

# Cyble - BianLian: New Ransomware Variant On The Rise

Published: 2022-08-18 · Archived: 2026-04-05 19:42:06 UTC

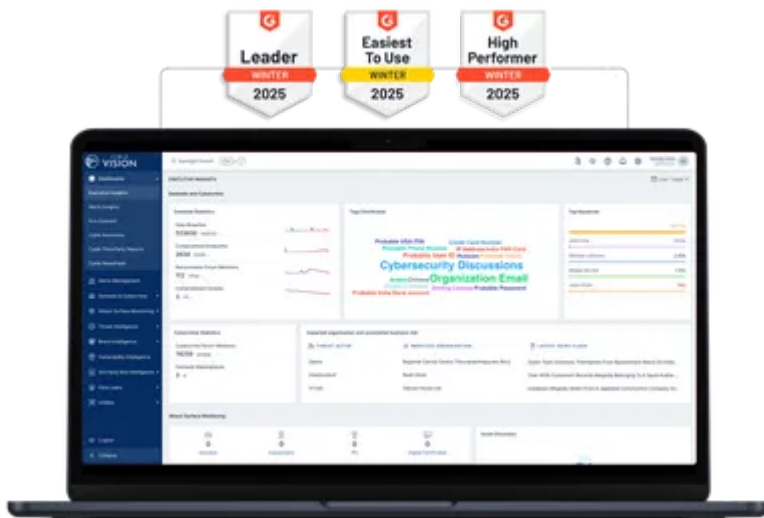
Cyble analyzes BianLian Ransomware and the increasing popularity of GoLang amongst Threat Actors.

## GoLang-based Ransomware targets multiple industries

Cyble Research Labs has observed that malware written in the programming language “Go” has recently been popular among Threat Actors (TAs). This is likely due to its cross-platform functionalities and the fact that it makes reverse engineering more difficult. We have seen many threats developed using the Go language, such as Ransomware, RAT, Stealer, etc.

During our routine threat-hunting exercise, we came across a [Twitter](#) post about a ransomware variant written in Go named “BianLian,” which was first identified halfway through July 2022.

World's Best AI-Native Threat Intelligence



The ransomware has targeted many well-known organizations (9 victims so far) across several industry sectors such as Manufacturing, Education, Healthcare, BFSI, etc. In the figure below, we have prepared a breakdown of the industries targeted by the BianLian ransomware.

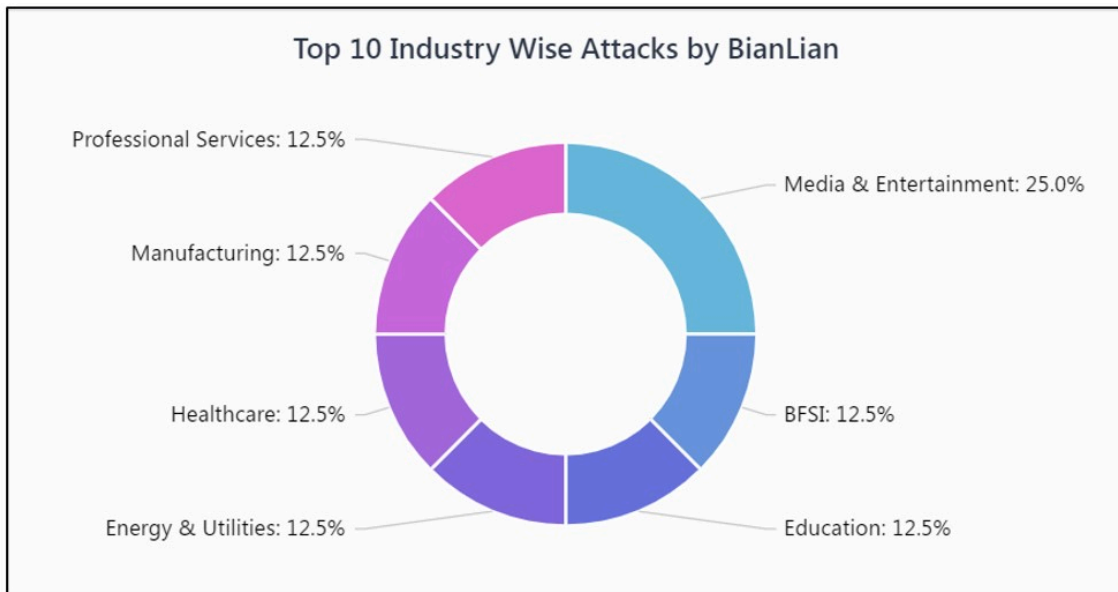


Figure 1 – Industries Targeted by the BianLian Ransomware

## Technical Analysis

We have taken the below sample hash for the purposes of this analysis:

(SHA256), *ea75e26c5e73f3db82cd07ea45e4d244ccb3ec3397ab5263a1a74add7bbcb6e2*, which is a 64-bit GoLang binary executable.

The unique build ID of the GoLang [ransomware](#) is shown below.



Figure 2 – Go Build ID

Upon execution of the ransomware, it attempts to identify if the file is running in a WINE environment by checking the *wine\_get\_version()* function via the *GetProcAddress()* API.

**CYBLE.** See What **2025** Really Looked Like Across **Every Region**  
Global | APAC | Europe | North America | META | Australia & New Zealand  
**Get Your Free Reports Today!**

```
mov rcx,qword ptr ds:[rsi]
mov rdx,qword ptr ds:[rsi+8]
mov r8,qword ptr ds:[rsi+10]
mov r9,qword ptr ds:[rsi+18]
movq xmm0,rcx
movq xmm1,rdx
movq xmm2,r8
movq xmm3,r9
call rax
add rsp,150
```

[rsi]: "M74"
[rsi+8]: "wine_get_version"
GetProcAddress

Figure 3 – Anti-analysis Technique

Then, the ransomware creates multiple threads using the *CreateThread()* API function to perform faster file encryption, making reverse engineering the [malware](#) more difficult. The below figure shows the multiple threads created by the ransomware.

