



## LockBit RaaS In-Depth Analysis

## Contents

<b>References</b>	<b>2</b>
<b>1 Introduction</b>	<b>4</b>
<b>2 Executive Summary</b>	<b>5</b>
2.1 Overview	5
2.2 LockBit Ransomware	5
2.3 RaaS Business Structure	6
<b>3 Technical Analysis</b>	<b>8</b>
3.1 The LockBit Attack Kill Chain	8
3.1.1 Target Selection	8
3.1.2 Preparation	9
3.1.3 Deployment and Execution	11
3.1.4 Demand and Negotiation	11
3.2 Management Panel	13
3.3 LockBit Decryptor	17
3.4 De-Anonymization	17
<b>4 Statistics and Observations</b>	<b>21</b>
4.1 Known Recruiter Profiles	22
4.2 Psychological analysis	22
<b>5 Money Flow</b>	<b>25</b>
<b>6 Conclusion</b>	<b>28</b>

Reference Number	CH-2021040801
Prepared By	PTI Team
Investigation Date	20.03.2021 - 08.04.2021
Initial Report Date	17.06.2021
Last Update	19.06.2021

### What's new ?

The PRODAFT Threat Intelligence (PTI) Team has published this report to provide in-depth knowledge about the threat actors who operate LockBit ransomware. The PTI Team has managed to extract decryption tools for most of the victims who were affected by LockBit. All affiliates of the ransomware group, including the developer, were also identified during the PTI team's investigation. This report answers questions such as : How do they select their targets? How many targets did they breach? How does the network operate? Who are the affiliates?

### Why does it matter ?

Ransomware is a growing problem and most of the research in this area is focused on analyzing malware samples and their encryption techniques. There are a limited number of sources that cover the working dynamics of the threat actors. Statistics related to the ransomware groups are formed by reported cases and approximations. This report contains the most accurate metrics and provides full visibility of a well-known ransomware group structure.

### What should be done ?

If no one pays any ransom, then the ransomware business will surely end. However, this is not an easy decision when C-levels are under constant pressure of losing reputation and money. The report will help the reader understand more about the threat actors and their operations. Several countermeasures will be provided along with the vulnerabilities used in ransomware cases. **#DontPanicDontPay**

## 1 Introduction

Ransomware is a type of malicious software that encrypts the victim's data and demands a ransom payment. In addition to making the data inaccessible, most of the attackers threaten to publish the victim's data unless the ransom is paid by a certain time ("*Double Extortion*"). Ransomware is mostly used as a money-making scheme by cyber criminals but it may also be used in different scenarios to coerce the user into any action by using leverage. While ransomware has been in use for decades, it has gained much popularity among cyber criminals in recent years due to the low level of experience it requires to conduct such attacks and the ease of using anonymous payment methods. It is expected that losses from ransomware attacks are likely to exceed \$20 billion by 2021 [2].

Ransomware can be separated into two groups based on their modus operandi, namely FAR (Fully Automated Ransomware) and SAR (Semi-Automated Ransomware). In FAR cases, ransomware generally infects the system via phishing emails or malicious web pages containing the malicious payload. The malware contains the code to spread deeper into the network, identify files, carry out the encryption, and leave a note to the victim, explaining how to make the payment for the recovery. Threat actors using FAR mostly focus on distribution channels and spreading methods of the malware and tend to stay away from making direct contact with the victim. Although the execution of FAR attacks is more straightforward, the success rate is much lower for high-value organizations as they have different protection tools such as AVs, access controls, and EDRs in place. Victims of FAR attacks are also more cautious about paying the ransom as there is a tendency among people to distrust automated systems. The behavior model is similar to a customer asking for a representative before purchasing to clarify doubts. It is troubling to see people still want to negotiate and discuss the payment with a human being, knowing that they are criminals.

On the other hand, SAR attacks involve manual interaction of cyber criminals with the victims' servers. To access the network of the target organization, attackers often use 0-day or N-day exploits. We also observe that some of the attackers buy RDP or VPN credentials directly from other hackers and underground markets. Upon successful entry, attackers use common pentest tools for lateral movement in the network, escalate their privileges, and carry out the encryption step via set of encryption tools and/or ransomware. On rare occasions, some of the encrypted data can be recovered due to operational mistakes [5].

Modern cyber crime businesses use hierarchical work flows to monetize their operations. X (Ransomware, Malware, Dropper, etc.) as a Service models became popular among criminals as a different skill set is required to conduct such advanced attacks. In this report, we will explain how RaaS models work in general and also present in-depth knowledge from the attackers' side. We believe that our findings will help other researchers understand the working dynamics of similar ransomware groups.

In this report, we will analyze a widely known ransomware called "LockBit" and provide a deep understanding of how criminals breach and monetize their operations. We will not focus on sample analysis as there are many resources covering the technical analysis of the malware execution. Instead, this will be the first report to presents all possible behind-the-scenes



information of a large ransomware group.

Please note that this report has two versions. The *"Private Release"* is provided to law enforcement agencies, applicable CERTS/CSIRTS, and members of our U.S.T.A. Threat Intel Platform (with appropriate annotations and reductions). Likewise, the *"Public Release"* is publicly disseminated for the purpose of advancing the global fight against high-end threat actors and APTs.

## 2 Executive Summary

### 2.1 Overview

LockBit is a relatively new ransomware which has become quite popular in the past few months. Formerly known as "ABCD" ransomware, it has since grown into a unique threat within the scope of these extortion tools [4]. Our PTI Team started analyzing the LockBit group around 20.03.2021 based on an emergency request from one of our clients. The investigation was completed by successfully retrieving the decryption keys and restoring the files of our client. Moreover, we helped dozens of other victims to retrieve their decryption keys, thus preventing an estimated 8 million dollars of loss. This report presents interesting facts about the ransomware business by accurately showcasing rates, commissions, infection techniques, and the criminal organization's structure.

### 2.2 LockBit Ransomware

LockBit ransomware is a malicious program that prevents users from accessing their computers unless the requested ransom payment is given to the attackers. LockBit can automatically scan a network for useful targets, spread the infection, and encrypt all computers that are available. This ransomware is used in unique attacks against companies and other organizations.

According to the statistics shared by Coveware [3], The LockBit ransomware attacks has increased drastically in the Q4 of 2020. The following table shows that LockBit ransomware is in the third place among other ransomware families, with 7.5% of the market share.

## Most Common Ransomware Variants in Q1 2021

Rank	Ransomware Type	Market Share %	Change in Ranking from Q4 2020
1	Sodinokibi	14.2%	-
2	Conti V2	10.2%	+4
3	Lockbit	7.5%	+6
4	Clop	7.1%	New in Top Variants
5	Egregor	5.3%	-3
6	Avaddon	4.4%	+3
7	Ryuk	4.0%	-4
8	Darkside	3.5%	New in Top Variants
9	Suncrypt	3.1%	-1
9	Netwalker	3.1%	-5
10	Phobos	2.7%	-1

*Top 10: Market Share of the Ransomware attacks*

**Figure 1. Coveware's Most Common Ransomware Variants in Q1 2020**

For ransomware creators, RaaS is a new business model. Said creators, similar to software as a service (SaaS) providers, sell or lease their ransomware variants to affiliates, who then use them to carry out attacks. This business model often includes a platform in the form of a management panel. Customers of LockBit service (affiliate threat actors) use this management panel to create new ransomware samples, manage victims, and get statistics about their attacks. According to the PTI Team's investigation, LockBit threat actors are also using methods such as extortion and victim shaming to force victims to pay the ransom money.

**Analyst Note :** The concept of "victim shaming" can be explained as a pressure tactic often used by ransomware groups to push victim organizations into fulfilling the ransom demand. These tactics may include threatening to release stolen confidential data of the victims or e-mailing the business partners of the victims about the ransomware attack.

### 2.3 RaaS Business Structure

RaaS owners employ multiple affiliates who are responsible for breaching into victims' systems and encrypt their files. These affiliates are selected mostly from forums among highly skilled hackers with penetration testing backgrounds. Another way of becoming an affiliate

