

# *Dissecting the Arsenal of LockBit*

S2W, Threat Analysis Team  
HuiSeong Yang  
([gmrkd@s2w.inc](mailto:gmrkd@s2w.inc))

## Index

1. Who is LockBit?
2. LockBit's History
3. LockBit's Arsenal
4. Conclusion

# About Me

## About Me

HuiSeong Yang



**#Malware #Ransomware #RaaS #APT**  
**#ThreatActor #TTPs #CyberCrime**  
**#ThreatIntelligence #Analysis #Affiliate**  
**#Botnet #Stealer #Darkweb**

 : @gmrkd

 : HuiSeong Yang

 : gmrkd@s2w.inc

**S2W, Threat Analysis Team, Researcher**

# About Me

S2W



## TALON

### IntelOps

- **Systematize** methodology
- **Strategic intelligence**
- Leveraging **DevOps**
- **Automation** Technologies to boost threat intelligence

### BLKSMTH

- **APT** Intelligence
- **Threat Actor** tracking
- **Detailed Malware analysis**

### HOTSAUCE

- DDW Intelligence
- Open-source Intelligence
- **User profiling**
- **Cryptocurrency tracking**
- **Incident Response**

### UNREAL

- **Offensive** Research
- **Core Technology Research**

# Who is LockBit ?

# Who is LockBit?

Background

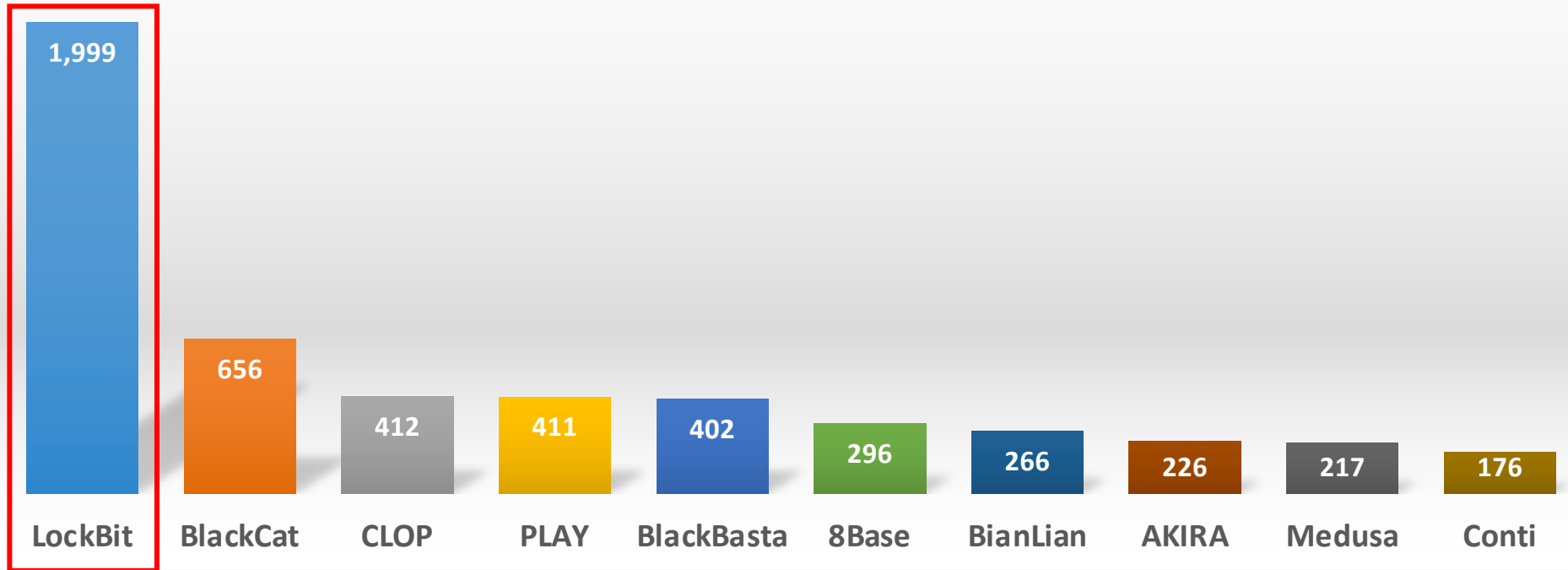


**LOCKBIT 3.0**

# Who is LockBit?

## Background

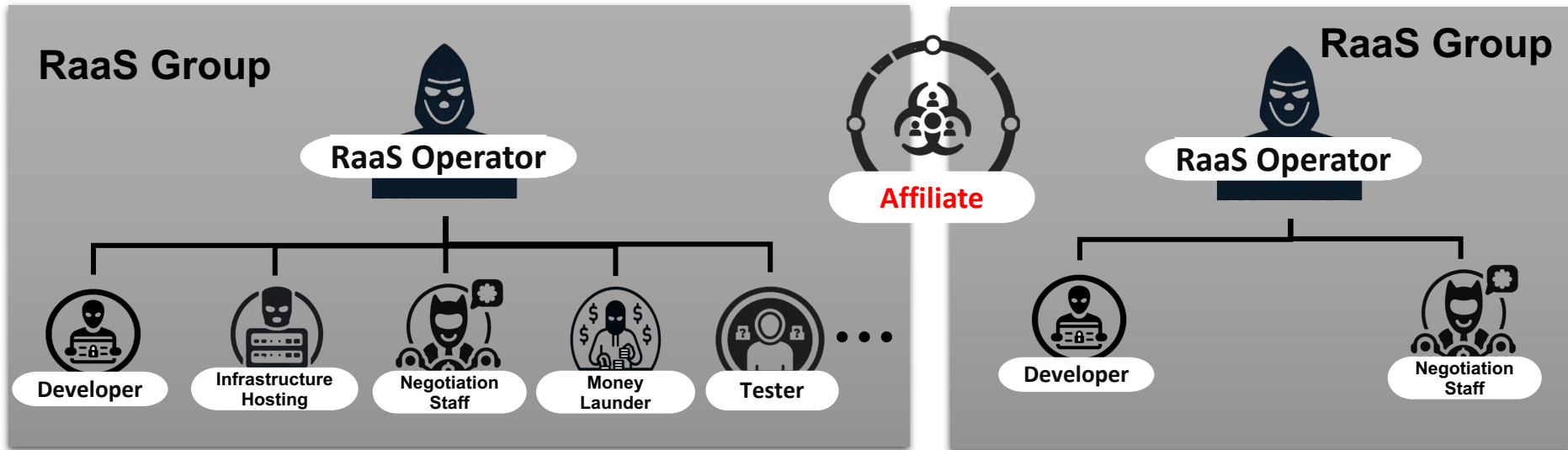
Ransomware Activity Top 10 (Jan 2022 ~ Apr 2024)





# Who is LockBit?

## Background



# Who is LockBit?

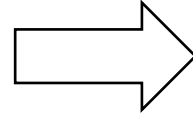
## Background

### Russian National Arrested and Charged with Conspiring to Commit LockBit Ransomware Attacks Against U.S. and Foreign Businesses



systems in the United States, Asia, Europe, and Africa.

Ruslan Magomedovich Astamirov (АСТАМИРОВ, Руслан Магомедович), 20, of Chechen Republic, will make his initial appearance later today.



or



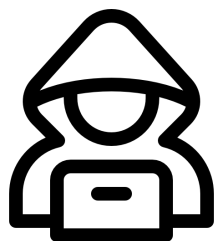
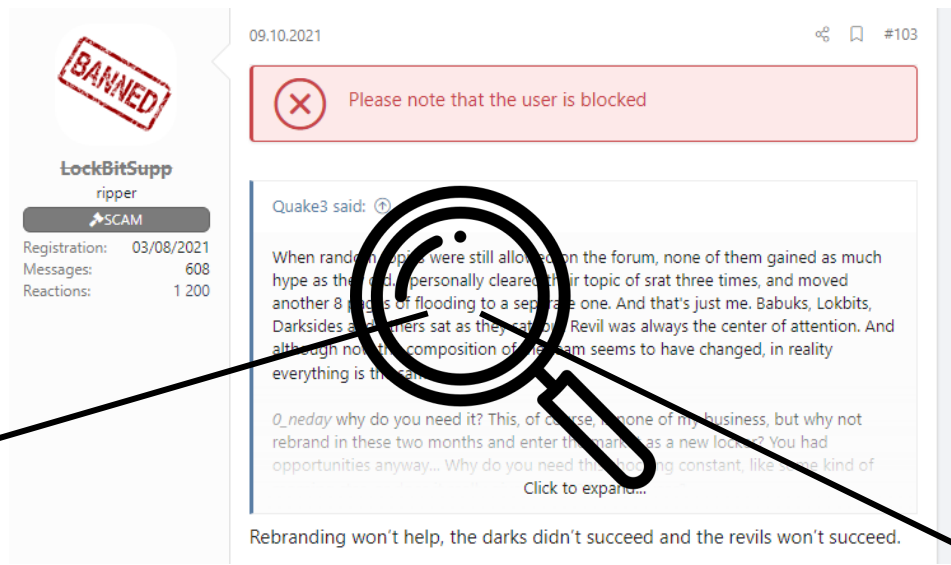
Service Stop



# Who is LockBit?

## Background

But, LockBit has never rebranded...