Number	ID	Entry	TEB	RIP	Suspend Count	Priority	Wait Reason	Last Error	User Time	Kernel Time	Creation Time	CPU Cycles	Name
44	1540	0000000000830FC0	000000C7744BF000	00007FF98F520C90	1	Normal	Executive	00000000	00:00:00.0000000	00:00:00.0156250	16:02:13.9907703	337AF5F6	
47	6644	0000000000830FC0	000000C7744D1000	00007FF98F70E241	1	Normal	Suspended	00000000	00:00:00.0156250	00:00:00.0156250	16:02:47.6762539	138E4EE	
48	1516	0000000000830FC0	000000C7744AF000	00007FF98F70E241	1	Normal	Suspended	00000000	00:00:00.0781250	00:00:00.0468750	16:02:13.9439735	10803C3	
49	3268	0000000000830FC0	000000C774501000	00007FF98F70E241	1	Normal	Suspended	00000000	00:00:00.0000000	00:00:00.0000000	16:02:48.917235	ADC112	Main Thread
36	8016	0000000000830FC0	000000C7744F7000	00007FF98F70E241	1	Normal	Suspended	00000000	00:00:00.0000000	00:00:00.0156250	16:02:48.6905216	19C3E59	
1	8176	00007FF98F82E000	000000C7744E8000	00007FF98F70F7F4	1	Normal	Suspended	00000000	00:00:00.0000000	00:00:00.0000000	16:02:13.951303	865396	
2	7088	00007FF98F82E000	000000C7744B3000	00007FF98F70F7F4	1	Normal	Suspended	00000000	00:00:00.0000000	00:00:00.0000000	16:02:13.9309226	9833E8	
7	7180	0000000000830FC0	000000C7744B0000	00007FF98F70E241	1	Normal	Suspended	00000000	00:00:00.0000000	00:00:00.0156250	16:02:13.985459	18A8954	
40	7256	0000000000830FC0	000000C7744E9000	00007FF98F70E241	1	Normal	Suspended	00000000	00:00:00.0000000	00:00:00.0000000	16:02:48.9124866	64D028	
3	8940	0000000000830FC0	000000C7744B5000	00007FF98F70E241	1	Normal	Suspended	00000000	00:00:00.0000000	00:00:00.2031250	16:02:13.9653053	35FDC46	
5	7344	0000000000830FC0	000000C7744B9000	00007FF98F70E241	1	Normal	Suspended	00000000	00:00:00.0000000	00:00:00.0000000	16:02:13.9683209	5823A8	
46	288	0000000000830FC0	000000C77450B000	00007FF98F70E241	1	Normal	Suspended	00000000	00:00:00.0000000	00:00:00.0000000	16:02:49.3498195	E9536E	
6	9160	0000000000830FC0	000000C7744B8000	00007FF98F70E241	1	Normal	Suspended	00000000	00:00:00.0156250	00:00:00.0625000	16:02:13.9841106	8597787	
4	7112	0000000000830FC0	000000C7744E7000	00007FF98F70E241	1	Normal	Suspended	00000000	00:00:00.0000000	00:00:00.0000000	16:02:13.9656547	62D9F83	
9	4844	0000000000830FC0	000000C7744C1000	00007FF98F70E241	1	Normal	Suspended	00000000	00:00:00.0156250	00:00:00.0468750	16:02:13.9939187	A7968D	
10	2068	0000000000830FC0	000000C7744C3000	00007FF98F70E241	1	Normal	Suspended	00000000	00:00:00.0156250	00:00:00.0156250	16:02:13.9974957	3CD5F5A	
48	2352	0000000000830FC0	000000C77450F000	00007FF98F70E241	1	Normal	Suspended	00000000	00:00:00.0000000	00:00:00.0000000	16:02:49.3538539	AC20E0	
26	8636	0000000000830FC0	000000C7744E3000	00007FF98F70E241	1	Normal	Suspended	00000000	00:00:00.0000000	00:00:00.0312500	16:02:48.0818999	C26246	
11	8012	0000000000830FC0	000000C7744C5000	00007FF98F70E241	1	Normal	Suspended	00000000	00:00:00.0000000	00:00:00.0312500	16:02:14.0030609	10M9E8	
20	2832	0000000000830FC0	000000C7744D7000	00007FF98F70E241	1	Normal	Suspended	00000000	00:00:00.0000000	00:00:00.0156250	16:02:47.6878827	DCC40A	
12	6816	0000000000830FC0	000000C7744C7000	00007FF98F70E241	1	Normal	Suspended	00000000	00:00:00.0000000	00:00:00.0156250	16:02:44.9971212	4200AEC	
13	4576	0000000000830FC0	000000C7744C9000	00007FF98F70E241	1	Normal	Suspended	00000000	00:00:00.0000000	00:00:00.0312500	16:02:44.9975468	A93960A	
43	4252	0000000000830FC0	000000C774505000	00007FF98F70E241	1	Normal	Suspended	00000000	00:00:00.0000000	00:00:00.0000000	16:02:49.1300859	8F5A44	
20	9392	0000000000830FC0	000000C7744E8000	00007FF98F70E241	1	Normal	Suspended	00000000	00:00:00.0000000	00:00:00.0000000	16:02:148.2906070	75816F	
14	4396	0000000000830FC0	000000C7744C8000	00007FF98F70E241	1	Normal	Suspended	00000000	00:00:00.0000000	00:00:00.0000000	16:02:45.4862300	1CE2422	
15	6800	0000000000830FC0	000000C7744D0000	00007FF98F70E241	1	Normal	Suspended	00000000	00:00:00.0000000	00:00:00.0312500	16:02:45.4862300	2738A05	
16	4752	0000000000830FC0	000000C7744E9000	00007FF98F70E241	1	Normal	Suspended	00000000	00:00:00.0000000	00:00:00.0312500	16:02:45.4862300	1881227	
18	6704	0000000000830FC0	000000C7744D3000	00007FF98F70E241	1	Normal	Suspended	00000000	00:00:00.0156250	00:00:00.0156250	16:02:47.6790081	F8D2C9	
19	6352	0000000000830FC0	000000C7744E5000	00007FF98F70E241	1	Normal	Suspended	00000000	00:00:00.0000000	00:00:00.0156250	16:02:47.6822014	1ACCF31	
21	340	0000000000830FC0	000000C7744D9000	00007FF98F70E241	1	Normal	Suspended	00000000	00:00:00.0000000	00:00:00.0156250	16:02:47.7006434	1ED5481	
22	6472	0000000000830FC0	000000C7744B0000	00007FF98F70E241	1	Normal	Suspended	00000000	00:00:00.0000000	00:00:00.0000000	16:02:47.7043146	196C951	
23	7700	0000000000830FC0	000000C7744D0000	00007FF98F70E241	1	Normal	Suspended	00000000	00:00:00.0156250	00:00:00.0156250	16:02:47.7469933	AC3C6A	
60	1920	0000000000830FC0	000000C774527000	00007FF98F70E241	1	Normal	Suspended	00000000	00:00:00.0000000	00:00:00.0000000	16:02:49.6031275	D022D1	
24	5328	0000000000830FC0	000000C7744E0000	00007FF98F70E241	1	Normal	Suspended	00000000	00:00:00.0156250	00:00:00.0156250	16:02:47.8763873	CF5EE	
37	3804	0000000000830FC0	000000C7744F9000	00007FF98F70E241	1	Normal	Suspended	00000000	00:00:00.0000000	00:00:00.0000000	16:02:48.6921065	808C7A	
32	7352	0000000000830FC0	000000C7744E0000	00007FF98F70E241	1	Normal	Suspended	00000000	00:00:00.0000000	00:00:00.0312500	16:02:48.3012354	139E180	
15	8904	0000000000830FC0	000000C7744E1000	00007FF98F70E241	1	Normal	Suspended	00000000	00:00:00.0000000	00:00:00.0000000	16:02:47.8772279	1190E5	
27	3300	0000000000830FC0	000000C7744E5000	00007FF98F70E241	1	Normal	Suspended	00000000	00:00:00.0000000	00:00:00.0000000	16:02:48.0820478	831F30	