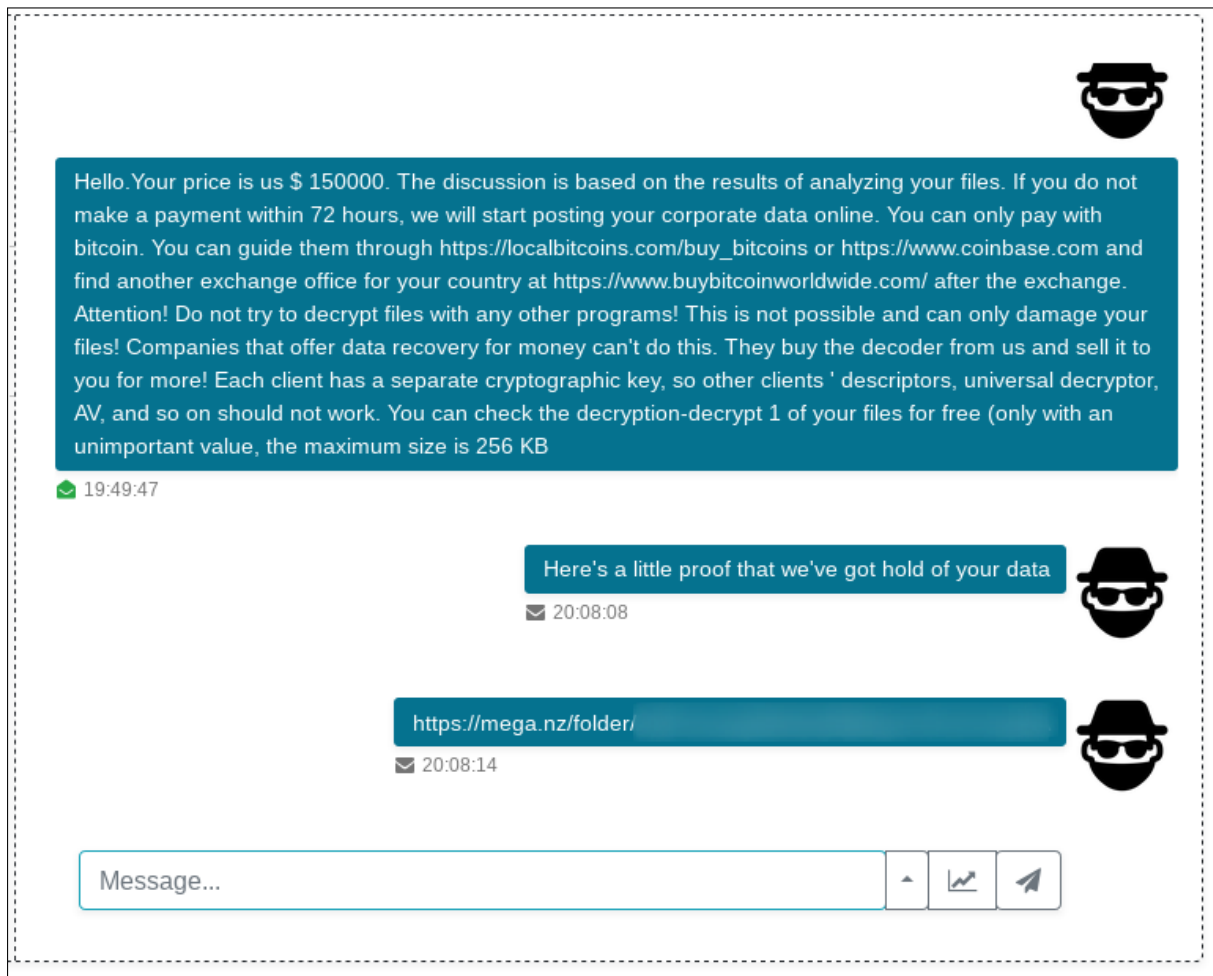


Figure 2. Example of LockBit threat actors using extortion

is to have an established trade network to obtain access to information from other criminals. In both cases, RaaS owners require references from other criminals before hiring any affiliate. Reputations of the criminals become essential in such cases. Most of the affiliates earn between 10%-30% commission from each ransom payment. RaaS owners also often provide virtual machines, exploits, and tools for their affiliates to support their attacks. Each affiliate has access to a panel where they can monitor their victims and communicate with them. An affiliate panel usually has the following capabilities :

- Creating/Building a ransomware executable
- Providing a decryptor program upon payment
- Providing a payment gateway (cryptocoins) for the victims
- Calculating the commission rates of the affiliates
- Monitoring victims and statistics
- Providing a chat functionality to talk with the victims

Affiliates try to maximize their profit by forcing victims to pay using different psychological

tactics (see Section 4.2). Moreover, affiliates are expected to be in a constant effort to breach new targets. Whenever an affiliate becomes inactive for a long period of time, RaaS owners remove the account of that affiliate, which also effects their reputation.

### 3 Technical Analysis

This section contains technical analysis of the LockBit ransomware as a service (RaaS) platform including the management panel, ransomware sample, decryptor software, and the step-by-step analysis of a LockBit attack kill chain. This section also contains intelligence about the threat actors (developers and affiliates) using LockBit service and their TTP analysis.

#### 3.1 The LockBit Attack Kill Chain

The following steps will briefly explain the overall LockBit attack kill chain. Every technique, tactic, and procedure is based on the LockBit service affiliates at the time of the PTI Team investigation. The attack vectors and every kind of actor-specific behaviour can be different in every LockBit attack, given that LockBit is a RaaS platform.

##### 3.1.1 Target Selection

Ransomware operators use multiple methods for selecting their next potential target. LockBit affiliates use mass vulnerability scanning, phishing, and credential stuffing[9] as main sources for finding new victims. According to our investigation, the most frequent method used by the LockBit group is to buy already-compromised servers & RDP accesses from underground shops. Such credentials can be purchased for as low as \$5, thus making it very lucrative for affiliates considering the demanded ransom amount. During the LockBit investigation, the PTI Team was also able to identify a couple of the attack vectors used for mass vulnerability scanning by the LockBit affiliates. According to the chat logs between the LockBit affiliates and multiple victims, the Fortinet VPN exploit [7] was one of the most used methods to gain access to the target company networks.



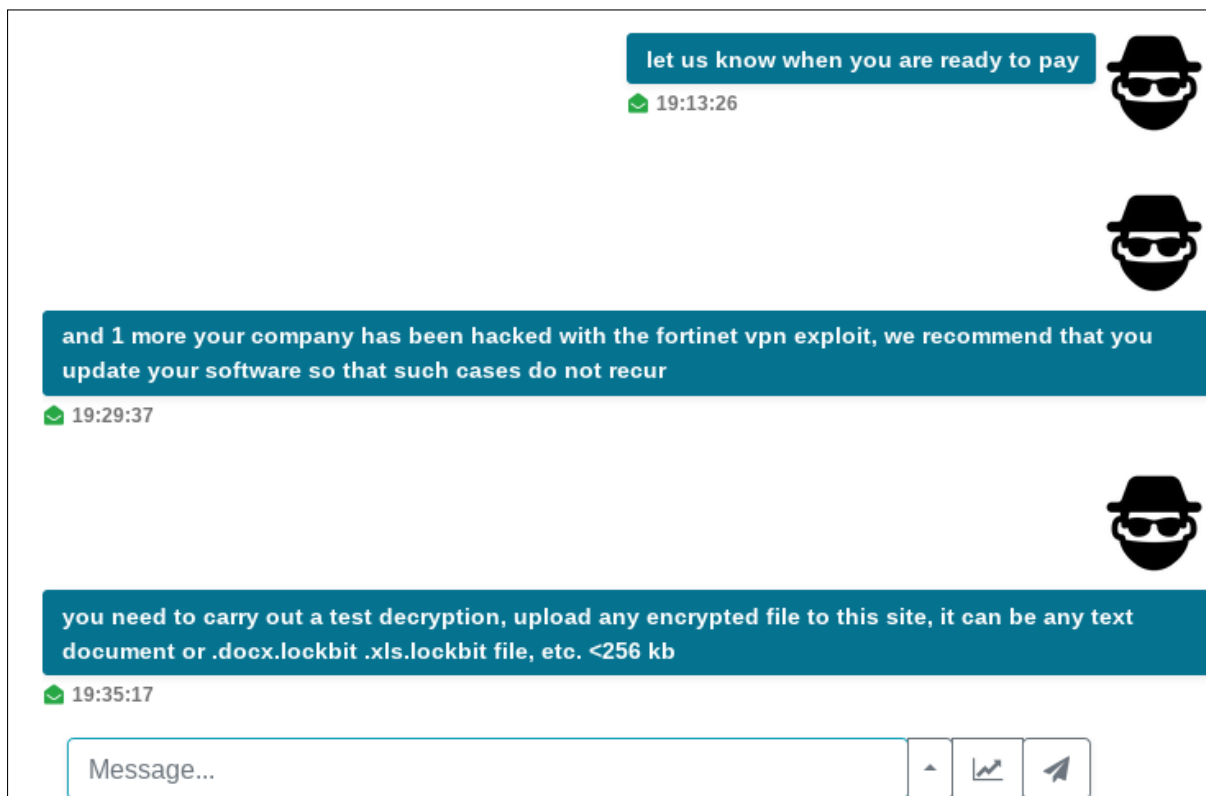


Figure 3. LockBit affiliate explaining the used attack vector

The PTI Team was also able to contact multiple LockBit victim companies. Based on the forensic analysis of the victim companies, the PTI Team came to the conclusion that LockBit affiliates also use generic phishing campaigns and credential stuffing attacks for gaining access to the target company servers.

### 3.1.2 Preparation

After gaining access to the target company servers, LockBit affiliates usually starts the enumeration process. According to our forensic investigations on multiple LockBit victims, the PTI Team observed that before launching the LockBit ransomware, attackers tries to identify mission critical systems such as domain controllers, backup servers or NAS devices. Once the necessary enumeration is done by the attackers, the data exfiltration phase begins. The LockBit attackers evaluate the data inside the breached system and decide whether it is important for the target company. The critical data gets exfiltrated by the attackers and uploaded to free file upload services such as MEGA. Uploaded data are used for extortion while negotiating with the victims.

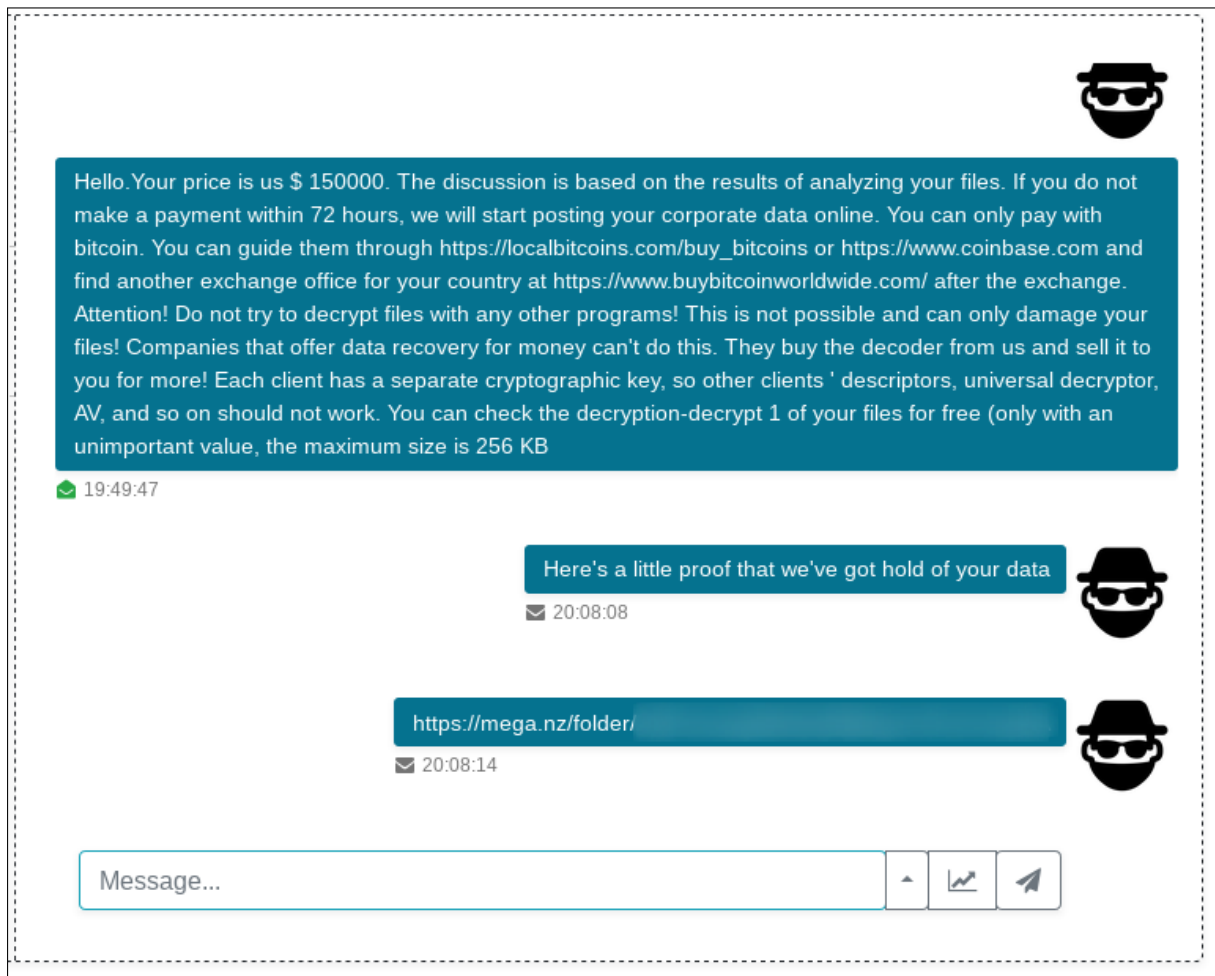


Figure 4. Exfiltrated data used for extortion

After the data exfiltration phase, a unique LockBit ransomware sample is generated from the build page of the LockBit management panel. The build page of the LockBit management panel is shown in the following image.