Forum User

**Why not rebrand in these two months and enter the market as a new locker?**

**Rebranding won't help ...**

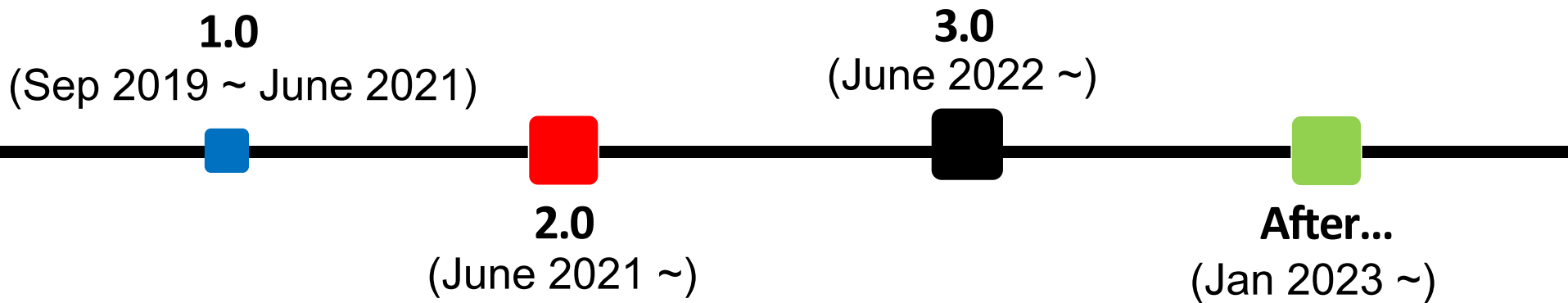


LockBitSupp

# LockBit History

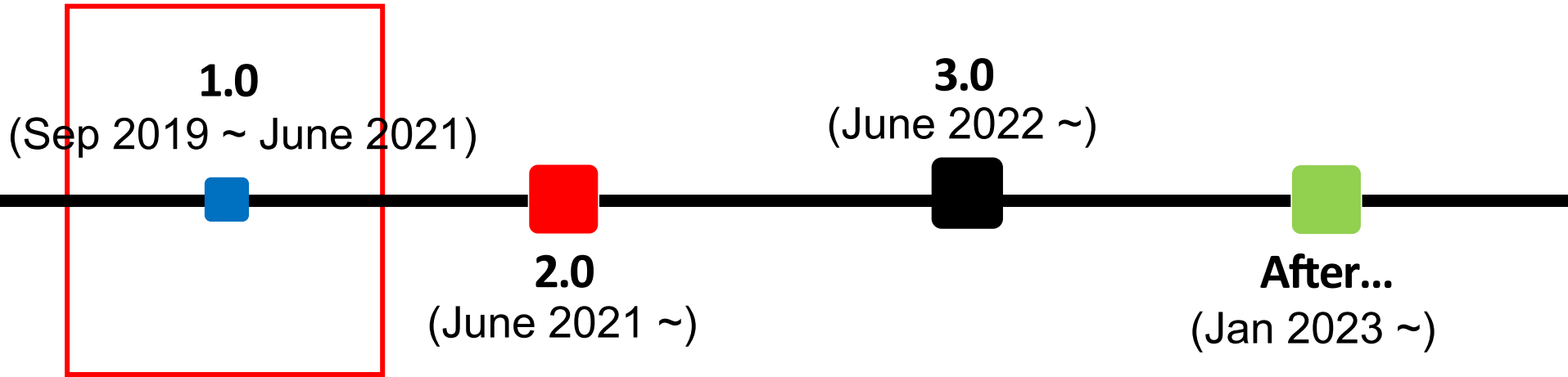
# LockBit History

Timeline



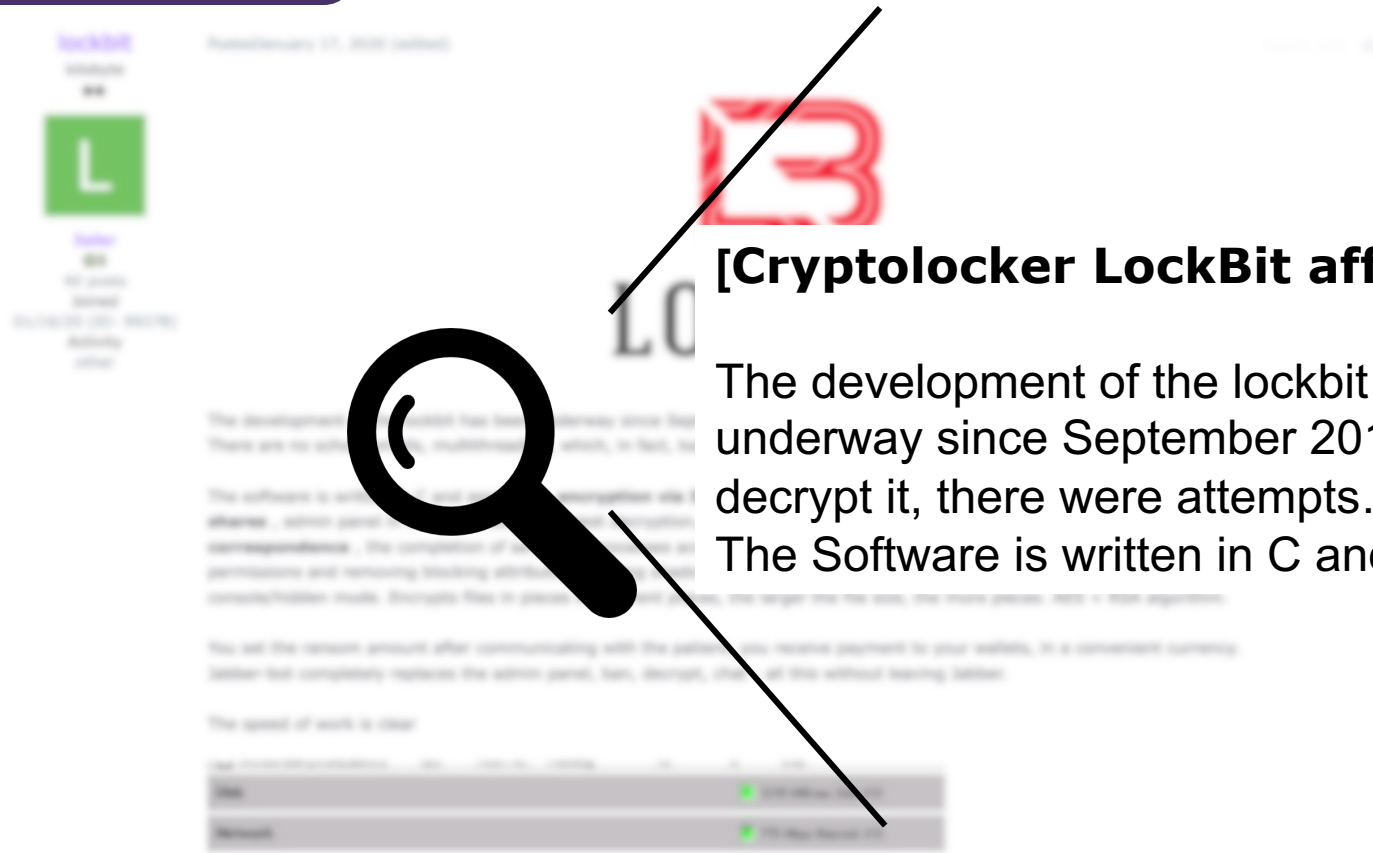
# LockBit History

Timeline



# LockBit History

1.0



## [Cryptolocker LockBit affiliate program]

The development of the lockbit has been underway since September 2019, they could not decrypt it, there were attempts...

The Software is written in C and assembler...

## Branding ABCD ransomware as LockBit

# LockBit History

1.0

I paid 20% of the ransom for the product to be stable and not break files... **It does not encrypt, but only renames files.**



Forum User posted reviews of the LockBit ransomware.



# LockBit History

1.0

The image displays three overlapping screenshots of a forum thread. The top screenshot shows a post by 'LockBit megabyte' dated September 1, 2020, discussing GDI design. The middle screenshot shows a post by 'LockBit megabyte' dated September 16, 2020, discussing AD Policy. The bottom screenshot shows a post by 'lockbit megabyte' dated September 16, 2020, discussing Native API. Red arrows point from text labels to specific underlined phrases in the posts.

**GDI design**

**AD Policy**

**Native API**

LockBit megabyte  
Posted September 1, 2020  
Report post

There is 150 lines of code that generates an image/bmp and saves it to disk.  
Task:  
By means of Gdiplus it is beautiful to design it, draw (namely, draw , and not take from the picture)  
a logo, boxes, add various effects to the text, and so on.  
A layout will be provided as an example.  
The code should work on WinXP-Win10.  
Deadline Sunday, price \$1666

lockbit megabyte  
Posted September 16, 2020  
Report post

Looking for a specialist.  
We need automation of one task for the entire domain. Active Directory Group Policies.  
The price starts from \$5k. Contact in PM.

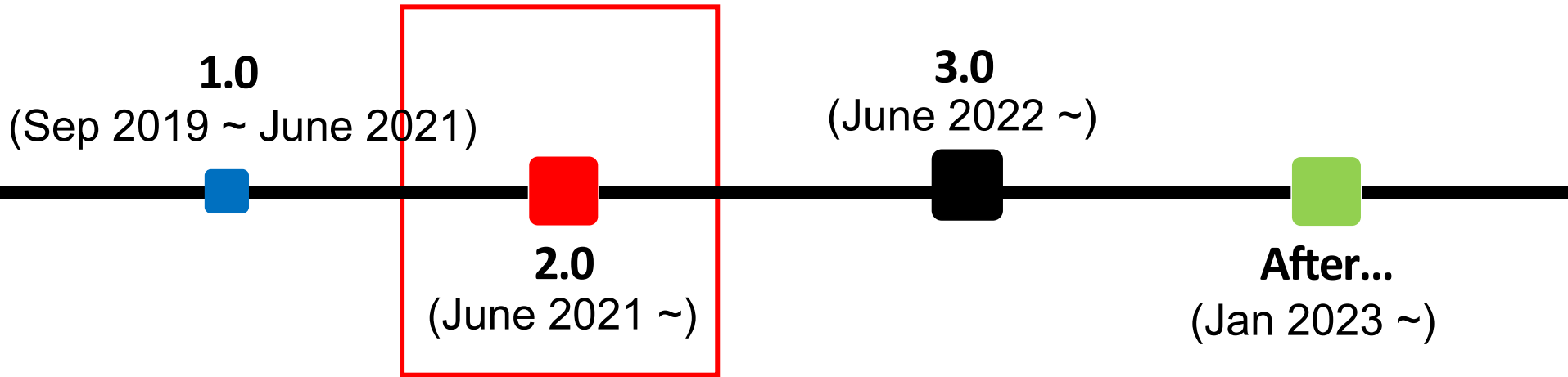
lockbit megabyte  
Posted September 16, 2020  
report post

Looking for a specialist.  
Deep knowledge of Windows system, native API. I/O termination port.  
The price starts from \$5k. Contact in PM.

Hire specialists in various fields

# LockBit History

Timeline



# LockBit History

2.0

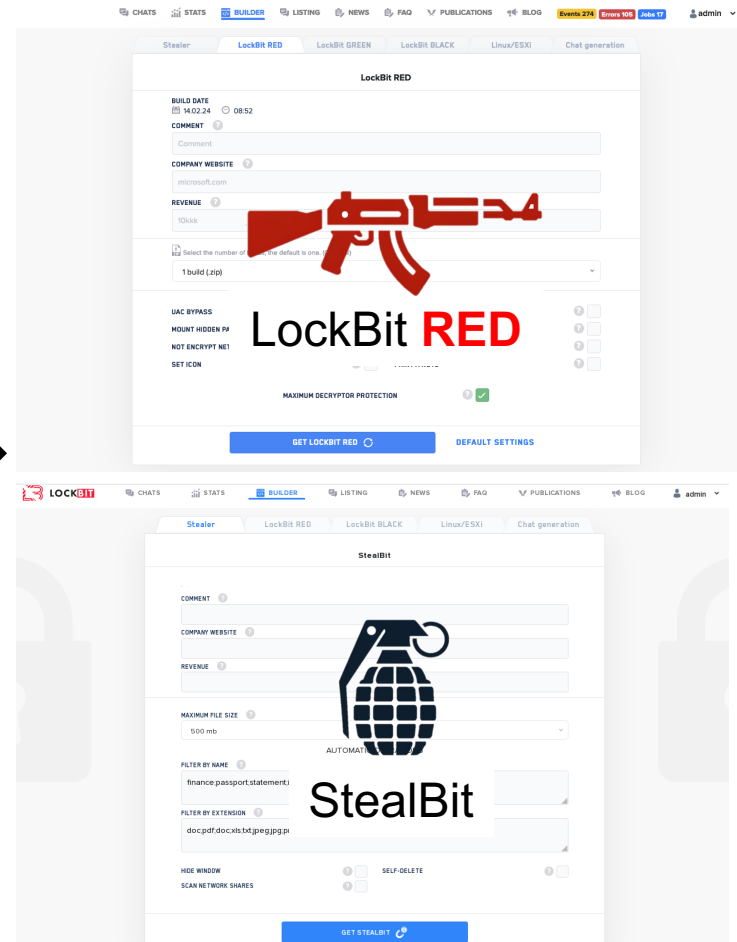
[Ransomware] LockBit 2.0 is an affiliate program.

Affiliate program LockBit 2.0 temporarily relaunch the intake of partners.

The program has been underway since September 2019, it is designed in origin C and ASM languages without any dependencies. Encryption is implemented in parts via the completion port (I/O), encryption algorithm AES + ECC. During two years none has managed to decrypt it.




## Update LockBit 2.0 !

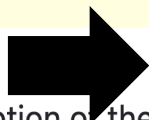


# LockBit History

2.0

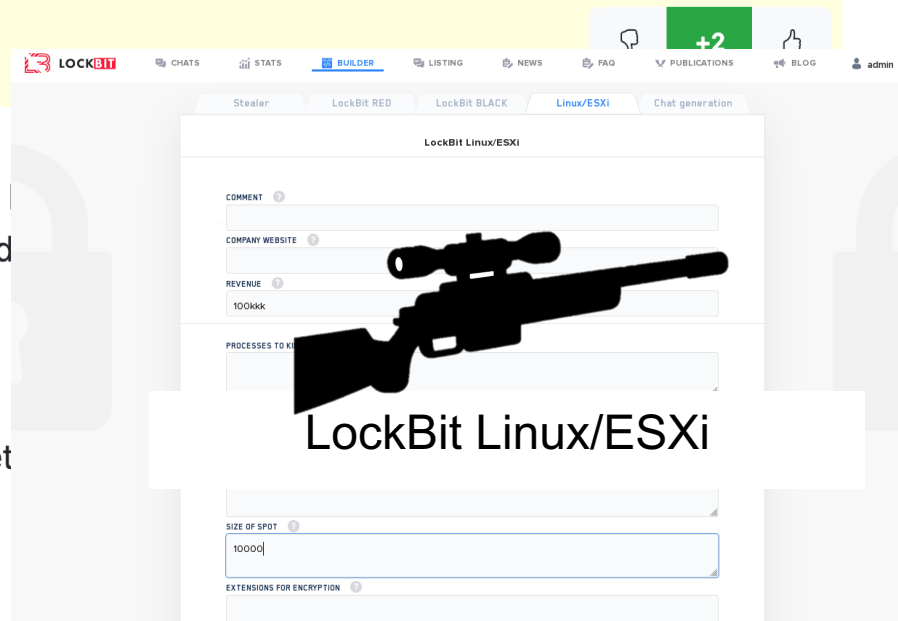
 **LockBit** October 05, 2021 at 10:57 pm  
LOCKBIT Salesman

LockBit Linux/ESXi locker V: 1.0.



The locker has 3 operating modes: encryption of the first N  
Versions of ESXi hypervisors on which the locker was tested  
Implementation language: pure C.  
Strong and proven encryption algorithm AES + ECC.  
Minimum file size for encryption: 4kb.  
Top functionality cannot be compared with competitors. Det

Answer



# LockBit History

2.0



**BlackCat  
(Ex-BlackMatter)**

**After BlackMatter shut down...**

*... Either the security guys will hack Lockbit , or they will merge their own builders. You earn millions of dollars, but you're wasting your money on coders' salaries. Shame on you all, colleagues. A shame!*

**VS**

*When you sat down a point after the ColonialPipeline and took with you several large payments from advertisers (who now work for me and know that you stupidly rebranded), **your former coder was smart enough to run over to me...***



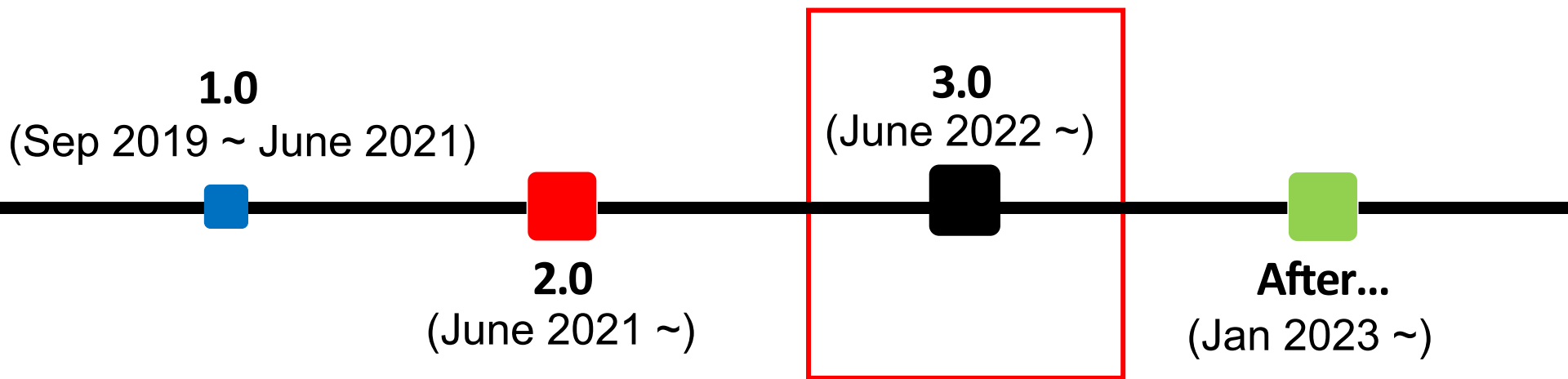
**LockBitSupp**



**BlackMatter Coder work for LockBit**

# LockBit History

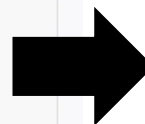
Timeline



# LockBit History

3.0

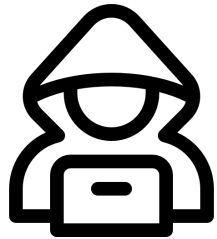
The screenshot shows the LockBit 3.0 website. At the top left is the 'LOCKBIT 3.0' logo. A red banner reads 'LEAKED DATA'. Navigation links include 'TWITTER', 'PRESS ABOUT US', 'HOW TO BUY BITCOIN', 'AFFILIATE RULES', 'CONTACT US', and 'MIRRORS'. The main heading is 'AFFILIATE RULES' in a large red box. Below it is a row of flags from various countries. The text below the flags reads: 'The oldest international [Ransomware] LockBit affiliate program welcomes you. We are located in the Netherlands, completely apolitical and only interested in money. We always have an unlimited amount of affiliates, enough space for all professionals. It does not matter what country you live in, what types of language you speak, what age you are, what religion you believe in, anyone on the planet can work with us at any time of the year. First and foremost, we're looking for cohesive and experienced teams of pentesters. In the second turn we are ready to work with access providers: sale or on a percentage of redemption, but you have to trust us completely. We provide a completely transparent process - you can control the communication with the victim. In case when the company was encrypted and has



The screenshot shows the LockBit Black interface. At the top is the 'LOCKBIT' logo and navigation links: 'CHATS', 'STATS', 'BUILDER', 'LISTING', 'NEWS', 'FAQ', 'PUBLICATIONS', 'BLOG', and 'admin'. The main heading is 'LockBit BLACK'. Below it are input fields for 'COMMENT', 'COMPANY WEBSITE', and 'REVENUE'. A section titled 'WHITE FOLDERS' contains a list of file paths: '\$recycle bin config msi', 'data.boot', 'data.boot', 'appdata.application', 'randata.system volume information', 'autorun.inf', 'font bin boot', 'desktop.inf', 'db.rmdir', 'ntuser.dat', 'ntuser.dat', 'log.rtu', 'ser', 'inthumbs', '...'. Below this is a 'WHITE FILES' section with paths: '386.adva', 'jdx.lst', 'hsk'. A 'WHITE HOSTS' section contains 'Pconnect'. A 'PROCESSES TO KILL' section contains: 'sqj', 'oracle', 'ocss4', 'dbsmnp', 'syncdme', 'agrtzvc', 'irgplussvc', 'fsvcccon', 'mydesktopservice', 'ocautoupds', 'encavc', 'firefox', 'birdconfig', 'mydesktoppos', 'occomm', 'dbeng50', 'sqbcoreservice', 'excel', 'infopath', 'msaccess', 'mspub', 'one'. A large black silhouette of an assault rifle is overlaid on the right side of the interface. The text 'LockBit Black' is written in large black font at the bottom right.