Figure 4 – Multiple Thread Creation

Next, the malware identifies the system drives (from A:\ to Z:\) using the *GetDriveTypeW()* API function and encrypts any files available in the connected drives. Then, the malware drops a ransom note in multiple folders with the file name “Look at this instruction.txt.”

The ransomware creates a ransom note with the content shown below.

```

0000 6648:0F6EC1      movq xmm0,r,cx
0000 6648:0F6ECA      movq xmm1,rdx
0000 6649:0F6ED0      movq xmm2,r,8
0000 6649:0F6ED9      movq xmm2,r,8
0000 FFDD          call rdx,writefile
0000 48:81C4 50010000  add r,r,150
0000 59           pop r,cx
0000 48:8941 18      mov qword ptr ds:[rcx+18],rax
    
```

rax=1

.text:0000000000830D1C new\_one.exe:\$60D1C #6031C

Address Hex ASCII

```

000000 59 6F 75 72 20 66 65 74 77 6F 72 68 20 73 79 73 Your network sys
000000 65 64 20 61 6E 64 20 65 6E 63 72 79 70 74 65 64 ed and encrypted
000000 2E 20 43 6F 6E 74 61 63 74 20 75 73 20 69 6E 20 . contact us in
000000 6F 72 64 65 72 20 74 6F 20 72 65 73 74 6F 72 65 order to restore
000000 20 79 6E 75 72 20 74 63 2E 20 74 63 2E 20 74 63 2E 20 your data. Do
000000 64 20 6D 61 68 65 20 61 6E 79 20 63 68 61 6E 67 t make any chang
000000 65 73 20 69 6E 20 79 6F 75 72 20 66 69 6C 65 20 es in your file
000000 73 74 72 75 63 74 75 72 65 3A 20 74 6F 75 63 68 structure: touch
000000 20 6E 6F 20 66 69 6C 65 73 2C 20 64 6F 6E 27 74 no files, don't
000000 79 6E 75 72 20 74 6F 20 74 63 2E 20 74 63 2E 20 try to recover
000000 62 79 20 79 6F 75 72 73 65 6C 6E 2C 20 74 68 61 by yourself, thi
000000 74 20 6D 61 79 20 6C 65 61 64 20 74 6F 20 69 74 t may lead to it
000000 27 73 20 63 6F 6D 70 6C 65 74 65 20 6C 6F 73 73 's complete loss
000000 2E 0D 0A 0D 0A 54 6F 20 63 6F 6E 74 61 63 74 20 ....To contact
000000 73 20 79 6F 75 20 68 61 76 65 20 74 6F 20 64 us you have to d
000000 6F 77 6E 6C 6F 61 64 20 22 74 6F 78 22 20 6D 65 ownload "tox" me
000000 73 73 65 6E 67 65 72 3A 20 68 74 74 70 73 3A 2F senger: https://
000000 2F 71 74 6F 78 2E 67 69 74 68 75 62 2E 69 6F 2F /github.io/
    
```