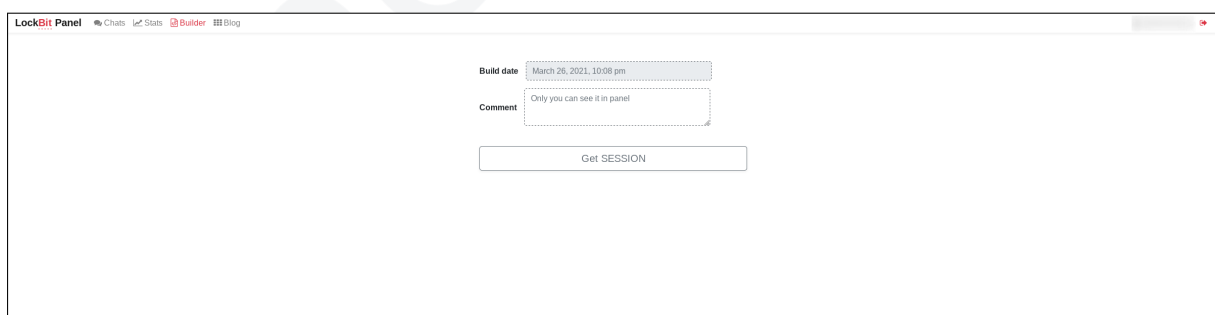


Figure 5. LockBit management panel build page

Affiliates are able to build unique ransomware samples by entering an explanatory comment. The build comments are used for identifying the victims and their systems. Usually LockBit

affiliates enter the target company name as a comment. Once the victim company starts a dialog with their unique session key, the chat session is tagged with the corresponding build comment on the LockBit management panel database.

### 3.1.3 Deployment and Execution

In this step, the LockBit ransomware generated by the affiliates is executed manually inside the target company systems. Once the LockBit ransomware is executed in a system, it will immediately begin the reconnaissance phase. In this phase of the ransomware attack. The LockBit sample will try to enumerate all the accessible directories and network shares inside the target system.

After the enumeration LockBit ransomware encrypts each file with a random AES key, which is encrypted with the static public key inside the LockBit sample. Finally encrypted AES key is inserted into a specific offset inside the file. Thus every file inside the target system is encrypted with a different key, and each file can only be opened by the randomly generated RSA private key during the build of the unique sample on the management panel.

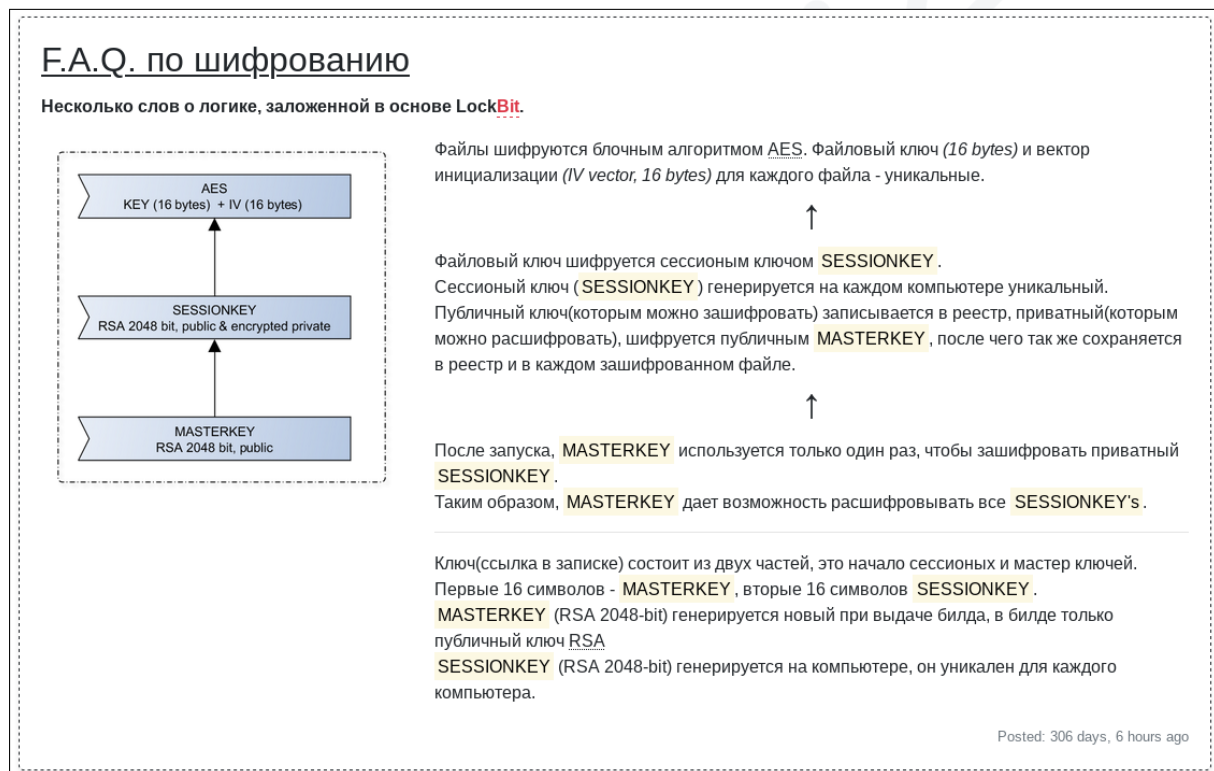


Figure 6. LockBit ransomware working logic

### 3.1.4 Demand and Negotiation

At the end of the ransomware execution phase, all important files of the victim are encrypted, backups are deleted, and the system wallpaper is changed to the following image.



Figure 7. Victim desktop after LockBit attack

As described in the wallpaper image, LockBit ransomware creates "Restore-My-Files.txt" and "LockBit-note.hta" files on the target system desktop. The HTA file is executed automatically upon creation. The "LockBit-note.hta" file is a well-designed HTML page explaining the situation and ways to contact the LockBit attackers for purchasing a decryptor software.

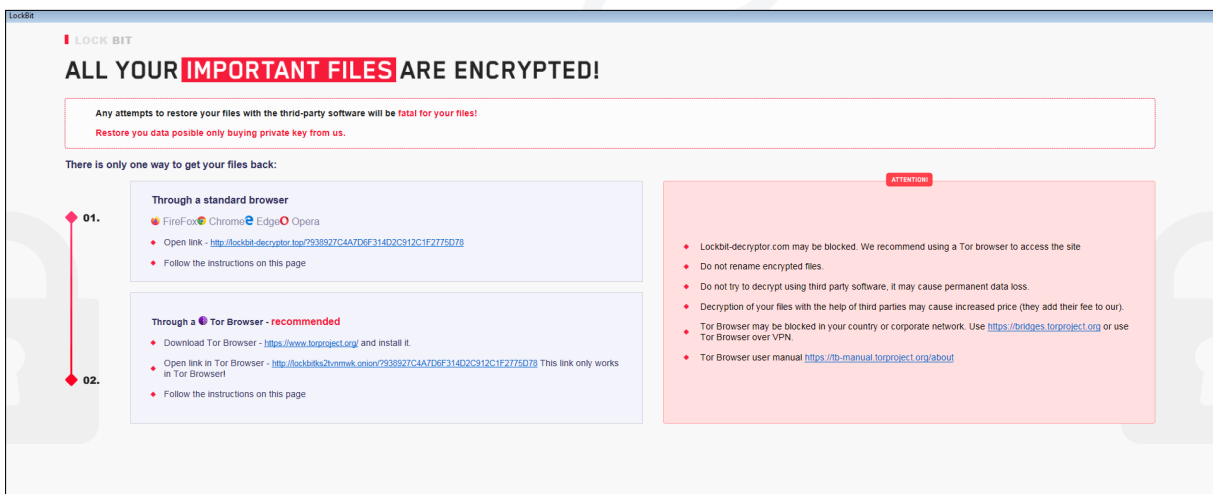


Figure 8. LockBit ransom note inside the victim's system

According to the ransom note, the <http://lockbit-decryptor.top/> and <http://lockbitks2vtmwmk.onion/> websites contain further instructions for purchasing a decryptor software. The ransom note also contains instructions about installing a TOR browser in order to access the LockBit's ONION web page. During the time of the PTI Team's investigation, lockbit-decryptor.top domain was no longer active. The links inside the ransom

note contain a get parameter value formed by victims' master and session keys. Once the victims visit the LockBit website with the given unique link, they are greeted with the following page.