## Update LockBit 3.0 !

### After LockBit 3.0 release...



BlackMatter Coder

*"After the release, I get 10% of the money he receives from adverts for further support of the 3.0 project. The payment of these interests will occur every first day of the month, after the release."*



*"Due to low activity and online presence during the development process, I refused to pay him and offered payment through a guarantor with post-payment after the work was completed..."*

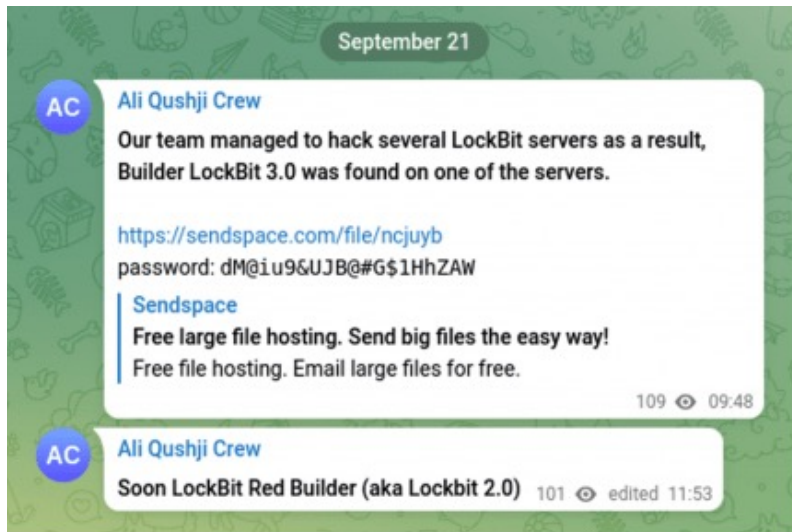


LockBitSupp



# LockBit History

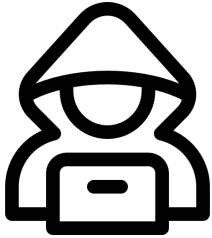
3.0



## Leaked LockBit Black Builder by BlackMatter Coder



## The original was patched and used



Forum User

*The leaked LockBit Black seems to have an **encryption flaw**.*

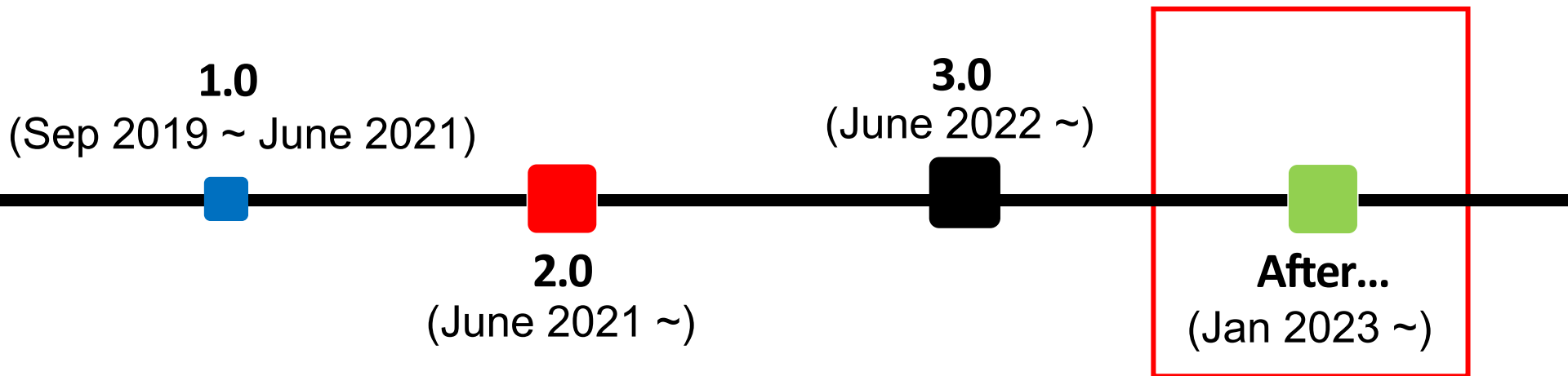
*There are no bugs in the **original**.*



LockBitSupp

# LockBit History

Timeline



# LockBit History

After...



Stealer   LockBit RED   **LockBit GREEN**   LockBit BLACK   Linux/ESXI   Chat generation

### LockBit GREEN

**BUILD DATE**  
📅 15.08.23 ⌚ 08:26

**COMMENT** ⓘ  
test

**COMPANY WEBSITE** ⓘ  
test.com

**REVENUE** ⓘ  
11kk

📄 Select the number of builds, the default is one. (Optional)   Select encryption size

1 build (.zip)   [dropdown]

## LockBit Green

**RUNNING ONE** ⓘ

**QUIET MODE** ⓘ  **NETWORK SHARES** ⓘ

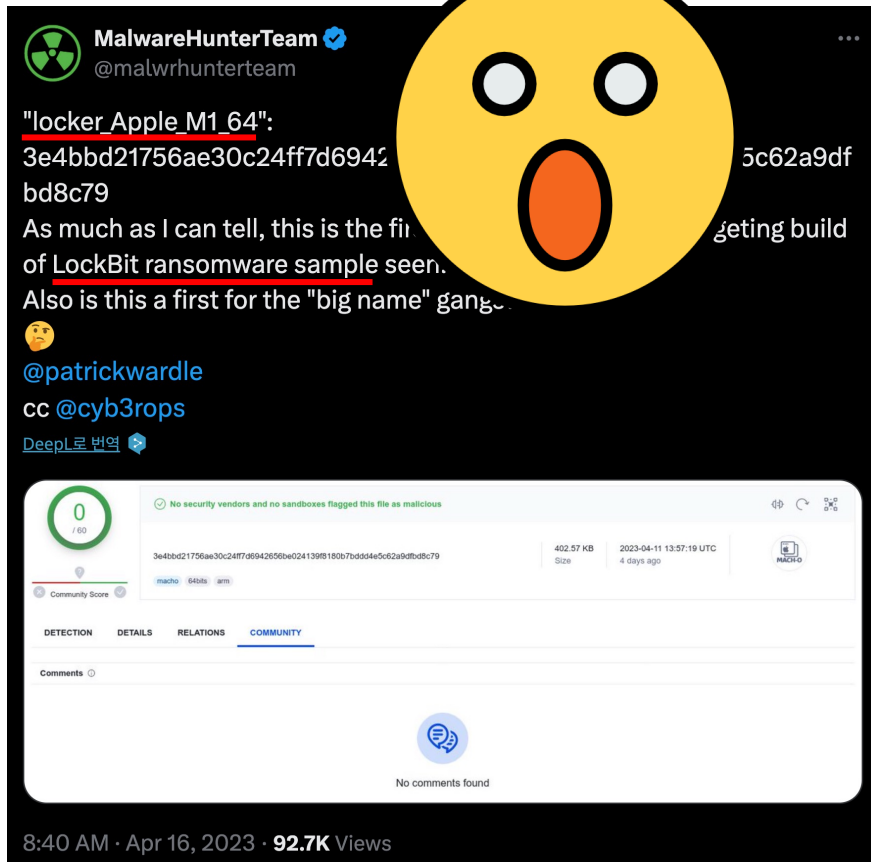
**SAME ENCRYPTION KEY** ⓘ  **MAXIMUM DECRYPTOR PROTECTION** ⓘ

[GET LOCKBIT GREEN](#) ⓘ   [DEFAULT SETTINGS](#)

# LockBit History

After...

## LockBit MacOS version?



**MalwareHunterTeam** @malwrhunterteam

"locker\_Apple\_M1\_64":  
3e4bbd21756ae30c24ff7d6942...5c62a9df  
bd8c79

As much as I can tell, this is the file... getting build  
of LockBit ransomware sample seen.  
Also is this a first for the "big name" gang...  
🤔

@patrickwardle  
cc @cyb3rops  
[DeepL로 번역](#)

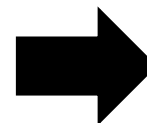
**File Details:**  
No security vendors and no sandboxes flagged this file as malicious  
3e4bbd21756ae30c24ff7d6942e56be0241398150b7b0554e5c62a9dfbd8c79  
402.57 KB Size | 2023-04-11 13:57:19 UTC | 4 days ago

**COMMUNITY**

Comments 0

No comments found

8:40 AM · Apr 16, 2023 · 92.7K Views



LockBit MacOS

## LockBit History

After...



# LockBit History

After...

## Operation CRONOS



Seized  
Infrastructures

LockBit data  
published




Infrastructures seized  
again

Additional LockBit data  
disclosures






## How did the operation occur?

 2024-02-19

smelly\_\_vx your website is seized?!?!

LockBit +

smelly\_\_vx что случилось???

LockBit FBI pwned me  **CVE-2023-3824**

smelly\_\_vx .....

# LockBit History

After...

**LOCKBIT 3.0**

**LEAKED DATA**

**THIS SITE IS NOW UNDER THE CONTROL OF THE UK, THE US AND THE CRONOS TASK FORCE**

**NCA** National Crime Agency

**FEDERAL BUREAU OF INVESTIGATION**

**EUROPOL**

**Press Releases**  
PUBLISHED  
Updated: 01 Feb, 2024, 04:12 UTC 3947

**LB Backend Leaks**  
PUBLISHED  
Updated: 31 Jan, 2024, 01:44 UTC 1182

**Lockbitsupp**  
PUBLISHED  
Updated: 31 Jan, 2024, 01:44 UTC 1182

**Who is LockbitSupp?**  
EXTENDED  
PUBLISHED  
Updated: 01 Feb, 2024, 04:12 UTC 31337

**You've Been Banned From LOCKBIT 3.0**

**The \$10m question**

# LockBit History

After...

## Operation CRONOS (First)

The screenshot shows a code editor with a sidebar on the left listing folders: root, home, www, blog, ajax, api, blocks, exceptions, includes, and migrations. The main editor window displays the file db\_prod.php with the following code:

```
1 |
2 | <?php
3 | const DB_HOST = 'localhost';
4 |
5 |
6 |
7 |
8 | const BLOG_API_KEY = '
9 | const BACKEND_API_KEY = '
10 |
11 | const BLOG_CLONE_API_URL = 'http://
12 | const BLOG_CLONE_API_KEY = '
13 |
14 | define('FOLDER_PATH', realpath("/mnt/virtual/good_files") . '/');
```

A white callout box with the text "LockBit Backend Data" is overlaid on the code, pointing to the API key and URL constants.

The screenshot shows a terminal window with the following output:

```
id:1 admin created_at:2022-01-31 22:20:43
id:2 Harold created_at:2022-06-25 12:31:59
id:3 Beverley created_at:2022-06-25 12:35:17
id:4 Jaye
id:5 Finn
id:6 Astor
id:7 Maxim
id:8 Denis
id:9 John created_at:2022-06-25 12:37:07
id:10 Kelsie created_at:2022-06-25 12:37:18
id:11 Ramsey created_at:2022-06-25 12:37:33
```

A white callout box with the text "Affiliate Username & Create Time" is overlaid on the terminal output, pointing to the columns of the data.

# LockBit History

After...