Figure 5 – Malware Writing Ransom Notes

After dropping the [ransom note](#), the malware searches files and directories for encryption by enumerating them using the *FindFirstFileW()* and *FindNextFileW()* API functions.

The ransomware excludes the below file extensions and file/folder names from encryption.

File extension	.exe, .dll, .sys, .txt, .lnk and .html
File names	bootmgr, BOOTNXT, pagefile.sys, thumbs.db, ntuser.dat and swapfile.sys

Folder names	Windows, Windows.old
--------------	----------------------

The ransomware uses GoLang Packages such as “crypto/cipher,” “crypto/aes” and “crypto/rsa” for file encryption on the victim machine.

```
crypto/cipher.newCBC
crypto/cipher.dup
crypto/cipher.NewCBCEncrypter
crypto/cipher.(*cbcEncrypter).BlockSize
crypto/cipher.(*cbcEncrypter).CryptBlocks
crypto/internal/subtle.InexactOverlap
crypto/internal/subtle.AnyOverlap
crypto/cipher.xorBytes
crypto/cipher.init
crypto/cipher.xorBytesSSE2
crypto/aes.encryptBlockGo
encoding/binary.bigEndian.Uint32
encoding/binary.bigEndian.PutUint32
crypto/aes.expandKeyGo
crypto/aes.rotw
crypto/aes.subw
crypto/aes.KeySizeError.Error
crypto/aes.NewCipher
crypto/aes.newCipherGeneric
crypto/aes.(*aesCipher).BlockSize
crypto/aes.(*aesCipher).Encrypt
crypto/aes.newCipher
crypto/aes.(*aesCipherAsm).BlockSize
crypto/aes.(*aesCipherAsm).Encrypt
crypto/aes.init
```

Figure 6 – Hardcoded Strings of “Crypto” GoLang Packages

For encryption, the malware divides the file content into 10 bytes chunks. First, it reads 10 bytes from the original file, then encrypts the bytes and writes the encrypted data into the target file. Dividing the data into small chunks is a method to [evade detection](#) by Anti-Virus products.

The figure below shows the code snippet of the encryption loop and the original and infected file content before and after encryption.