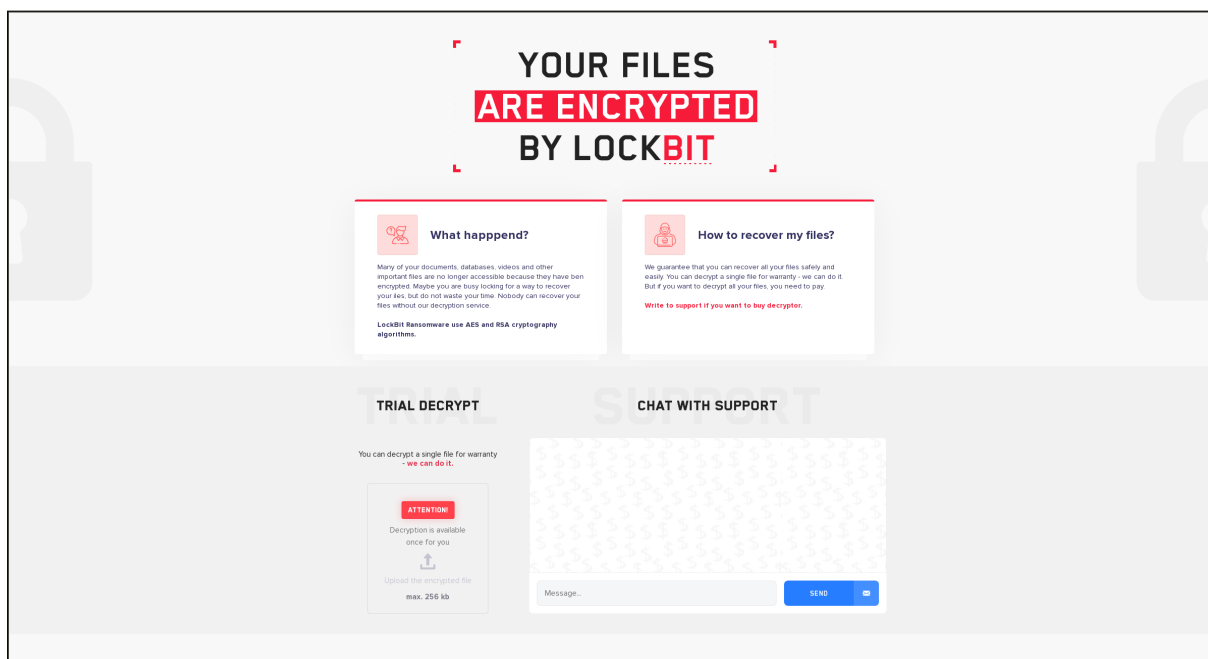


Figure 9. LockBit victims' landing page

The LockBit contact page contains "CHAT WITH SUPPORT" and "TRIAL DECRYPT" sections. Victims are expected to get in contact with the LockBit attacker using the chat window regarding the purchase of the decryptor software. Once a victim sends a message over their unique contact URL, a new victim tab with the corresponding build comment shows up on the LockBit management panel dashboard. The "TRIAL DECRYPT" section inside the victim dashboard allows the victims to decrypt a single file with a size smaller than 256KB. This particular file must originate from the system with the corresponding ID (unique contact URL). The LockBit panel automatically checks whether the given file actually belongs to the corresponding victim ID and then serves the decrypted file to the victim. This feature ensures the victims that LockBit attackers are able to decrypt their files successfully and in an automated fashion.

### 3.2 Management Panel

During the investigation, the PTI Team was able to detect and gain access to some parts of the LockBit RaaS infrastructure. The LockBit infrastructure consists of a management panel hosted as a TOR hidden service website with the address <http://lockbitaptku3l2q.onion/>. The management panel is mainly used for managing victims, affiliate accounts, generating new ransomware builds, and serving the decryptor software if the demanded ransom is paid.



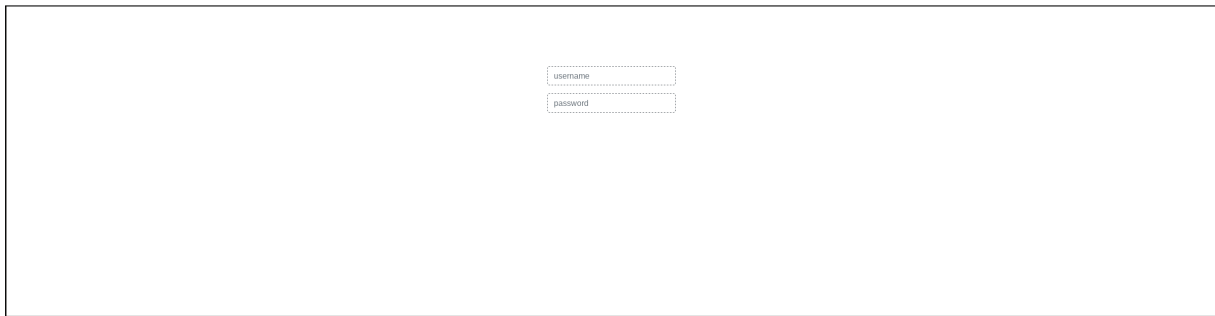


Figure 10. LockBit management panel login page

As described in the previous step, the main dashboard of the LockBit management panel contains the chat window. As can be seen in the following image, the LockBit affiliate often starts the conversation with a prepared text that explains the situation briefly and informs the victims about the current decryptor price, payment deadline, payment method (BTC), and instructions about how to obtain bitcoin for payment.

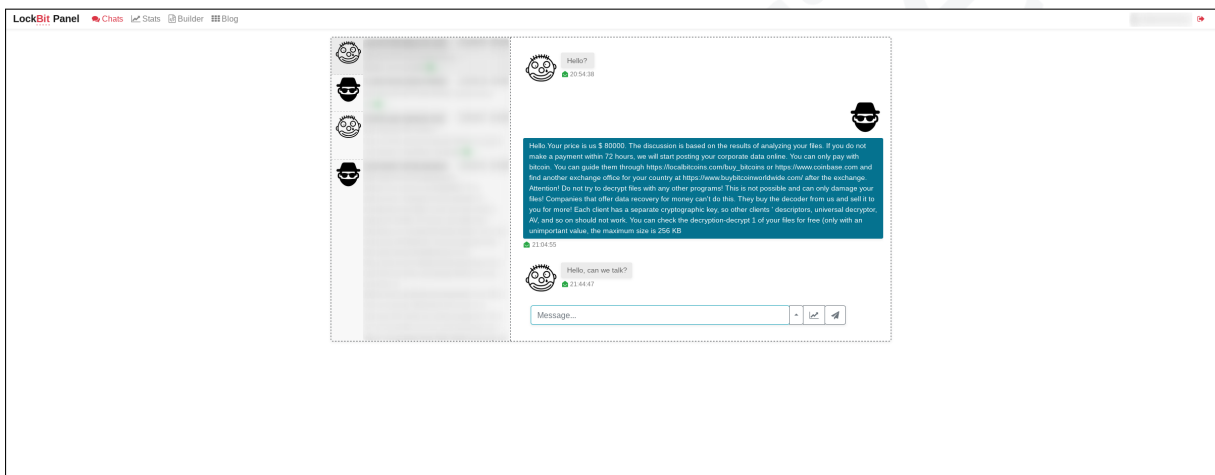


Figure 11. LockBit management panel chat page

Affiliates also explain the "TRIAL DECRYPT" mechanism to the victims because the trial decrypt step is mandatory for purchasing the decryptor software. Each victim must upload a file for trial decrypt in order to get the decryptor software. This mechanism prevents third-party intervention and ensures that the negotiator actually has access to the victim's files. On the chat window there is a victim details button that displays the victim master and session keys, first and last visit dates, total views, build date, and build comments. The following image contains the mentioned victim details window.



Figure 12. LockBit management panel victim details

The LockBit affiliates can also view their current victim' statistic on the management panel statistics page. The page contains a view chart, recently visited victims, and recently uploaded test files. The affiliates are able download the decrypted victim test files from this page.

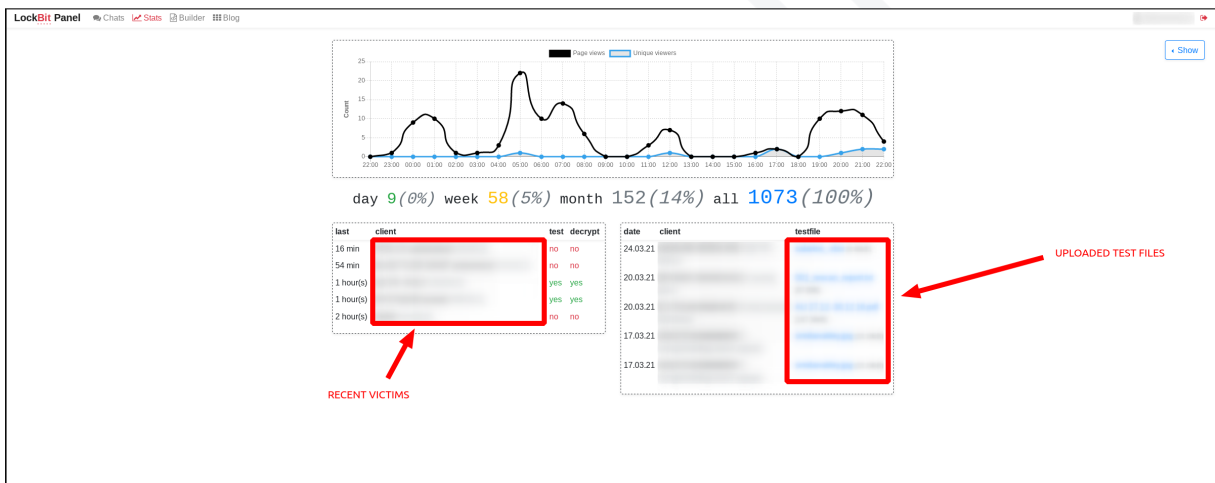


Figure 13. LockBit management panel statistics page

Finally, inside the affiliate management dashboard chat window there is a "Decrypt" button for automatically generating the decryptor for that particular LockBit victim. In order to successfully generate the decryptor, victims need to upload an encrypted file for trial decryption. Once the decryptor is generated for that particular victim, the chat session gets removed from the LockBit affiliate's dashboard and the conversation ends.

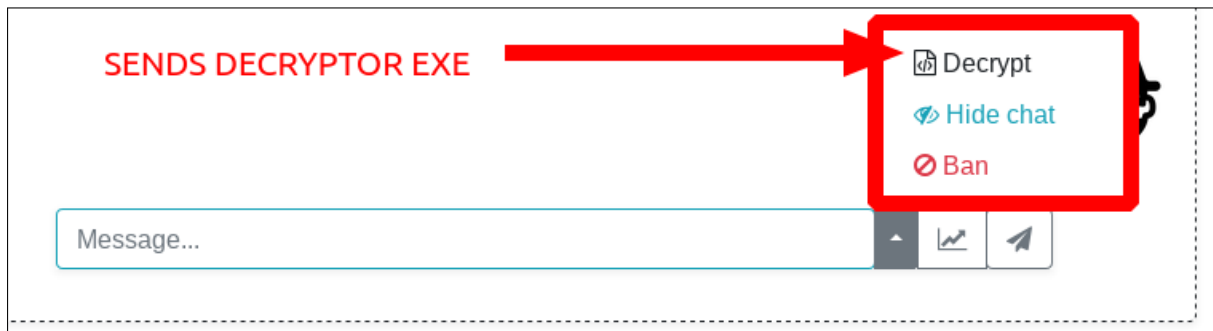


Figure 14. LockBit management panel victim decrypt button

Another role of the LockBit management panel is managing the affiliate accounts. When the admin user logs into the management panel, the user is greeted with extra "Users", "BlogPost", "PhpMyAdmin" pages for adding new affiliate accounts, publishing new blog post entries and accessing the PhpMyAdmin panel.