## Operation CRONOS (Second)

# REWARD

OF UP TO

## \$10,000,000 USD

FOR INFORMATION LEADING TO THE ARREST AND/OR CONVICTION OF  
LOCKBIT RANSOMWARE VARIANT ADMINISTRATOR

### DMITRY YURYEVIKH KHOROSHEV

FOR VIOLATIONS INCLUDING THE COMPUTER FRAUD AND ABUSE ACT

Submit tips to FBI via:

Signal: @FBISupp.01

Telegram: @LockbitRewards

Email: fbisupp@fbi.gov

TOX: 80B98577F0541160C7458464E4  
2C9A8782B036682FAD59D5F22  
8EA758F71691BE68A8E08BD55

STATE.GOV FBI.GOV

National Crime Agency

## Operation Cronos Affiliate ID and usernames

---

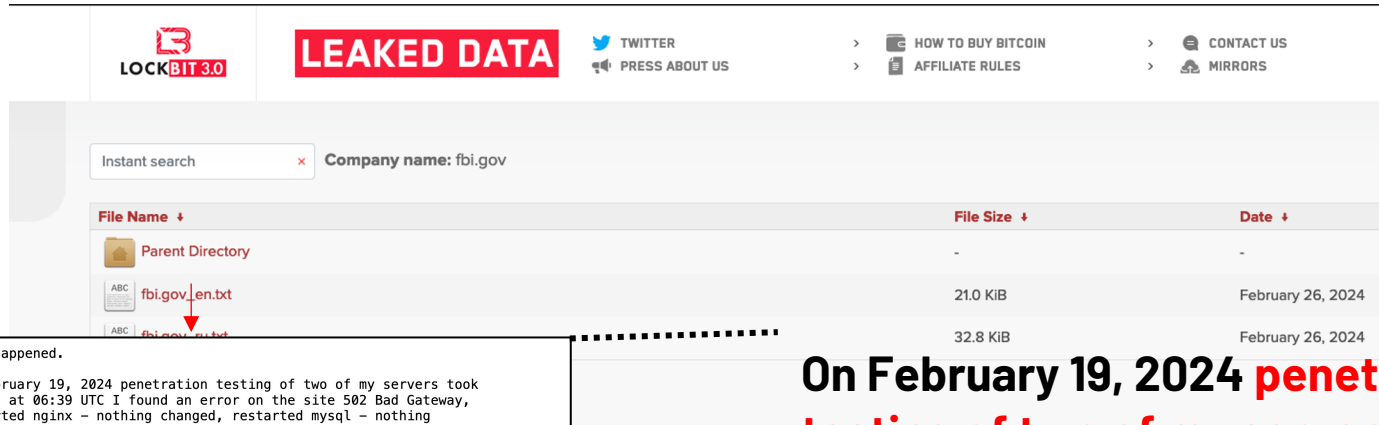
User ID

login

**\*\*NEW\*\* since Feb 24  
Now with surnames!**

1	admin	70	Dwayne	139	Hutton	1	admin
2	Harold	71	Dustin	140	uluulu	2	Terry Ryan
3	Beverley	72	Jody	141	Norman	3	Richard Campbell
4	Jaye	73	Frankie	142	Terrell	4	Steven Vega
5	Finn	74	Aric	143	Powerful	5	William Guzman
6	Aston	75	Vinnie	144	Billie	6	David Ramsey
7	Maximus	76	Bradly	145	Corrie	7	Michael Phillips
8	Denise	77	Kurt	146	Raleigh	8	Phillip Watson
9	John	78	Wynne	147	Marley	9	Howard Collins
10	Kelsie	79	Kameron	148	Darwin	10	Russell Price
11	Ramsey	80	Godfrey	149	Russel	11	Kenneth Nelson
12	Vern	81	Rawley	150	Daron	12	Glen Ortega
13	Mayer	82	Quinnton	151	Zohan	13	Ramon Keller
14	Devyn	83	Brett	152	Weldon	14	Nathan Davis
15	Burton	84	Torey	153	Chris	15	Kelly Bryant
16	Ardell	85	Ronal	154	Reinhold	16	William Brown
17	Harley	86	Dayton	155	Roscoe	17	Robert Hansen
18	Chad	87	Niko	156	Kelton	18	Nicholas Walker
19	Truman	88	Nicholas	157	Bretton	19	Nicholas Holland
20	Ranzi	89	Mickey	158	Burdette	20	Douglas Baker

## What LockBit Did After Operation CRONOS?



What happened.

On February 19, 2024 penetration testing of two of my servers took place, at 06:39 UTC I found an error on the site 502 Bad Gateway, restarted nginx – nothing changed, restarted mysql – nothing changed, restarted PHP – the site worked. I didn't pay much attention to it, because for 5 years of swimming in money I became very lazy, and continued to ride on a yacht with titsy girls. At

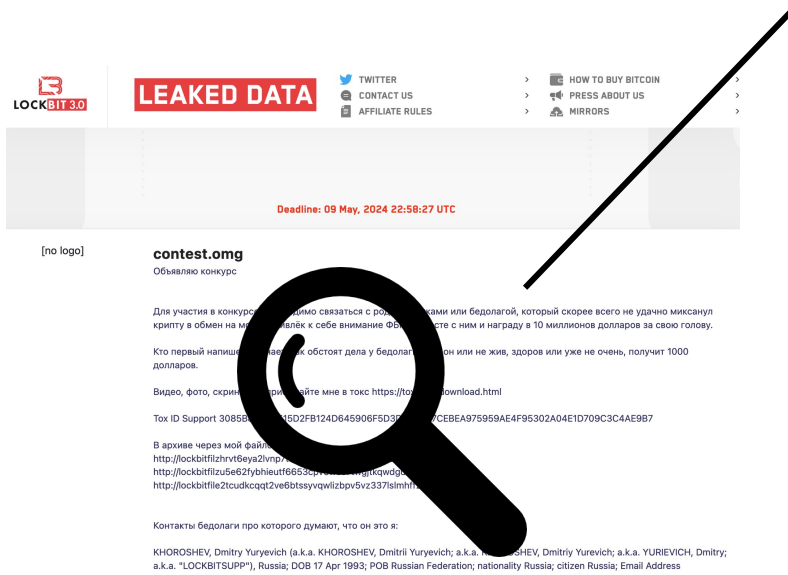
### LockBit's Statement

Due to my personal negligence and irresponsibility I relaxed and did not update PHP in time, the servers had PHP 8.1.2 version installed, which was successfully penetration tested most likely by this CVE <https://www.cvedetails.com/cve/CVE-2023-3824/>, as a result of which access was gained to the two main servers where this version of PHP was installed. I realize that it may not have been this CVE, but something else like 0day for PHP, but I can't be 100% sure, because the version installed on my servers was already known to have a

**On February 19, 2024 penetration testing of two of my servers took place...**

**... I relaxed and did not update PHP in time, the servers had PHP 8.1.2 version installed, which was successfully penetration tested ...**

### What LockBit Did After Operation CRONOS?



Whoever is the first to write and find out how the **poor guy** is doing, whether he's alive or not, healthy or not so healthy anymore, will get **1000 dollars**.

### Find the Dmitri Contest !

### What LockBit Did After Operation CRONOS?

#### TOX Status-Updates

**LockBitSupp**: The FBI is bluffing, **I m not Dimon**, I feel sorry for the real Dimon ))) oh and he will get pussy for my sins )))

**LockBitSupp**: Can you figure out how to prove that **I'm not a Dimon?** How can we show the whole world that the FBI made a mistake or deliberately framed a Dimon?

## In Operation CRONOS...



### Trend Micro

Lockbit has regularly been seen right at the very top of the ransomware ecosystem when it came to number of data leaks per month, and impact on the internet overall. But beneath that seemingly successful outward persona, the groups have had notable issues and difficulties in recent times – reaching across all aspects of their criminal enterprise. They also have not had a major updated version of their core flagship ransomware suite in over a year – giving their competitors a chance to step up with more innovative solutions.

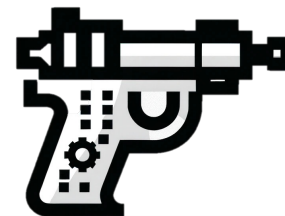
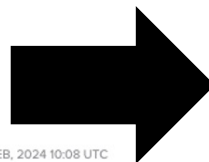
In this publication by Trend Micro researchers, we discuss the history of the group, and show evidence that it has not all gone as smoothly as it may appear on the surface. Working in collaboration with the NCA, we will also publish for the first time a detailed technical analysis of what we believe was a next potential platform agnostic rewrite of the Lockbit code, which we track as Lockbit-NG-Dev. Over the publication we show that while successful, it is not without its internal issues, and that no criminal group is too big to fail.

Links:

- <https://research.trendmicro.com/lockbit-blog>

UPLOADED: 26 JAN, 2024 13:21 UTC

UPDATED: 07 FEB, 2024 10:08 UTC



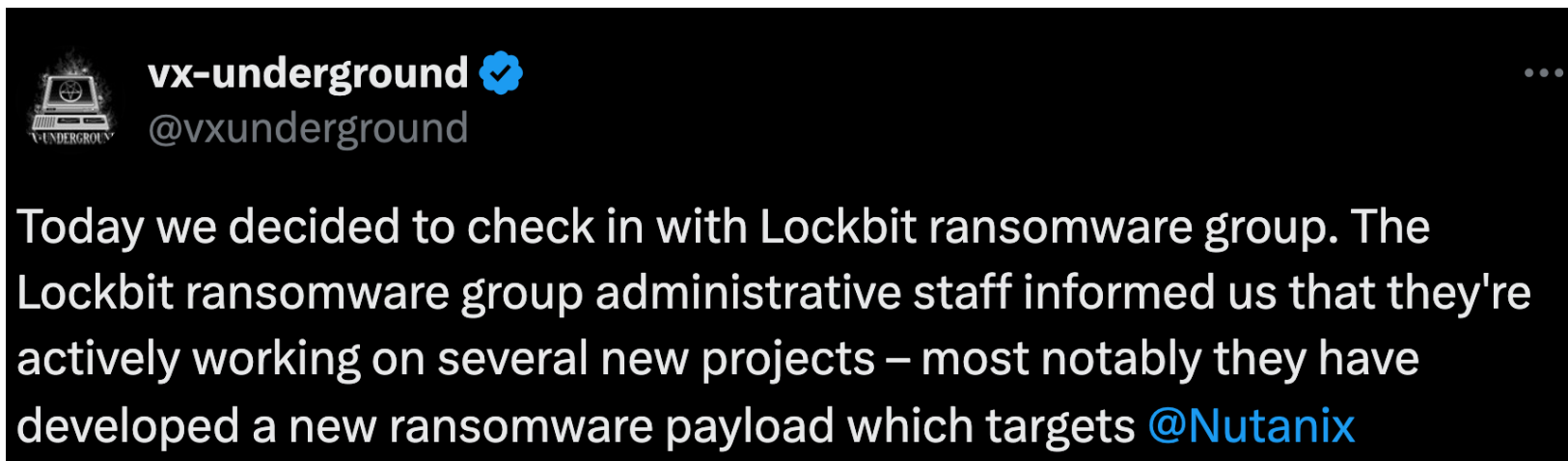
LockBit-NG-Dev



# LockBit History

After...

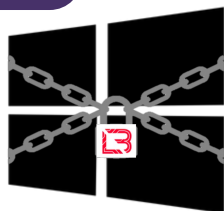
## New payload targeting nutanix environment



# LockBit's Arsenal

# LockBit's Arsenal

Arsenal



LockBit **RED**



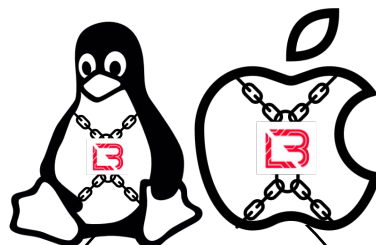
LockBit **Black**



LockBit **Green**



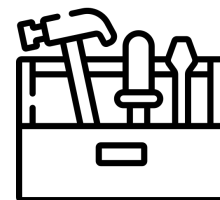
LockBit-NG-Dev



LockBit Linux/ESXi



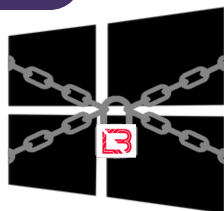
LockBit MacOS



StealBit

# LockBit's Arsenal

Arsenal



LockBit **RED**



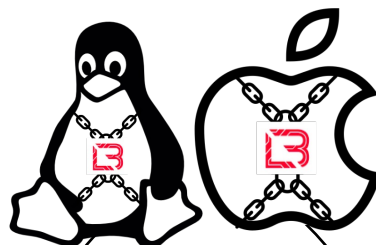
LockBit **Black**



LockBit **Green**



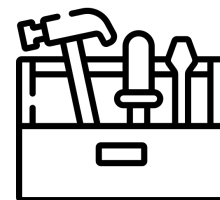
LockBit-NG-Dev



LockBit Linux/ESXi



LockBit MacOS



StealBit

# LockBit's Arsenal

## LockBit RED

	LockBit	LockBit RED	LockBit BLACK	LockBit GREEN	
Basic Feature	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>			
API Resolving		FNV1a			
Printing Bomb			<input checked="" type="checkbox"/>		
Self-Spread (GPO)			<input checked="" type="checkbox"/>		

Adding features from legacy LockBit

# LockBit's Arsenal

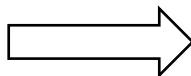
LockBit RED

## Update wallpaper via GDI



Legacy LockBit  
(LockBit 1.0)

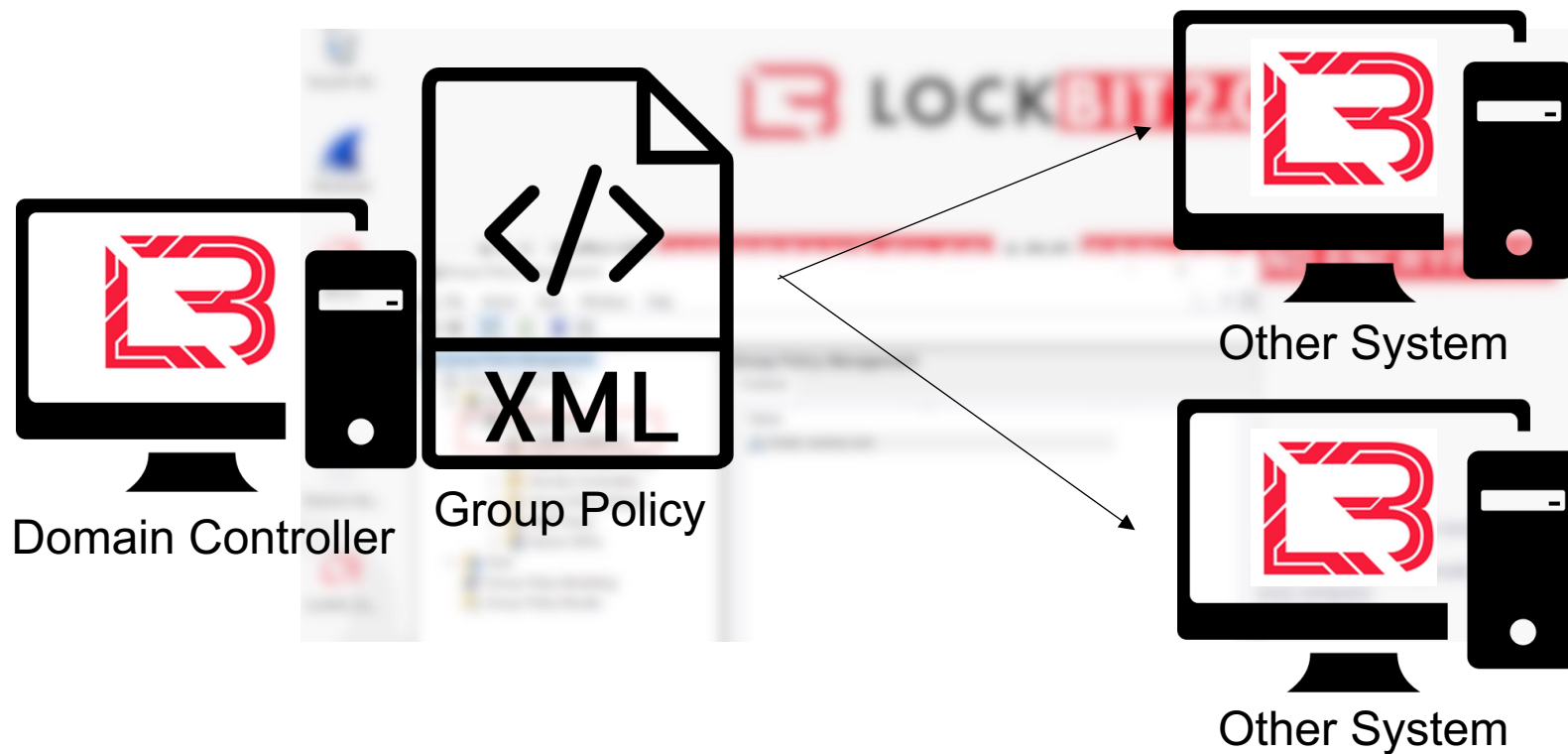
Change Layout



LockBit RED

Would you like to earn millions of dollars?  
Our company acquire access to networks of carious companies,  
as well as **insider information** that can help you steal the most  
valuable data of any company