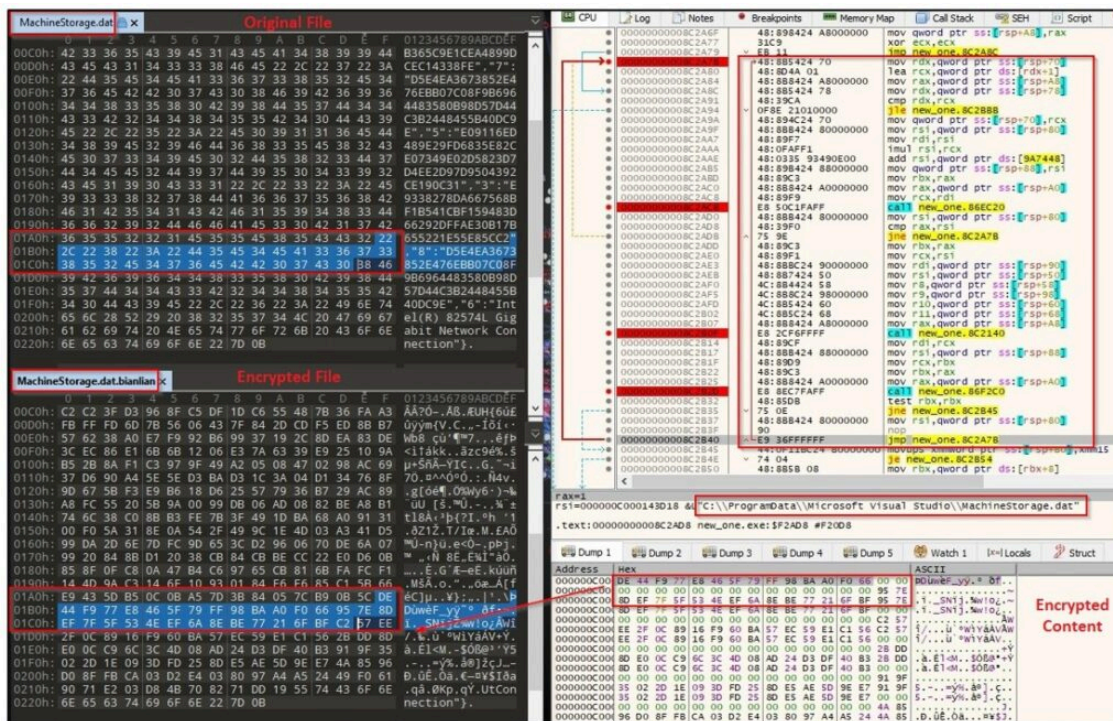


Figure 7 – Encryption routine and Original/Encrypted file content

In the next step, the malware renames the encrypted files with the “bianlian” extension and replaces them with the original file using the *MoveFileExW()* API function, as shown below.

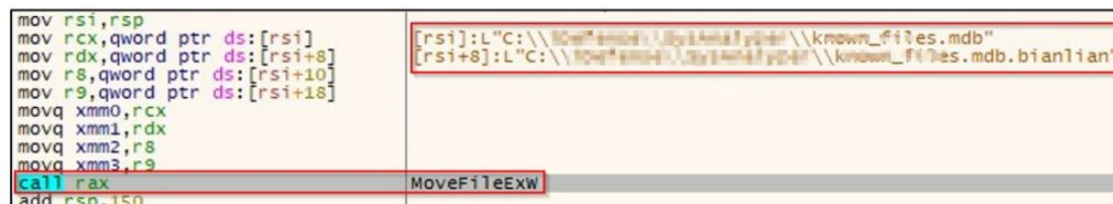
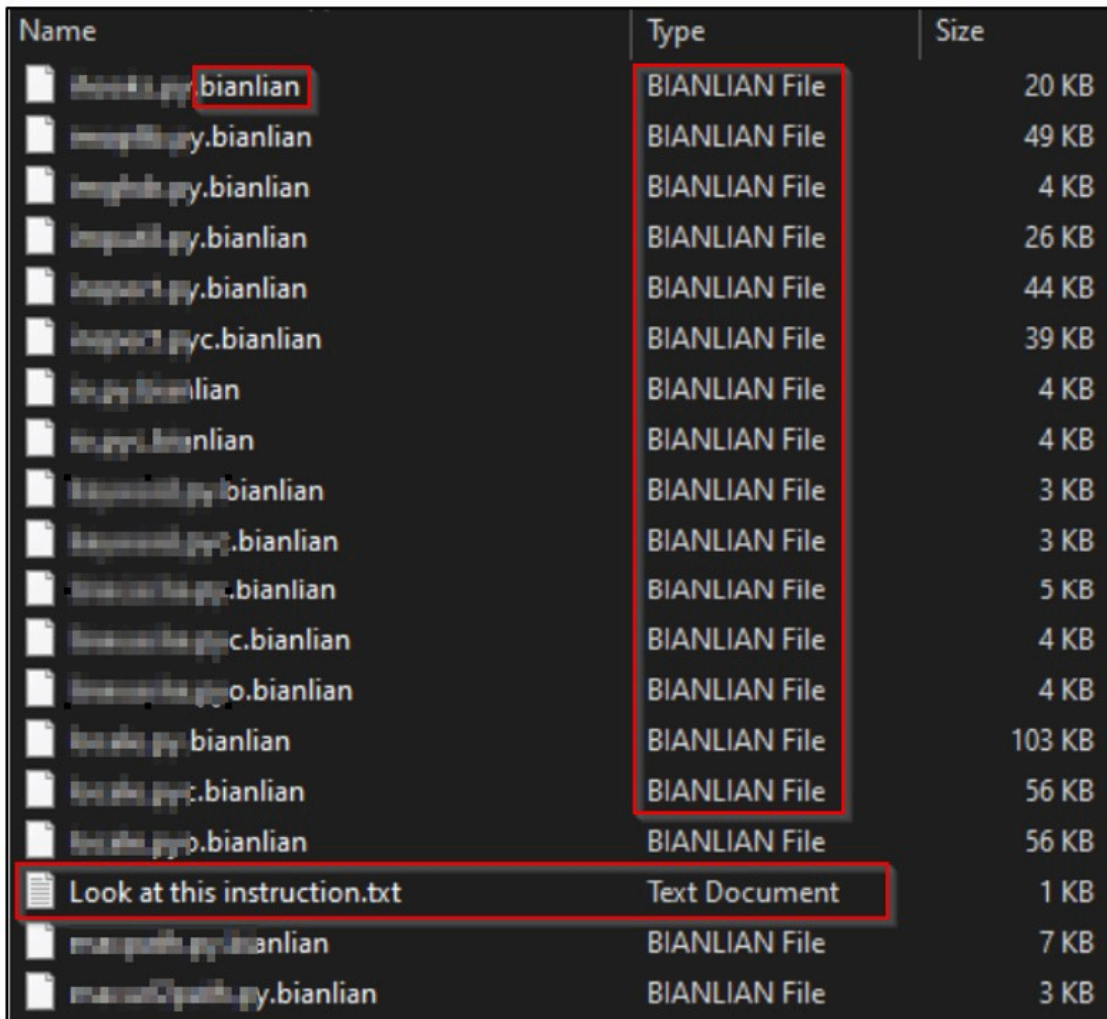