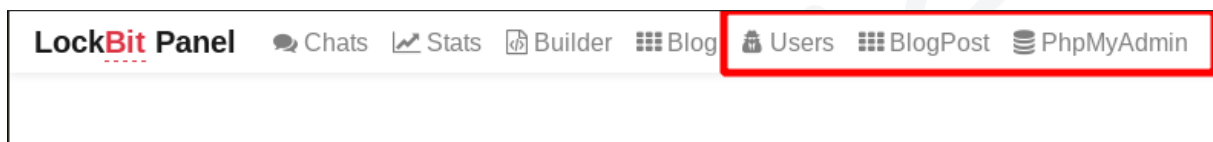


Figure 15. LockBit admin user panel menu

The admin user is also able to view every affiliate chat session inside the main dashboard of the management panel. The statistics page also includes all victim page views of every affiliate account when logged in with the admin user.

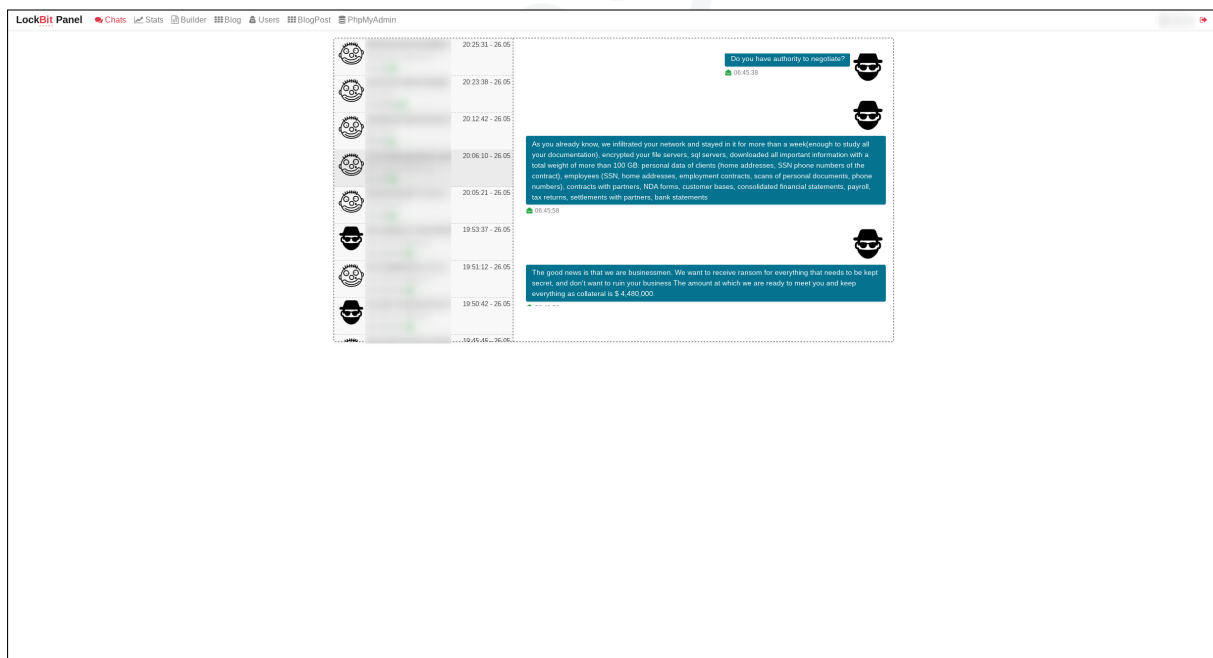


Figure 16. LockBit admin user dashboard

The admin user is also able to access the PhpMyAdmin panel for removing affiliate users and manually extracting decryption keys of the victims. The PhpMyAdmin panel is found at address <http://lockbitaptku3l2q.onion/bfdnffektc/>.

### 3.3 LockBit Decryptor

Once the decrypt button is pressed for a victim on the management panel, a unique decryptor EXE file is generated for that particular victim's ID (master and session keys). If the victim used the trial decryption attempt, the generated decryptor software link will be displayed at the bottom of the victim's chat page. From this point, victims can download the decryptor EXE file and run inside their encrypted systems for decrypting their files.

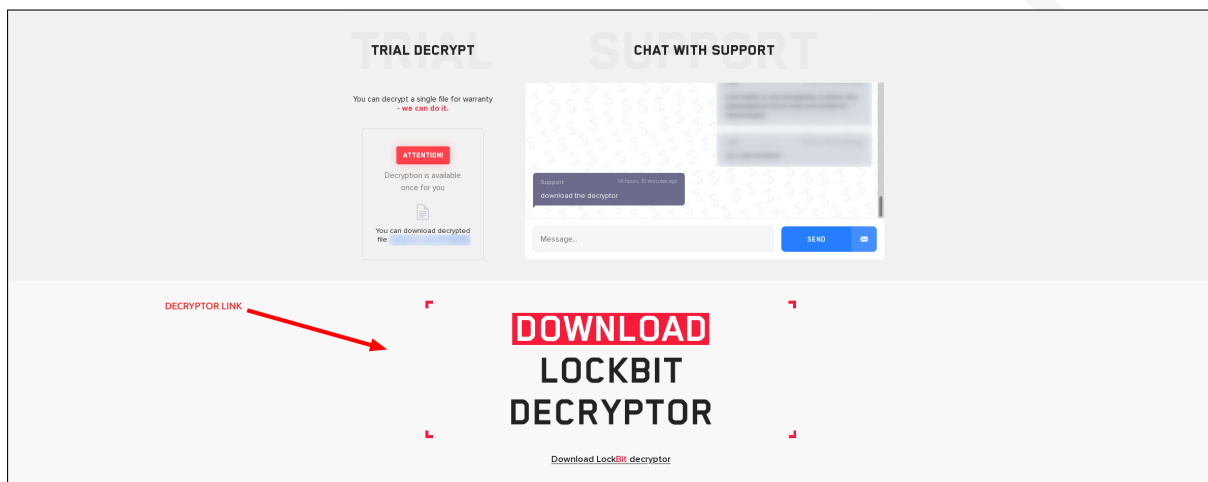


Figure 17. Enabled LockBit decryptor link inside the victim chat dashboard

According to the PTI Team analysis, decryptor software successfully decrypts the locked files inside the victim's system without performing any malicious activity.

### 3.4 De-Anonymization

The PTI Team also focused on revealing the identity of the LockBit affiliates, retailers, and developers. The management panel analysis revealed much information about the LockBit affiliates. As described in Section 3.2, the admin user is able to view and manage affiliate accounts on the system. As can be seen in the following image, every affiliate account is created with a Jabber contact address.

The screenshot shows the 'Users' page of the LockBit admin panel. It features a table with columns for '#', 'Username', 'Reg date', 'Jabber', and 'Last access'. The table lists 28 users, with the first 15 highlighted in green and the remaining 13 in yellow. Below the table is a login form with fields for 'Login', 'Jabber', and 'Password', and a 'Login' button.

#	Username	Reg date	Jabber	Last access
1	OFFTITAN [64]	18:57 16.05		19:56:58 26.05
2	petya [10]	10:29 06.01		19:56:57 26.05
3	term2 [104]	12:54 21.04		19:56:55 26.05
4	qwasaqwa [93]	17:05 15.09		19:56:53 26.05
5	mk2232 [96]	12:27 11.11		19:56:52 26.05
6	mctom87 [90]	16:37 29.08		19:46:42 26.05
7	term [54]	08:46 23.04		19:18:18 26.05
8	Bryce [38]	23:04 04.05		19:18:13 26.05
9	Jokerservice [36]	17:48 29.02		19:13:58 26.05
10	Mikki [71]	17:18 09.06		18:56:08 26.05
11	wallstreet88 [44]	11:56 11.03		15:20:44 26.05
12	Samuel_J [80]	18:28 01.08		15:15:17 26.05
13	advercap0 [100]	18:31 02.02		14:28:45 26.05
14	Blacklion [70]	14:07 29.05		20:40:13 24.05
15	digitalocean [68]	15:15 22.05		13:24:56 21.05
16	anzucruz [98]	21:55 08.12		15:46:47 11.05
17	johnyee12 [34]	20:32 16.02		16:17:13 30.04
18	bleepingcomputer [94]	19:46 26.09		20:10:34 22.04
19	Baster [84]	12:40 15.08		10:48:49 02.04
20	waza [67]	13:04 19.05		02:27:18 16.03
21	masteryoda [31]	13:53 12.02		01:05:25 14.03
22	shock [91]	15:23 31.08		14:56:58 10.03
23	valerinc [83]	13:58 12.08		19:19:54 20.02
24	malbudad [102]	16:36 14.02		10:23:42 17.02
25	Adv72 [103]	13:06 16.02		13:06:12 16.02
26	Parliament [92]	13:39 04.09		21:45:21 08.02
27	adv17 [101]	18:38 02.02		11:49:45 08.02
28	s4 [99]	11:28 23.12		22:19:34 23.12

Figure 18. User's page of the LockBit admin panel

Table 1 contains the usernames, number of victims, register and last access dates for every LockBit affiliate.



Username	Victims	Register Date D.M H:M	Last Access Date D.M H:M
OFFTITAN	64	16.05 18:57	26.05 19:56
petya	10	06.01 10:29	26.05 19:56
term2	104	21.04 12:54	26.05 19:56
qwsaqwsa	93	15.09 17:05	26.05 19:56
mik2232	96	11.11 12:27	26.05 19:56
mctom97	90	29.08 16:37	26.05 19:46
term	54	23.04 08:46	26.05 19:18
Bryce	58	04.05 23:04	26.05 19:18
Jokerservice	36	29.02 17:48	26.05 19:13
Mikki	71	09.06 17:18	26.05 18:56
wallstreet88	44	11.03 11:56	26.05 15:20
Samuel_J	80	01.08 18:28	26.05 15:15
advertcap0	100	02.02 18:31	26.05 14:28
Blacklion	70	29.05 14:07	24.05 20:40
digitalocean	68	22.05 15:15	21.05 13:24
aruzcruz	98	08.12 21:55	11.05 15:46
johnyes12	34	16.02 20:32	30.04 16:17
bleepingcomputer	94	26.09 19:46	22.04 20:10
Baster	84	15.08 12:40	02.04 10:48
waza	67	19.05 13:04	16.03 02:27
masteryoda	31	12.02 13:53	14.03 01:05
shock	91	31.08 15:23	10.03 14:56
valterinc	83	12.08 13:58	20.02 19:19
malibudad	102	14.02 16:36	17.02 10:23
Adv72	103	16.02 13:06	16.02 13:06
Parliament	92	04.09 13:39	08.02 21:45
adv17	101	02.02 18:38	08.02 11:49
s4	99	23.12 11:28	23.12 22:19

**Table 1.** Full List of LockBit Affiliate Information

The reconnaissance on the Jabber addresses and aliases of the affiliates revealed that two of the threat actors might also be working for the Babuk [6] and REvil [10] ransomware groups.