### Add self-spreading to AD environment



# LockBit's Arsenal

LockBit **RED**

## Added Printing Bomb

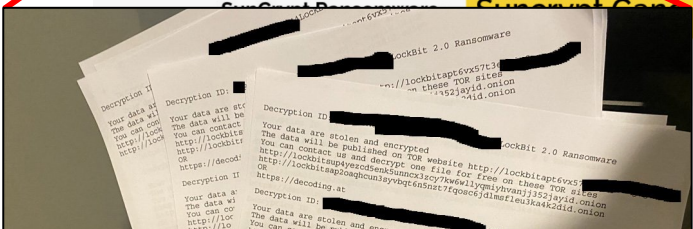
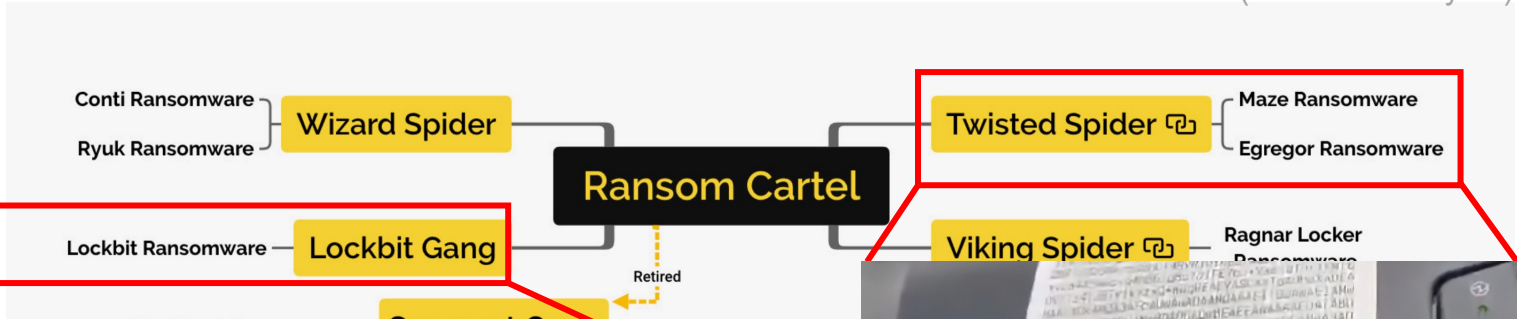




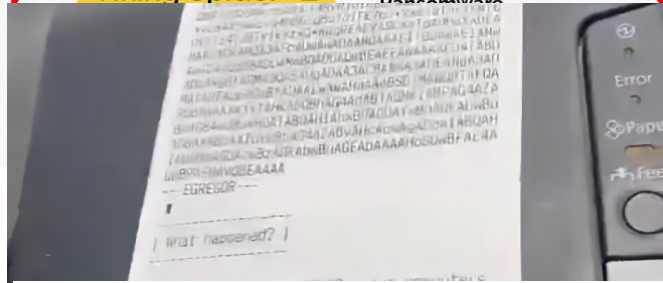
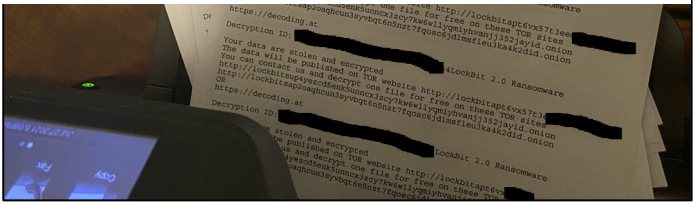
# LockBit's Arsenal

## LockBit RED

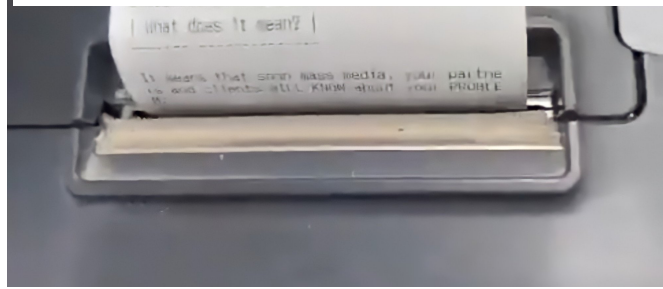
(Sources: analyst1)



### LockBit RED



### Egregor

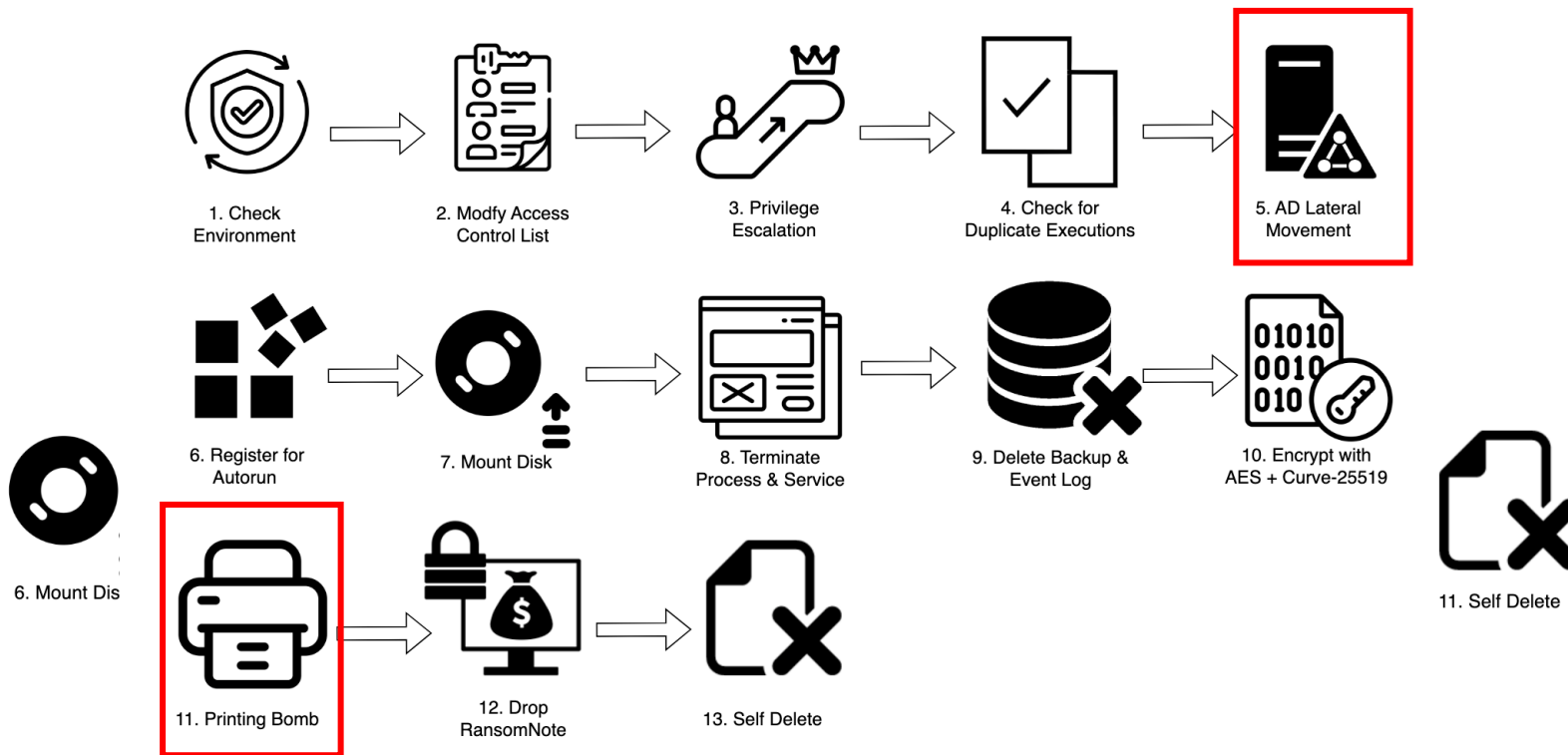


# LockBit's Arsenal

## LockBit RED

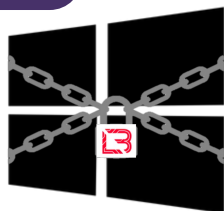


## LOCKBIT 2.0



# LockBit's Arsenal

Arsenal



LockBit **RED**



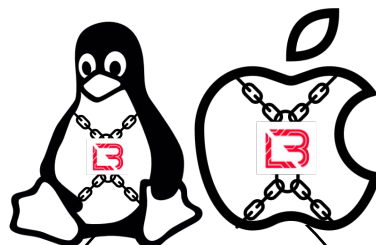
LockBit **Black**



LockBit **Green**



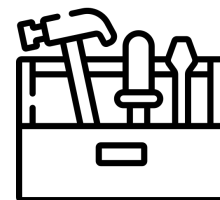
LockBit-NG-Dev



LockBit Linux/ESXi










LockBit MacOS



StealBit

# LockBit's Arsenal

## LockBit Black

	LockBit	LockBit RED	LockBit BLACK	LockBit GREEN	LockBit-NG-Dev
Basic Feature		Based on LockBit	Based on BlackMatter		
API Resolving		<b>FNV1a</b>	<b>RoR13 + XOR</b>		
Printing Bomb					
Self-Spread (GPO)					
Encrypted Memory					
Password Guardrail					

} Security ↑

# LockBit's Arsenal

## LockBit Black

### Features added in LockBit Black

```
if ( Connect_DC_sub_453860(LDAP, v53, v55, v46, &v52) )// Connect to GPOs with LDAP
{
  if ( Set_Attribute_sub_450480(v52) ) // Setting Attributes ( gPCMachineExtensionName, gPCUserExtensionName )
  {
    if ( GPTINI_write_sub_44FA70(LDAP) ) // GPO path\\GPT.INI File Update ( Version, displayName )
    {
      XML_Write_Networkshare_setting_sub_44D8D0(LDAP);// GPO Path\\Preferences\\NetworkShares\\NetworkShares.xml File Update
      if ( XML_Write_Services_stop_sub_44C150(LDAP) )// GPO Path\\Preferences\\Services\\Services.xml File Update
      {
```

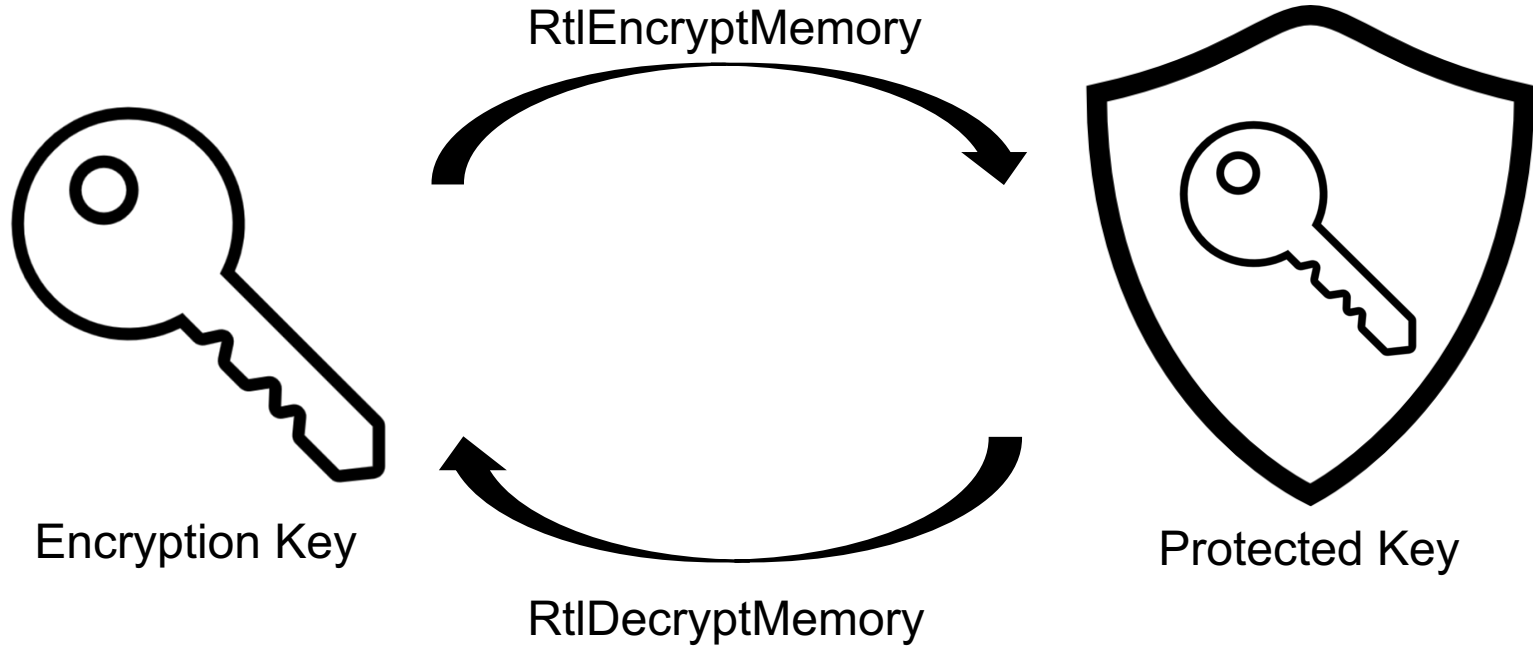
LockBit **RED**



```
&& Connect_DC_sub_417C44(v6, v4, a1, &v5)// Connect to GPOs with LDAP
&& Set_Attribute_sub_417848(v5) // Setting Attributes ( gPCMachineExtensionName, gPCUserExtensionName )
&& GPTINI_write_sub_416780(v6) // GPO path\\GPT.INI File Update ( Version, displayName )
&& XML_Write_NetworkShare_setting_sub_4175A4(v6)// GPO Path\\Preferences\\NetworkShares\\NetworkShares.xml File Update
&& StopDefender_RegistryPool_commentcmtx_write_sub_4172D4(v6)
&& XML_Write_Services_stop_sub_416970(v6)// GPO Path\\Preferences\\Services\\Services.xml File Update
&& XML_Write_File_Scheduletask_sub_416C00(v6, a1, v4) )
{
```