Figure 8 – MoveFileExW() API

Finally, the ransomware deletes itself using the following command line, leaving only the encrypted files and the ransom note on the victim’s machine.

- `cmd /c del C:\Users<Admin>\Desktop\new_one.exe`

The below figure shows the BianLian ransomware encrypted files and ransom note text file after the successful infection of a victim’s machine.



Name	Type	Size
...bianlian	BIANLIAN File	20 KB
...py.bianlian	BIANLIAN File	49 KB
...py.bianlian	BIANLIAN File	4 KB
...py.bianlian	BIANLIAN File	26 KB
...py.bianlian	BIANLIAN File	44 KB
...pyc.bianlian	BIANLIAN File	39 KB
...bianlian	BIANLIAN File	4 KB
...bianlian	BIANLIAN File	4 KB
...bianlian	BIANLIAN File	3 KB
...bianlian	BIANLIAN File	3 KB
...bianlian	BIANLIAN File	5 KB
...c.bianlian	BIANLIAN File	4 KB
...o.bianlian	BIANLIAN File	4 KB
...bianlian	BIANLIAN File	103 KB
...c.bianlian	BIANLIAN File	56 KB
...b.bianlian	BIANLIAN File	56 KB
Look at this instruction.txt	Text Document	1 KB
...bianlian	BIANLIAN File	7 KB
...py.bianlian	BIANLIAN File	3 KB

Figure 9 – Files encrypted by BianLian Ransomware

In the dropped ransom note, victims are given instructions on how they can contact the TAs to restore their encrypted files.

The TAs threaten their victims, stating that their important data, such as financial, client, business, technical, and personal files, has been downloaded and will be posted on their leak site if the ransom is not paid within ten days.

The ransom note also contains the ID of TOX Messenger for ransom negotiations and the Onion URL of the leak site page – shown in the figure below.