Detailed information about the connection between the two threat actors and other ransomware groups is redacted due to ongoing investigation.

The analysis on the victims' chat logs revealed several other BTC wallet addresses shared additionally with some of the victims. The PTI Team is still conducting taint analysis on the wallet addresses to detect shared spending or laundering attempts.

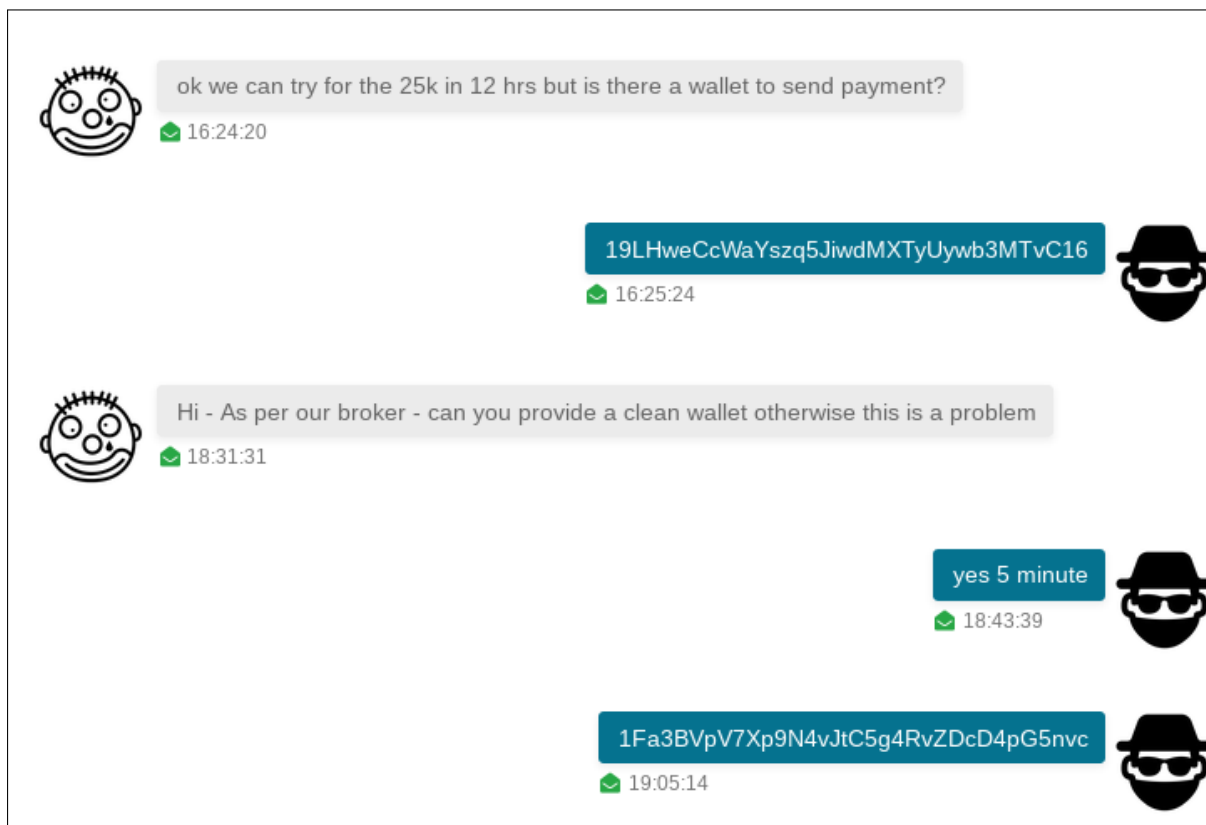


Figure 19. LockBit threat actor giving out alternative wallet addresses

The PTI team was able to capture the **45.135.187.132** IP address on Monday, 22 March 2021, at 21:30:03 UTC, which is the IP address of one of the LockBit developers. Based on our observation, the IP is another proxy layer (probably a VPN) used before accessing the TOR network. We were also able to identify the OS details of the hidden server during our investigation. The hidden service host is found to be a Ubuntu server with the host name "Fibonacci".

```
Linux Fibonacci 4.15.0-99-generic #100-Ubuntu SMP Wed Apr 22 23:32:56 UTC+3 2020
x86_64
/>> █
```

Console 1. OS Details of the LockBit onion server

The captured IP address with the corresponding timestamp were shared with the local law enforcement authorities for further legal action.

## 4 Statistics and Observations

According to the victim details obtained from each of the affiliate accounts on the LockBit management panel, the PTI Team discovered that the LockBit RaaS platform has successfully infected thousands of devices around the world. Almost all of the victims are enterprise corporations. The average ransom amount is calculated to be roughly \$85,000.

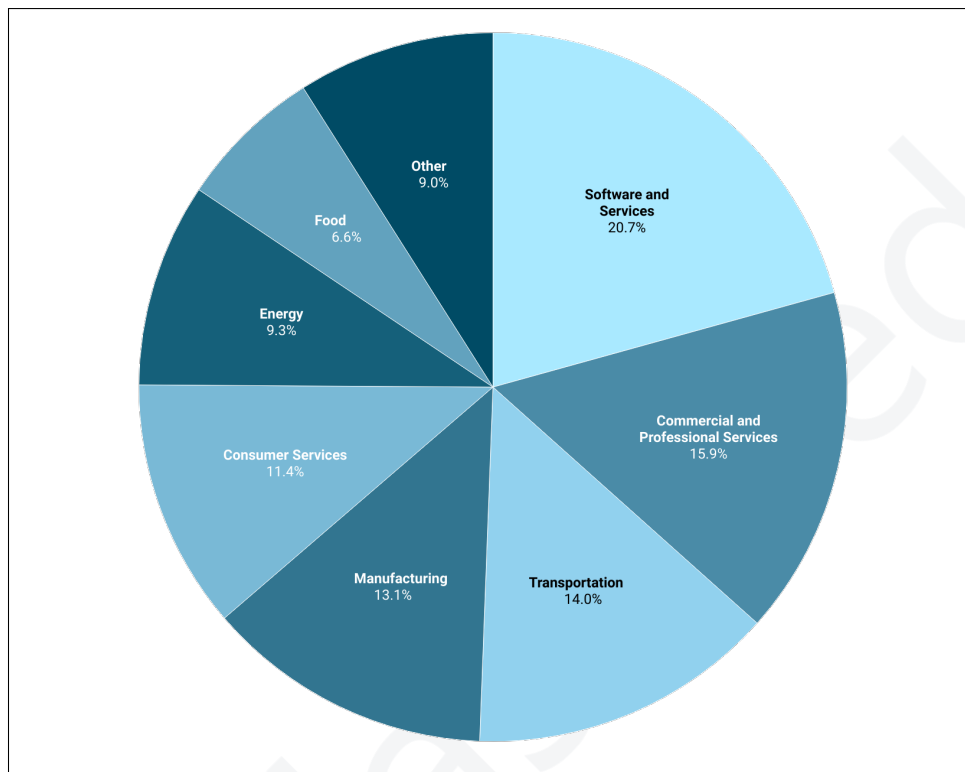


Figure 20. Sector distribution of victims

Victim sector distribution does not show a significant value for the investigation as criminal groups buy accesses and scan vulnerable hosts almost in a random fashion. We can see that more than 20% of the victims were operating in the software and services sector. Commercial and professional services as well as the transportation sector were also highly targeted by the LockBit group. However, it should be noted that the value of the ransom is determined by the affiliate after various checks using online services. This value does not solely depend on the sector of the victim.

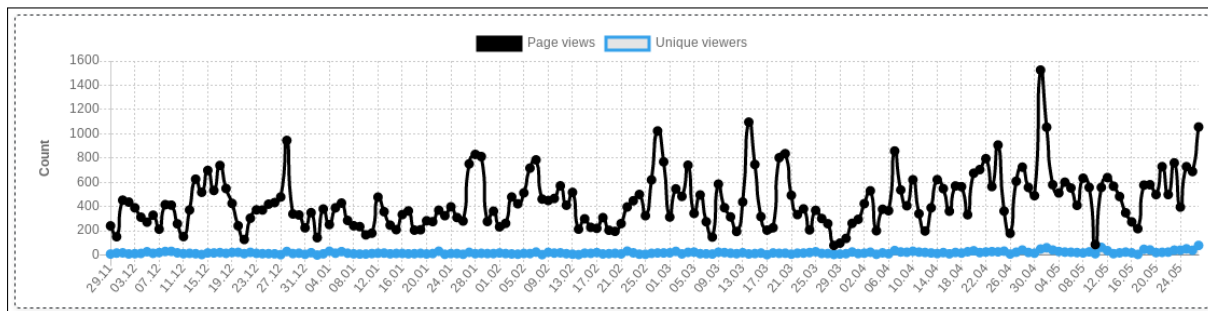


Figure 21. Victim page view statistics

Page view statistics show us who the ransomware victims are. We can clearly see that the activity peaked around the beginning of May 2021. The indicator also shows that on the 11th of May, there were no page views. This might be caused by a fault, system upgrade, or a possible DDOS attack. Several other ransomware groups were also presented in global articles around these times, which might be another indicator of a possible server upgrade/transfer. The server became active after the 12th of May, and the activity increased for the following week. As the TOR hidden server reroutes the traffic to 127.0.0.1, the unique IP count is shown as 0 on most of the dates. Several deviations present local page hits (mainly from the developer side).

#### 4.1 Known Recruiter Profiles

Ransomware groups hire several people from deepweb/darknet forums to attract new affiliates into their network. These recruiters generally create topics in well-known forums and discussion boards. In order to become an affiliate, one must have high skills, motivation, and good references who can verify the candidate. In the following examples, we present several "Call for Application" posts written by the LockBit recruiters.

On average, affiliates gain between 10%–30% commission from each ransom payment.

#### 4.2 Psychological analysis

"Do you accept the terms of the contract?"