LockBit **Black**

### Features added in LockBit Black



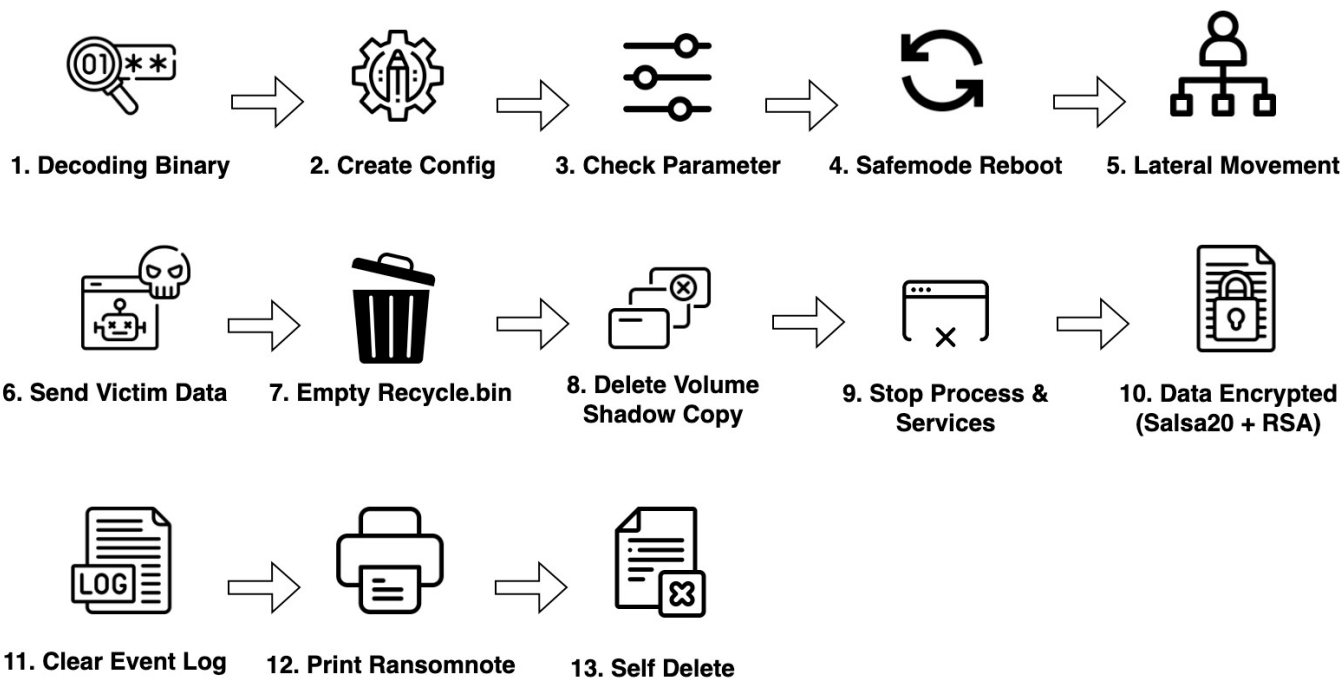
### Features added in LockBit Black

Parameter	Comment
-path	Encrypt only the path given as a parameter
<b>-pass</b>	Keystrokes required to execute the ransomware
-safe	Reboot to safe mode
-wall	Change wallpaper
<b>-gspd</b>	Lateral Movement in AD environment (GPO)
<b>-psex</b>	Lateral Movement in network share
<b>-del</b>	Self Delete
<b>-gdel</b>	Remove Group Policy

# LockBit's Arsenal

## LockBit Black

# LOCKBIT 3.0

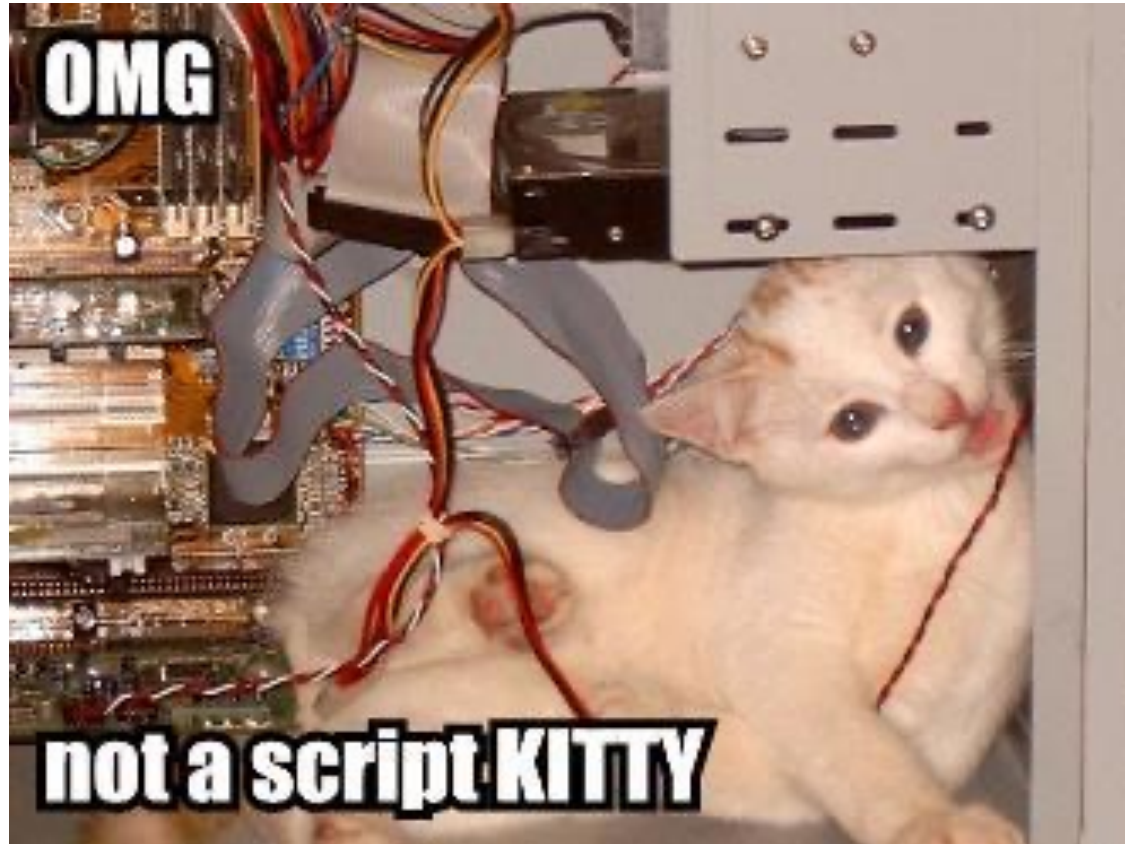




# LockBit's Arsenal

## LockBit Black

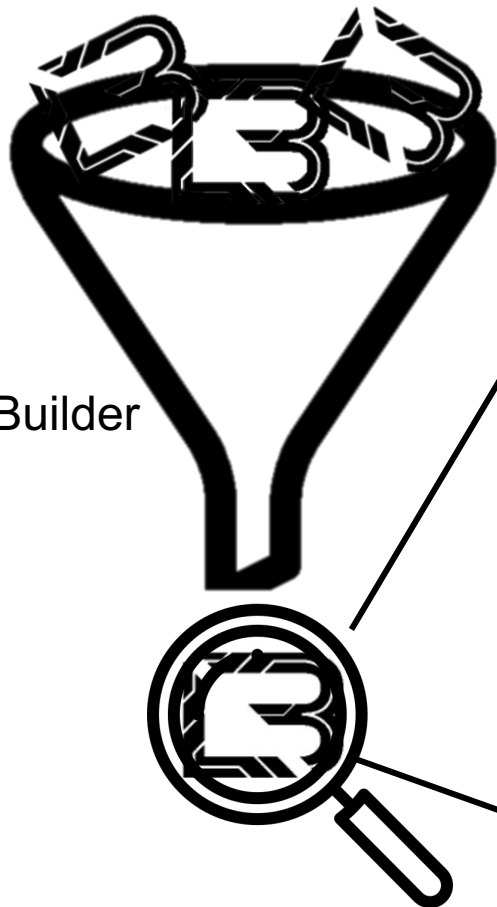
### Who uses Leaked LockBit Black Builder?



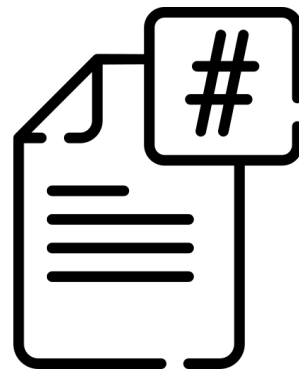
# LockBit's Arsenal

## LockBit Black

Leaked Builder



TimeStamp



Section Hash

# LockBit's Arsenal

LockBit Black

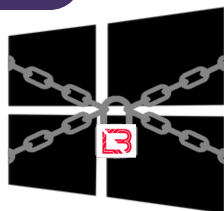
## Same value created with the leaked builder

—— @protonleaks  
—— @ali\_qushji

<b>(EXE)</b>		
TimeStamp	2022-09-09 01:27:01 UTC	2022-09-1 23:30:57 UTC
Section MD5 Hash (.text)	cfbda2c44e51b3b0b00bcbbc767c62a2	57ad8095d0d1b2e0663fbd3ef4405410
Section MD5 Hash (.itext)	6f4cd57381bb5584c0a0755384d25180	0adcc204eb91a7bbe4f95e6c65202fe1
Section MD5 Hash (.rdata)	bd829aa493ecd52fe5bec776d207f206	9264ea7f335858b063b39397d3c51d14
Section MD5 Hash (.reloc)	3f87e4c23650dfad0bee7da98889ba94	68a4352eca889669f544bd64baa3f961
<b>(DLL)</b>		
TimeStamp	2022-09-09 01:27:08 UTC	2022-09-13 23:31:03 UTC
Section MD5 Hash (.text)	f8ab18e0bfbd0004a80bcebcf532343a	25daf073d97d73bb80d8914fdbbc28e1a
Section MD5 Hash (.itext)	cd4af6ba5a134688efd0ac2ec0d14db4	dd0955a2f9ce023b0f38d8364083634a
Section MD5 Hash (.rdata)	27a341926a3ac1f0ec9362037fe96453	eb51a9196a386b2a314f42f823a6affd
Section MD5 Hash (.reloc)	36e3dfe630cbdf2fc5b330e9d27cc6dd	331d3773bf65049a3d59a6e22111815f
<b>(Reflective DLL)</b>		
TimeStamp	2022-09-09 01:26:27 UTC	2022-09-13 23:31:10 UTC
Section MD5 Hash (.text)	82dab83476a4f0d8d45c2b7888f7d400	9580c791df2e6fb2d69380d24bfa7a42
Section MD5 Hash (.itext)	4f07d3a1da418dc00ee94ade03d8f897	69ce49de89357d50159262cb1e3f509c
Section MD5 Hash (.reloc)	45eafaa8681394b9fb50e447d793710f	49d290bb6d3a8651b266c5b81e78c897

# LockBit's Arsenal

Arsenal



LockBit **RED**



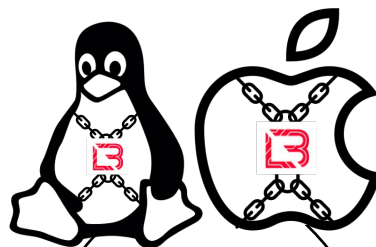
LockBit **Black**



LockBit **Green**



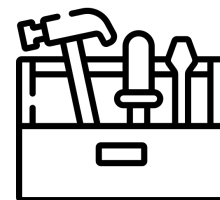
LockBit-NG-Dev



LockBit Linux/ESXi



LockBit MacOS



StealBit

# LockBit's Arsenal

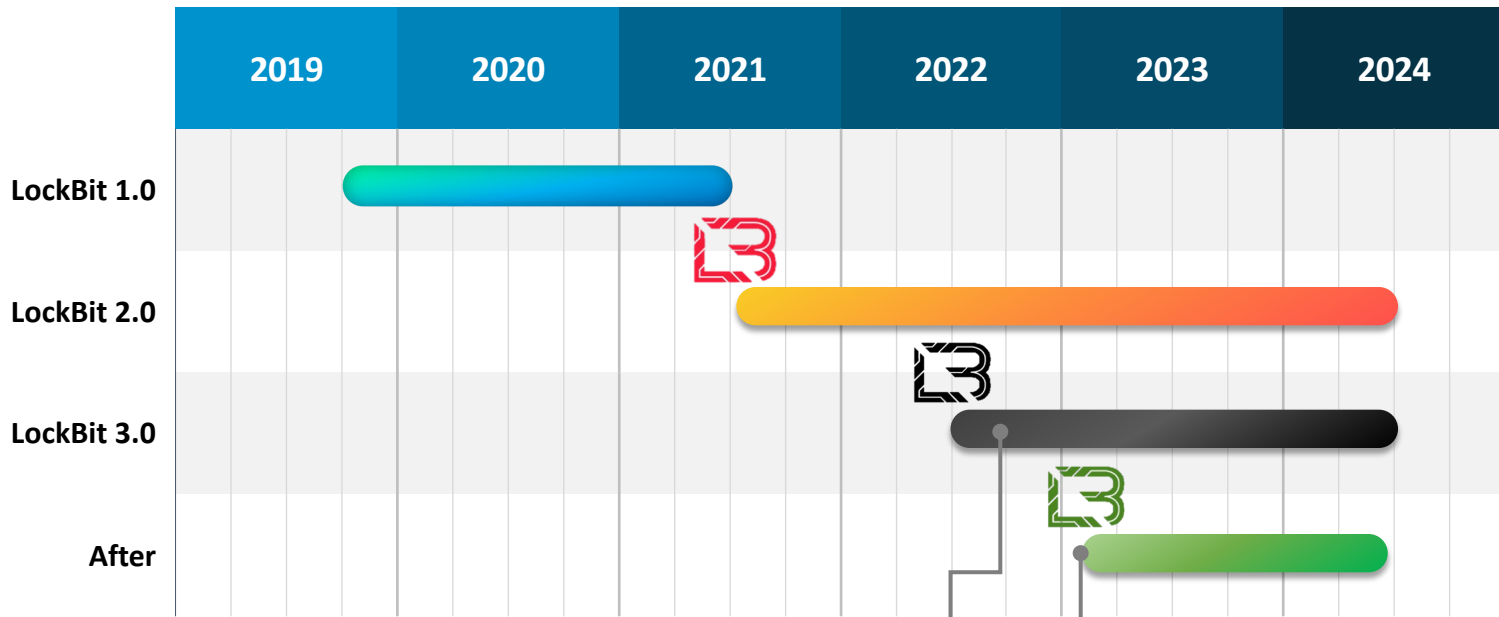
## LockBit Green

	LockBit	LockBit RED	LockBit BLACK	LockBit GREEN	LockBit-NG-Dev
Basic Feature	✓	✓	Based on BlackMatter	Based on Conti v3	
API Resolving		FNV1a	RoR13 + XOR	Murmur	
Printing Bomb		✓	✓	✓	
Self-Spread (GPO)		✓	✓	✓	
Encrypted Memory			✓	✓	
Password Guardrail			✓	✓	

Why?

