. Comput. Sci. Softw. Eng.*, vol. 3, no. 4, 2013.

[8] N. M. Hai, M. Ogawa, and Q. T. Tho, “Packer identification based on metadata signature,” 2017, doi: 10.1145/3151137.3160687.

[9] S. YusirwanS, Y. Prayudi, and I. Riadi, “Implementation of Malware Analysis using Static

and Dynamic Analysis Method," *Int. J. Comput. Appl.*, vol. 117, no. 6, 2015, doi: 10.5120/20557-2943.

[10] L. Xu, D. Zhang, N. Jayasena, and J. Cavazos, "HADM: Hybrid Analysis for Detection of Malware," in *Lecture Notes in Networks and Systems*, vol. 16, 2018.

[11] 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.

[12] E. H. Hwang, S. J. Cho, K. J. Kim, Y. J. Kim, S. H. Yoon, and J. W. Jeon, "A recovery algorithm for PE files in a multi-core system," 2012.

[13] P. H. Meland, Y. F. F. Bayoumy, and G. Sindre, "The Ransomware-as-a-Service economy within the darknet," *Comput. Secur.*, vol. 92, 2020, doi: 10.1016/j.cose.2020.101762.

[14] K. Barik, S. Das, K. Konar, B. Chakrabarti Banik, and A. Banerjee, "Exploring user requirements of network forensic tools," *Glob. Transitions Proc.*, vol. 2, no. 2, 2021, doi: 10.1016/j.gltp.2021.08.043.

[15] A. Ospanova, B. Tuleuov, G. Karzhauova, and L. Kussepova, "Advanced Administration of Windows Based on Open Source Utilities," in *Lecture Notes in Engineering and Computer Science*, 2021, vol. 2242.

[16] V. V. Nikulin, "WINDOWS SECURITY AND WINDOWS DEFENDER," *Vestn. Obraz. konsortsiuma Sredn. Univ. Informatsionnye tekhnologii*, no. 2, 2021, doi: 10.52374/12569525_2021_18_2_7.

[17] T. H. Kim, G. C. Park, and S. S. Kim, "OS security enhancement system by considering security level," *Int. J. Multimed. Ubiquitous Eng.*, vol. 2, no. 4, 2007.

[18] M. Bhaganagare, P. Ghongade, P. Jadhav, and S. Nakate, "Customize Linux Operating System and Adding own Feature," *Int. J. Comput. Appl.*, vol. 109, no. 10, 2015, doi: 10.5120/19224-0889.

[19] R. Diesch, M. Pfaff, and H. Krcmar, "A comprehensive model of information security factors for decision-makers," *Comput. Secur.*, vol. 92, 2020, doi: 10.1016/j.cose.2020.101747.

[20] M. Krichanov and V. Cheptsov, "UEFI virtual machine firmware hardening through snapshots and attack surface reduction," 2022, doi: 10.1109/ispras53967.2021.00010.

[21] M. W. Hammond CISA, CRISC, CISSP, "How Do Your IT Controls Measure Up Against The Information Security Triad?," *CPA Pract. Advis.*, vol. 23, no. 2, 2013.