It bears all the hallmarks of the final sentence of a success business conversation – albeit preceded by :

"ALL YOUR DATA IS ENCRYPTED. To recover the data, you need a decryptor. The cost of the decryptor is 1000 US dollars. Payment is accepted only in bitcoins. After payment, you will receive a decryptor and instructions on how to counteract hacking. Your data will be restored within 15–30 minutes. Do you accept the terms of the contract?"

The sense of panic is spreading. Perhaps your whole business is thrown down a black hole, and since you want to save your business and the data it has generated in terms of business intelligence, you engage with the organised group whose business idea happens to be a

criminal one. They prey on the notion that your livelihood is under threat and you expect to save it. Victim shaming is a powerful tool of persuasion.

Looking at Figure 9, one can not note the "business as usual" atmosphere that is conveyed. There "What" and "How" boxes adequately describe what happened and how you can solve it. Like any proper vendor they offer a sample of their product – the victim is given an opportunity to "TRIAL DECRYPT" one of the ransomed files. Similar to regular businesses they offer "CHAT WITH SUPPORT", should you have any questions ...

We managed to acquire chat logs between the two parties i.e. the victims of extortion and the perpetrators. In most cases, they start with the message above or a similar one and follow a certain pattern : from duress, threats, and prof of data and payment instructions to (almost) friendly advice.

Once the initial sense of helplessness settles, the victims reach out through the platform – the chat forum – provided by the extortionists. What follows is rather a normal conversation between two parties engaged in negotiations :

Negotiations :

"name the amount you are willing to pay"

"If you offer the amount and it suits us, we will make a deal"

Duress and threats :

"If you do not make a payment within 72 hours, we will start posting..."

"I will accept your offer if you pay within 12 hours! Hurry up!"

"24 hours for payment, then the amount will increase to \$30,000"

and :



"Attention! Do not try to decrypt files with any other programs! This is not possible and can only damage your files!"

"Don't mess with us"

To further their business case the perpetrators offer proof :

"Here's a little proof that we've got hold of your data"

followed by a link.

Payment instructions :

"You can only pay with bitcoin. You can guide them through..."

followed by specific instructions and bitcoin wallet information.

Once the victim has provided the wallet to the perpetrators, they start to stall before they engage in ransom jacking, from the simple

"wait" to

"the key production time is from 12 to 24 hours"

They also try to come across as if they are doing you a favor, similar to a regular business transaction such as purchasing an insurance :

"After the payment, we will tell you the vulnerability and you will close it. A second attack will be excluded"

Generally the conversations follow a pattern of standardised answers as seen above, however one cannot refrain from thinking that they may be Star Wars fans : *"Look for options, time you have."*

Crime as a service (CaaS) is in this case manifested as ransomware as a service (RaaS) – a service provided by computer experts who happen to be part of criminal networks. It is beyond the scope of this report to further describe the underworld of organised crime. However, this is a highly organised and well-developed undertaking.

The chat logs indicate a pattern, comparable to a regular telemarketing call, where the individual perpetrators have the freedom to offer discounts and manage deadlines while still being in control. Considering the nature of the organizational chart of organised

crime, it cannot be disregarded that, as a management tool, the use of force, whether implicitly or explicitly, is always a option. As for the victims, they all have their account of what happened and the reason for accepting to pay the ransom. Regardless of the circumstances and the justification for agreeing, paying ransom continues to fuel the industry.

“We appreciate your patience and understanding”

## 5 Money Flow

During our analysis, we investigated some of the wallet addresses and investigated the money flow throughout the blockchain. We observed that the crime group frequently uses CoinJoin mixing techniques (Wasabi wallet) and several money-laundering services to obfuscate their transactions. In addition to that, closer inspection of the transactions shows some of the money has been converted into different cryptocurrencies (Monero, Zcash) using prevalent exchangers like Changenow, Simpleswap, etc. These results provide further support for the idea that KYC/AML procedures are inadequate to stop the ransom payments due to the nature of the operation. Some of the wallet addresses and received amounts are listed in Table 2.

Wallet ID	Received Amount
1PtfhwkUSGVTG6Mh6hYXx1c2sJXw2ZhpeM	5.79744443 BTC
13fd2yY6YZCfxBThW56b2qB64GoDAdZ5kX	0.55172631 BTC
141H8ggje2xpkaU5omBM2NKmVRaXRrDUP	0.17925505 BTC
14gDLtXDbeEoABDNdBWfo8gwzAEgrFVSi3	0.52314268 BTC
1AtNrniXD3VNshFJV9VCrkYyojttq7XfS	0.48942500 BTC
1ECam5rHSnvDdayDTJhyhgu9vmsZA7RPVk	0.52958356 BTC
1GDyofmVdpDQorFSJCMALcJpGKEMZGfEvh	1.25979324 BTC
1HPz7rny3KbjEUURHKHivwDrNWAAsGVvPH	3.64764636 BTC
1JRy9iccU7WapSzdoCDLxFZ8VKViPrvjPA	0.18086716 BTC
1LQnQBGq62xsqpm7e3f5PgSTfVaPopHMY	3.03000000 BTC
1PCAxk4jqA7fnLdcrQj2o9swa95DejVpv6	1.16662661 BTC
bc1qq9p72p304ct8fgel6a02qpp5wyd0q8fm2lggzt	2.53950000 BTC
bc1qrqfa59znk9g6u5u52ryzhpqyv8nu4rp6rgc5z	0.12000000 BTC
bc1qvqpu75msnccdyx744dkz2q8adkdy6eccg0svp2	0.30491839 BTC

**Table 2.** Some of the wallet addresses used during extortions

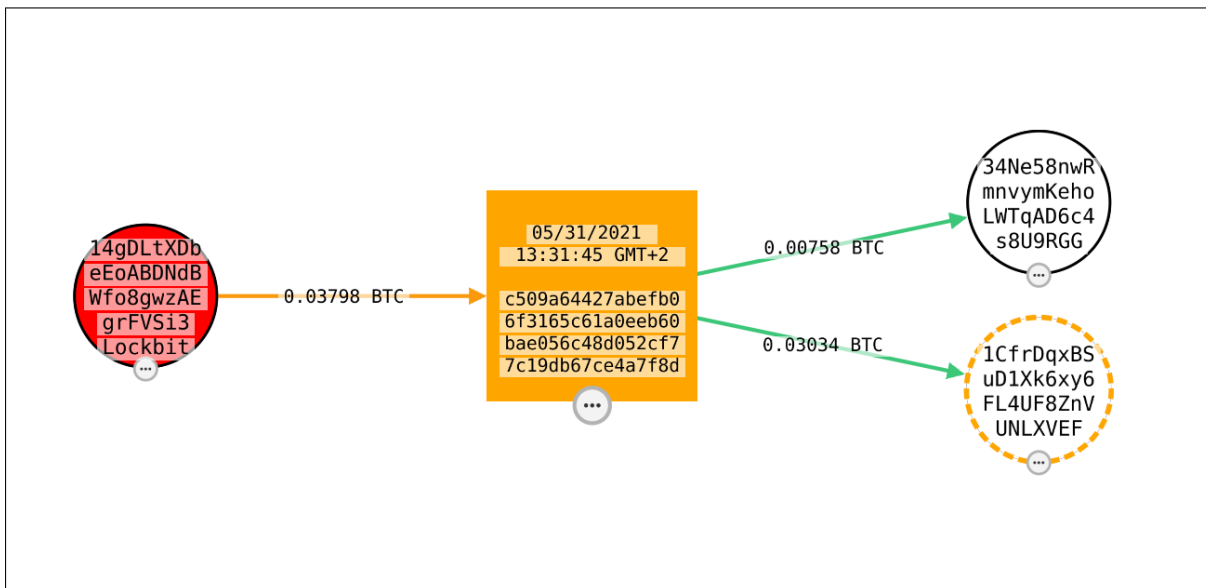


Figure 22. Most of the transactions were immediately send to mixers

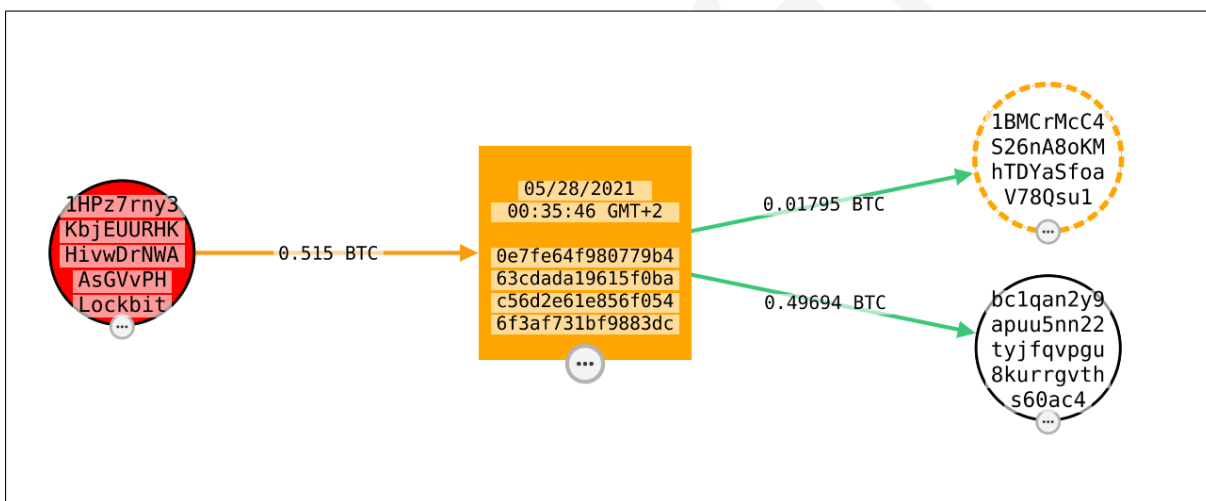


Figure 23. Another example of a transaction which is sent to a mixer

Dashed circle in yellow in Figure 22, Figure 24, Figure 25, and Figure 23 represent mixer wallet address.

We used CipherTrace [1] crypto-asset monitoring platform in order to have a clear view of the crypto transactions. However, most of the destination addresses were obscured using mixers. However, in rare instances, we could not identify any advanced medium for obfuscation. We leave this part for the authorities to conduct a thorough investigation.