# LockBit's Arsenal

## LockBit Green



(2022-08)

(2023-01)

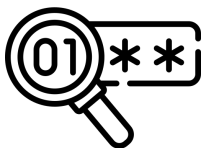
LockBit Black Builder Leaked

LockBit Green released

# LockBit's Arsenal

## LockBit Green

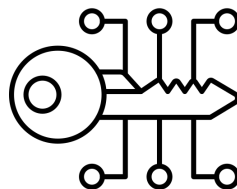
### Features added in LockBit Green



#### Decrypting extensions



```
lstrlenA = GetProc_sub_4052F0(15, 0x167D3EDD, 106);  
if ( lstrlenA(Extension_byte_436898) ) // .fc59d76b  
{  
  do  
  {  
    Extension_byte_436898[v4++] ^= 0x78u;  
    v6 = GetProc_sub_4052F0(15, 0x167D3EDD, 106);  
  }  
  while ( v4 < v6(Extension_byte_436898) );  
}
```



#### Decoding RSA Public Key



#### CryptDecodeObject function (wincrypt.h)

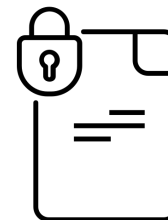
article • 2023. 08. 27.

[feedback](#)

#### Contents of this document

- construction
- parameter
- return value
- explanation
- Show 2 more

The `CryptDecodeObject` function decodes a structure of the type indicated by the `lpszStructType` parameter. `CryptDecodeObjectEx` offers significant performance improvements and is recommended as an API that performs the same functionality.



#### Update RansomNote



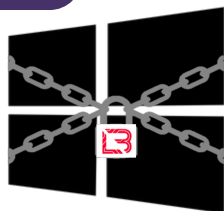
#### Readme.txt



!!!-Restore-My-Files-!!!.txt

# LockBit's Arsenal

Arsenal



LockBit **RED**



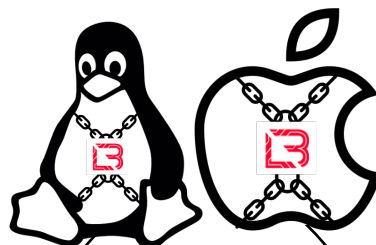
LockBit **Black**



LockBit **Green**



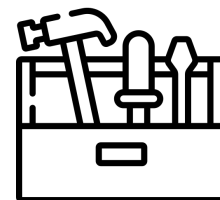
LockBit-NG-Dev



LockBit Linux/ESXi



LockBit MacOS



StealBit



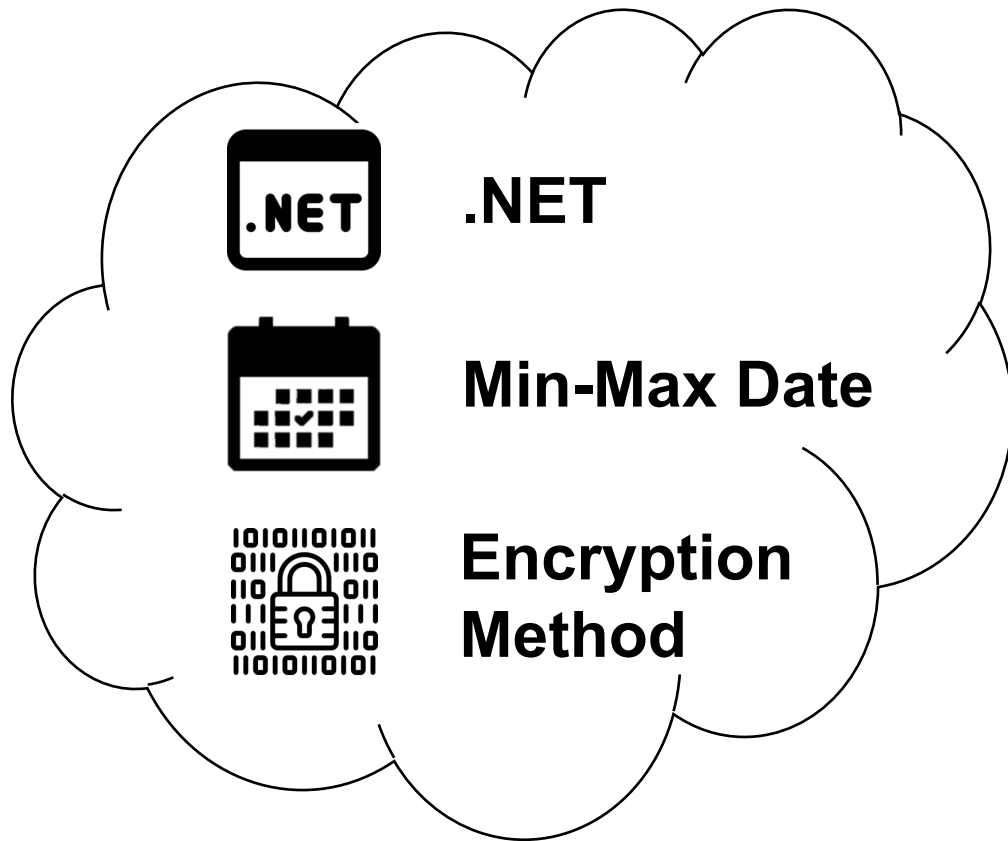
# LockBit's Arsenal

## LockBit-NG-Dev

	LockBit	LockBit RED	LockBit BLACK	LockBit GREEN	LockBit-NG-Dev
Basic Feature	✓	Based on LockBit	Based on BlackMatter	Based on Conti v3	Based on -
API Resolving		FNV1a	RoR13 + XOR	Murmur	-
Printing Bomb		✓	✓		□
Self-Spread (GPO)		✓	Update Later? ✓		□
Encrypted Memory			✓		□
Password Guardrail			✓		□
Execution date limit					✓

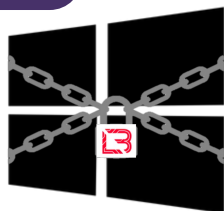
# LockBit's Arsenal

## LockBit-NG-Dev



# LockBit's Arsenal

Arsenal



LockBit **RED**



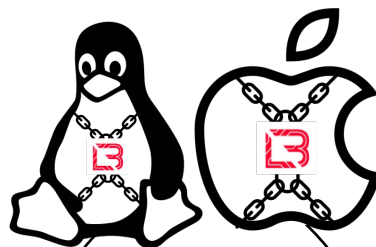
LockBit **Black**



LockBit **Green**



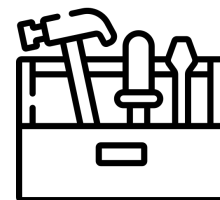
LockBit-NG-Dev



LockBit Linux/ESXi



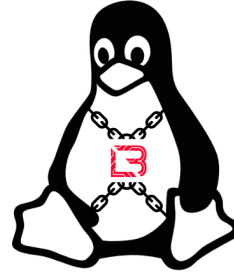
LockBit MacOS



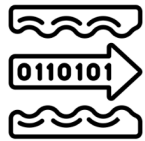
StealBit

# LockBit's Arsenal

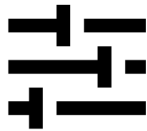
Linux/ESXi



## LockBit Linux/ESXi



1. Decode String



2. Parameter Check



3. Detect VM



4. Encrypt Files  
(AES-128+ECC)



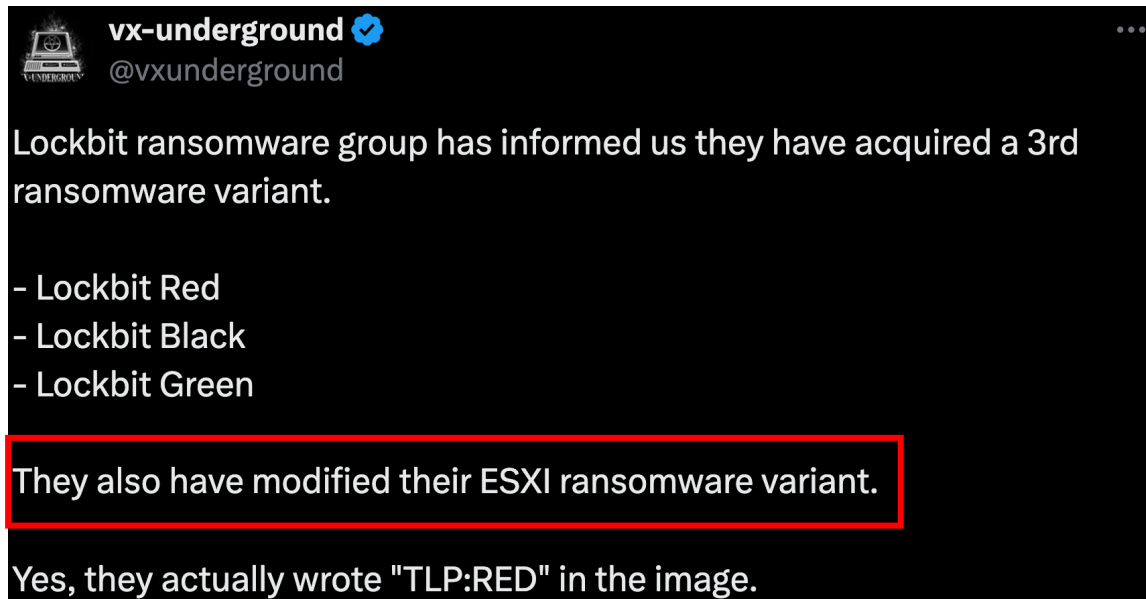
5. Make Ransomnote



6. Logging

# LockBit's Arsenal

Linux/ESXi



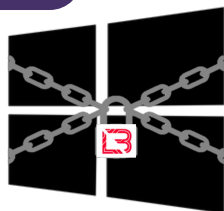
# LockBit's Arsenal

## Linux/ESXi

	Version 1.0	Version 1.1	Version 1.2	Version 1.3
Basic Features		✓		Updated Encryption Logic & Logging File name
Error Handling	✗		✓	
VM Discovery	✗		✓	
Exclude Paths		✗		/etc/sudoers.d, /usr/share
Additional Parameters		✗		<p><b>-p/--pass</b>            -f/--full            -a/-delay            -y/--noexts  <b>-v/--vmdk</b>            -t/--wipe</p>
List Items		✗		Directories, Processes, Usernames

# LockBit's Arsenal

Arsenal



LockBit **RED**



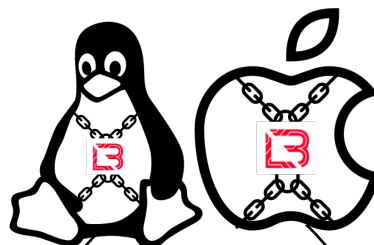
LockBit **Black**



LockBit **Green**



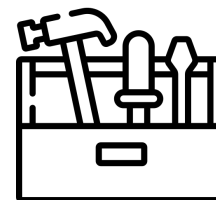
LockBit-NG-Dev



LockBit Linux/ESXi



LockBit MacOS



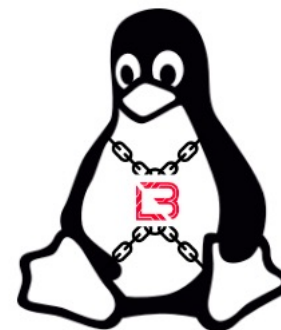
StealBit

# LockBit's Arsenal

LockBit MacOS



**LockBit MacOS**



**LockBit Linux/ESXi**



# LockBit's Arsenal

## LockBit MacOS

```
de_xor_all(); // Decode String XOR
except_foler1 = (__int64)strdup(&sudoers_d);
except_foler2 = (__int64)strdup(&usr_share);
if ( byte_1000596D2 )
{
    __strcat_chk(&byte_1000596D2, &comma, 512LL);
    v14 = basename((char *)*argv);
    __strcat_chk(&byte_1000596D2, v14, 512LL);
}
else
{
    v15 = basename((char *)*argv);
    __strcpy_chk(&byte_1000596D2, v15, 512LL);
}
__strcat_chk(&byte_1000596D2, &comma, 512LL);
__strcat_chk(&byte_1000596D2, &logg_1, 512LL);
go(argc, argv); // Check Parameter & Encryption
finished_time = time(0LL);
all_files = get_all_files(); // Get all files
get_all_processes(all_files); // Get all Processes
v23 = time(0LL);
v17 = gmtime(&v23);
strftime(v24, 0x100uLL, &time_fmt, v17);
PrintLog2(&version);
v18 = gmtime(&v23);
v19 = strftime(v24, 0x100uLL, &date_time_fmt, v18);
get_uname_a(v19); // Get User name
get_version(); // Get Vmware Version
get_processorinfo(); // Get CPU Model
get_volumes_info(); // Get Volume Info
v20 = PrintLog2(&reports); // Print Logging
```

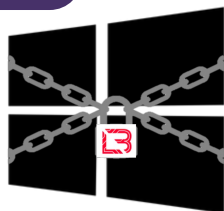
MacOS

```
Decode_string_sub_404200(); // Decode String XOR
except_folder1_qword_642710 = __strdup(&unk_640F37);
except_folder2_qword_642718 = __strdup(&unk_640F46);
if ( :s )
{
    strcat(&:s, &byte_640424);
    v22 = __xpg_basename(*a2);
    strcat(&:s, v22);
}
else
{
    v11 = __xpg_basename(*a2);
    strcpy(&:s, v11);
}
strcat(&:s, &byte_640424);
strcat(&:s, locklog_unk_63D072);
go_sub_408110(a1, a2); // Check Parameter & Encryption
finished_time_qword_642CC0 = time(0LL);
mw_ListVolume(); // Get all files
mw_ReadProcessList(); // Get all Processes
timer = time(0LL);
v12 = gmtime(&timer);
strftime(s, 0x100uLL, &format, v12);
mw_OutputString(unk_640860);
v13 = gmtime(&timer);
strftime(s, 0x100uLL, aXm, v13);
v14 = qword_642CA8;
v15 = qword_6428A8;
v16 = finished_time_qword_642CC0 - qword_642890;
v24 = qword_642CD8;
v23 = qword_6427F0;
EsxiStorageList = mw_GetEsxiStorageList(); // Get Volume Info
v26 = qword_6427E8;
CpuModel = mw_GetCpuModel(); // Get CPU Model
VmwareVersion = mw_GetVmwareVersion(); // Get Vmware Version
Uname = mw_GetUname(); // Get User name
mw_OutputString(); // Print Logging
```

Linux/ESXi V 1.2

# LockBit's Arsenal

Arsenal



LockBit **RED**



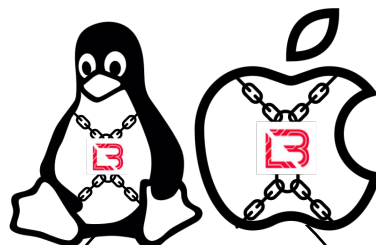
LockBit **Black**



LockBit **Green**



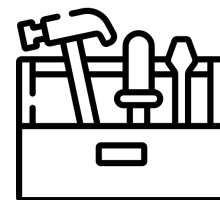
LockBit-NG-Dev



LockBit Linux/ESXi



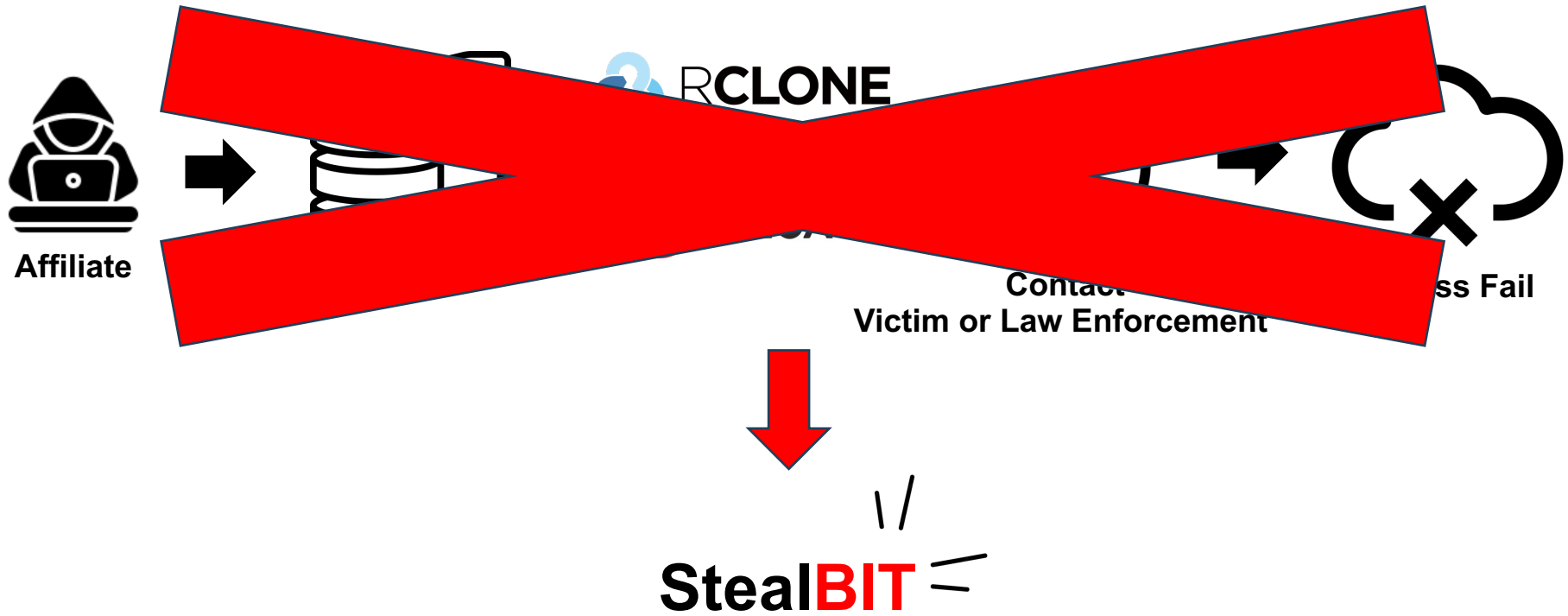
LockBit MacOS



StealBit

# LockBit's Arsenal

StealBit



# LockBit's Arsenal

## StealBit

```
StealBit
[21:39:21] [+] WinSock initialized
[21:39:21] [+] IO completion port initialized...
[21:39:21] Connecting to 88.80.147.102
[21:39:21] Check server 88.80.147.102...
[21:39:22] Connecting to 168.100.11.72
[21:39:22] Check server 168.100.11.72...
[21:39:23] Connecting to 139.60.160.200
[21:39:23] Check server 139.60.160.200...
[21:39:24] Connecting to 193.38.235.234
[21:39:24] Check server 193.38.235.234...
[21:39:25] Connecting to 174.138.62.35
[21:39:25] Check server 174.138.62.35...
[21:39:26] Connecting to 88.80.147.102
[21:39:26] Check server 88.80.147.102...
```

**StealBit 1.0**

```
StealBit 1.1
[21:54:49] StealBit 1.1 config:
Network limit: unlim
Self delete: No; Hide Window: No
Skip system files: Yes; folders: Yes
Max filesize: unlim
[21:54:49] PC: MalAnalysis@NODOMAIN
[21:54:49] [+] WinSock initialized
[21:54:49] [+] IO completion port initialized...
[21:54:50] Connecting to 185.182.193.120
[21:54:50] Check server 185.182.193.120...
[21:54:51] Connecting to 185.182.193.120
[21:54:51] Check server 185.182.193.120...
[21:54:52] Connecting to 185.182.193.120
[21:54:52] Check server 185.182.193.120...
[21:54:53] Connecting to 185.182.193.120
[21:54:53] Check server 185.182.193.120...
[21:54:54] Connecting to 185.182.193.120
```

**StealBit 1.1**

# LockBit's Arsenal

## StealBit

	StealBit 1.0	StealBit 1.1
<b>API Resolving</b>	FNV1a	Shift + XOR
<b>Parameter</b>	<Path>	<Path> -hide/-h -delete/-d -net/-n -once/-o -file/-f -skipfiles -skipfolders
<b>CIS Check</b>	O	X
<b>Anti-Debugging</b>	O	O
<b>I/O Completion</b>	O	O

### Similarities Function to LockBit RED

```
if ( (NtCurrentPeb()->NtGlobalFlag & 0x70) != 0 )  
{  
    while ( 1 )  
    ;  
}
```

#### Anti-Debugging

```
v0 = j_FNV_KERNEL32_405D4D();  
GetSystemDefaultUILanguage_ = sub_40BA69(v0);  
v2 = GetSystemDefaultUILanguage_();  
if ( v2 == 0x82C // Cyrillic from Azerbaijan  
    v2 == 0x42C // Azerbaijani (Latin from Azerbaijan)  
    v2 == 0x42B // Armenian  
    v2 == 0x423 // Belarusian  
    v2 == 0x437 // Georgian  
    v2 == 0x43F // Kazakh from Kazakhstan  
    v2 == 0x440 // Kyrgyzstan  
    v2 == 0x819 // Russian from Moldova  
    v2 == 0x419 // Russian  
    v2 == 0x428 // Tajik (Cyrilic from Tajikistan)  
    v2 == 0x442 // Turkmenistan  
    v2 == 0x843 // Cyrillic from Uzbekistan  
    v2 == 0x443 // Latin from Uzbekistan  
    v2 == 0x422 ) // Ukranian  
{  
    v3 = j_FNV_KERNEL32_405D4D();  
    ExitProcess_ = sub_40BA6E(v3);  
    ExitProcess_(0);  
}
```

#### Check CIS

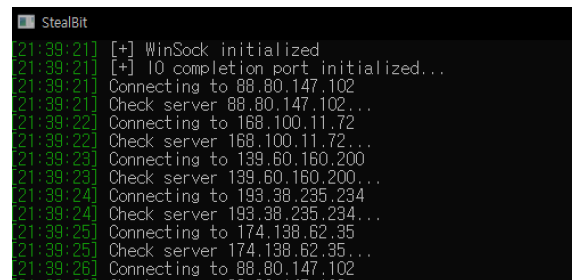
#### FNV hash parameters [ edit ]

The above FNV prime constraints and the definition of the FNV offset basis yield the following table of FNV hash parameters:

FNV parameters [4][4]

Size in bits	Representation	FNV prime	FNV offset basis
32	Expression	$2^{24} + 2^8 + 0x93$	
	Decimal	16777619	2166136261
	Hexadecimal	0x01000193	0x811c9dc5

#### API Resolving (FNV1a)



#### Debugging shortcut key (Shift + F2)

### Why don't use StealBit?



**The function does not work**



**Frequently detected and blocked**

# Conclusion



# Conclusion

## Lesson

Many functions of Lockbit that are similar to Conti, indicating that Lockbit has numerous examples of code from

1. I have said more than once that **I want to collect as many top lockers as possible in one panel ...**
2. It would be a sin not to take **the sources of the**

## Constantly Looking for source code !



Forum Users

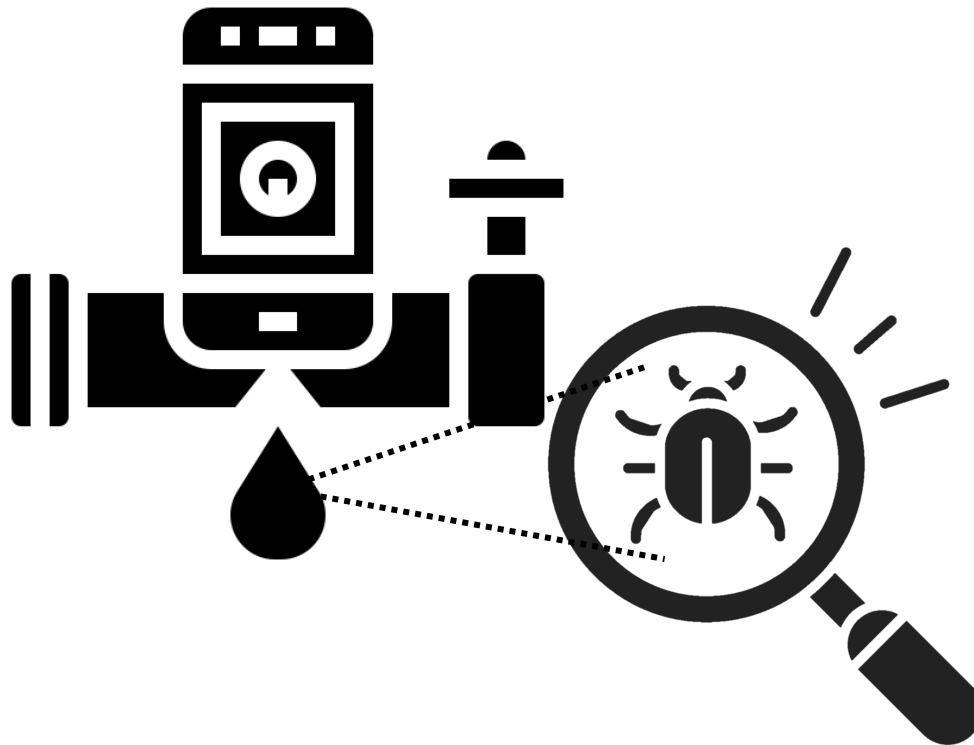
When you write to me in a personal message, do not check the box "Encrypt correspondence (AES256+SHA256)", if you are afraid to read your personal messages, then write through a secure [PRIVATE NOTE](#) and you can send a picture or file through a secure [FILE](#)



LockBitSupp

## Conclusion

### Lesson



**Immediate analysis and detection points for leaked ransomware**

## Conclusion

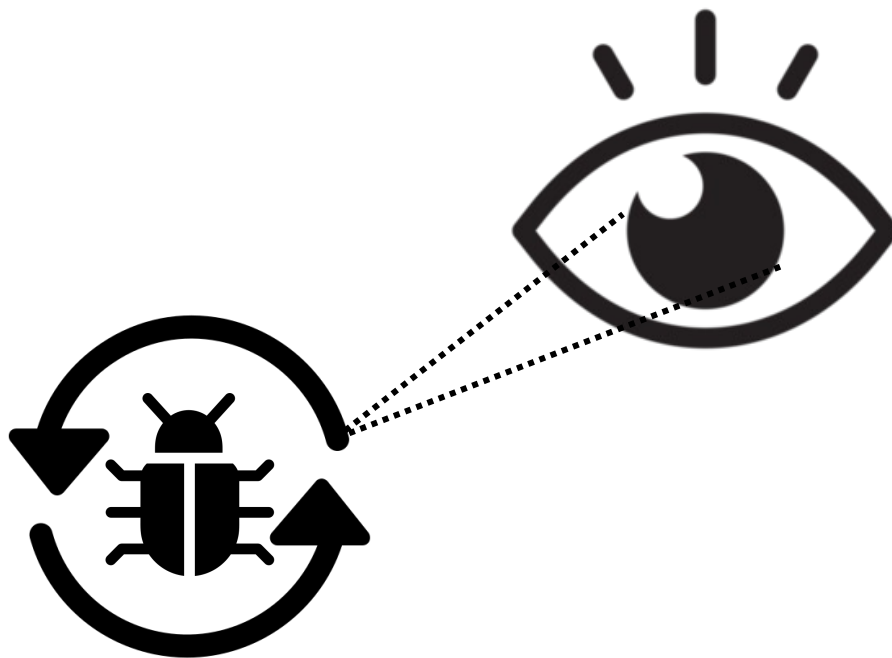
Lesson

Also...



## Conclusion

### Lesson



**Keep track of LockBit's arsenal by identifying its key features**



---

## About S2W

**S2W** is a big data intelligence company specialized in hidden channels and cryptocurrencies.

**S2W** captures massive amount of data from various channels and conducts analysis with the unique AI based multi-domain analytics engine.

**S2W** Offers a threat intelligence solution **S2-XARVIS**, cryptocurrency anti-money laundering solution **S2-EYEZ**, digital fraud detection system **S2-TRUZ**.

---

## Contact

For any queries, please contact

[info@s2w.inc](mailto:info@s2w.inc)

[www.s2w.inc](http://www.s2w.inc)