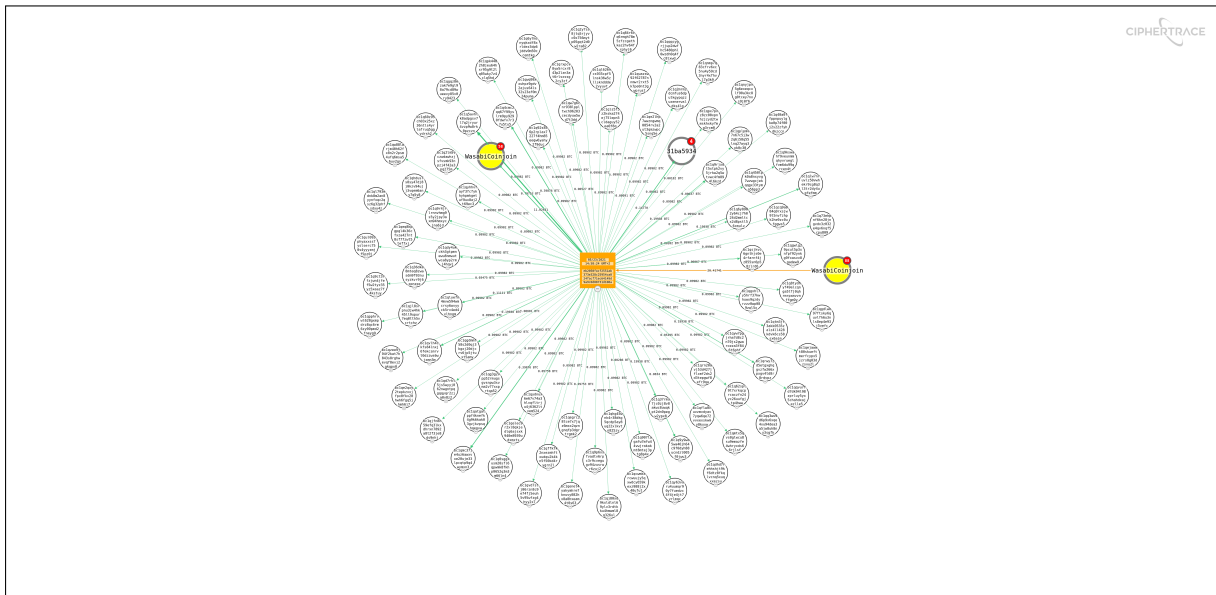


Figure 24. Wasabi CoinJoin usage - Image taken from CipherTrace

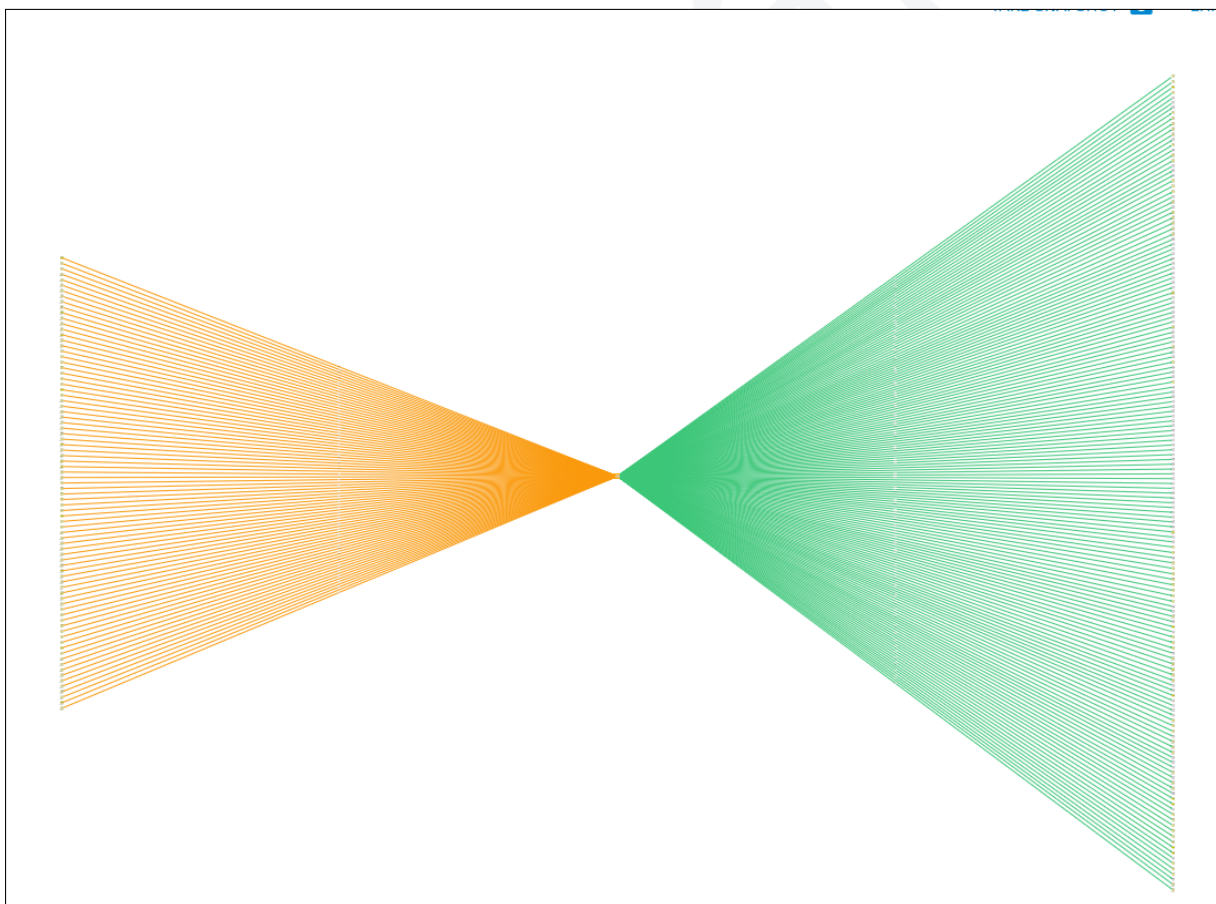


Figure 25. Wasabi CoinJoin usage - Image taken from CipherTrace

## 6 Conclusion

There is a growing body of research that recognizes the methodologies of ransomware attacks. Besides, the recent Colonial Pipeline attack showed how these attacks could be dangerous in the physical world, apart from the cyber domain. In this report, we presented the inner workings of one of the best-known ransomware group and helped many victims recover their data. However, rapid acceptance of cryptocurrencies and shifting to remote work will significantly increase these ransomware attacks in the near future. In order to disrupt the operation of cybercriminals while tackling complex challenges, public and private bodies need to work collaboratively. We believe that our research will shed light on the inner structures of the cybercriminals and help others to identify the LockBit operatives' external connections (like ReVil) as a part of a broader investigation. As we also presented in our research that some of the affiliates do not bother to decrypt the victim's files even if they were paid in full. Cybercriminals should not be trusted. We advise all potential victims not to pay any ransom and report the incident to the authorities immediately. We also advise to follow other ransomware prevention initiatives such as "The No More Ransom Project" [8] to get an up-to-date information about recent cases and decryption opportunities.

## Références

- [1] CipherTrace. *CipherTrace Cryptocurrency Risk Intelligence*. url : <https://ciphertrace.com/>. (accessed : 18.06.2021).
- [2] Comparitech. *2018-2021 Ransomware statistics and facts*. url : <https://www.comparitech.com/antivirus/ransomware-statistics/>. (accessed : 25.03.2021).
- [3] Coveware. *Most Common Ransomware Variants in Q1 2021*. url : <https://www.coveware.com/blog/ransomware-attack-vectors-shift-as-new-software-vulnerability-exploits-abound>. (accessed : 17.06.2021).
- [4] Darktrace. *LockBit ransomware analysis : Rapid detonation using a single compromised credential*. url : <https://www.darktrace.com/en/blog/lock-bit-ransomware-analysis-rapid-detonation-using-a-single-compromised-credential/>. (accessed : 17.06.2021).
- [5] Difose. *Most Popular Ransomware : CryptoLockers*. url : <https://medium.com/databulls/most-popular-ransomware-cryptolockers-378fe068598>. (accessed : 17.06.2021).
- [6] Malpedia. *Babuk Ransomware*. url : <https://malpedia.caad.fkie.fraunhofer.de/details/win.babuk>. (accessed : 17.06.2021).
- [7] nist.gov. *CVE-2018-13379*. url : <https://nvd.nist.gov/vuln/detail/CVE-2018-13379>. (accessed : 17.06.2021).
- [8] NoMoreRansom. *The No More Ransom Project*. url : <https://www.nomoreransom.org/en/index.html>. (accessed : 18.06.2021).
- [9] Owasp. *Credential Stuffing*. url : [https://owasp.org/www-community/attacks/Credential\\_stuffing](https://owasp.org/www-community/attacks/Credential_stuffing). (accessed : 17.06.2021).
- [10] Wikipedia. *REvil*. url : <https://en.wikipedia.org/wiki/REvil>. (accessed : 17.06.2021).



**Acknowledgement**

We would like to thank "Police Cantonale Vaudoise / Switzerland" and our advisors for their valuable guidance and support throughout this research.

The public version of the report will be shared from our web page <https://www.prodaft.com>. The readers can find new samples, IOCs, and new versions of our reports from our github page as we will constantly update our page based on new findings.

Unclassified

## Historique

Version	Date	Auteur(s)	Modifications
1.0	23.05.2021	PTI Team	Initial TLP:RED DRAFT release
1.1	18.06.2021	PTI Team	Initial TLP:WHITE release
1.2	18.06.2021	PTI Team	Typos fixed, affiliate list updated
1.3	19.06.2021	PTI Team	Proofread fixes done, CipherTrace reference added
1.4	19.06.2021	PTI Team	Typos fixed



PRODAFT was founded as a cyber threat intelligence company in 2012.

Aimed at creating a difference through expertise, the brand has significantly evolved thanks to its apposite technologies, all of which are developed in-house.

By looking at cyber threats from a realistic perspective, PRODAFT has always positioned itself as a "professionally unconventional" provider in its field, thanks to a suite of proprietary solutions.

PRODAFT continues to serve a range of global brands and critical industries via its threat intelligence, penetration testing and security research teams.

To ensure proactive nature of PRODAFT's solutions, our operational cycles are constantly reviewed and adapted to emerging challenges within cyber arena. Owing to this constant state of flux, PRODAFT is always prepared for the new realities and challenges of cyber security.

Our clients will never find themselves blindsided by any newly evolving cyber trend. Our commitment in this regard is the main reason behind PRODAFT's popularity among high-profile organizations.

Contact: [info@prodaft.com](mailto:info@prodaft.com)  
Address: Y-Parc, rue Galilée 7, 1400 Yverdon-les-Bains, Switzerland