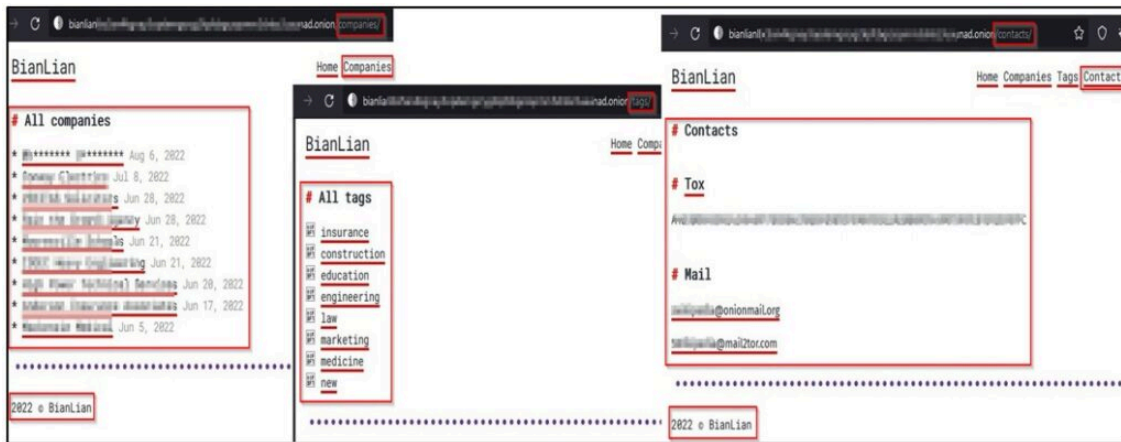


Figure 12 – BianLian Leak site affected companies list & TAs contact details

## Conclusion

Ransomware is becoming an increasingly common and effective attack method that affects organizations and their productivity. BianLian is GoLang-based ransomware that continues to breach several industries and demand large ransom amounts. The TAs also use the double extortion method by stealing an affected organization’s files and leaking them online if the ransom is not paid on time.

TAs write their ransomware in GoLang for various reasons; the language enables a single codebase to be compiled into all major [operating systems](#). The TAs behind BianLian are constantly making changes and adding new capabilities to avoid detection.

Cyble Research Labs will continue to monitor BianLian and other similar Ransomware groups’ activities and analyze them to better understand their motivations.

## Our Recommendations

We have listed some [essential cybersecurity](#) best practices that create the first line of control against attackers. We recommend that our readers follow the best practices given below:

### Safety Measures Needed to Prevent Ransomware Attacks

- Conduct regular backup practices and keep those backups offline or in a separate network.
- Turn on the automatic software update feature on your computer, mobile, and other connected devices wherever possible and pragmatic.
- Use a reputed anti-virus and [Internet security](#) software package on your connected devices, including PC, laptop, and mobile.
- Refrain from opening untrusted links and email attachments without verifying their authenticity.

### Users Should Take the Following Steps After the Ransomware Attack

- Detach infected devices on the same network.
- Disconnect external storage devices if connected.
- Inspect system logs for suspicious events.

## Impact of BianLian Ransomware

- Loss of Valuable data.
- Loss of the organization’s reputation and integrity.
- Loss of the organization’s [sensitive business information](#).
- Disruption in organization operation.
- Financial loss.

## MITRE ATT&CK® Techniques

Tactic	Technique ID	Technique Name
Execution	<a href="#">T1204</a>	User Execution
	<a href="#">T1059</a>	Command and Scripting Interpreter
Defense Evasion	<a href="#">T1497</a>	Virtualization/Sandbox Evasion
	<a href="#">T1027</a>	Software Packing
	<a href="#">T1036</a>	Masquerading
Discovery	<a href="#">T1082</a>	System Information Discovery
	<a href="#">T1083</a>	File and Directory Discovery
	<a href="#">T1518</a>	Security Software Discovery
	<a href="#">T1120</a>	Peripheral Device Discovery
Impact	<a href="#">T1486</a>	Data Encrypted for Impact
Lateral Movement	<a href="#">T1091</a>	Replication Through Removable Media

## Indicator Of Compromise (IOCs)

Indicators	Indicator Type	Description
0c756fc8f34e409650cd910b5e2a3f00	MD5	BianLian
70d1d11e3b295ec6280ab33e7b129c17f40a6d2f	SHA1	Ransomware
eaf5e26c5e73f3db82cd07ea45e4d244ccb3ec3397ab5263a1a74add7bbcb6e2	Sha256	Executable
08e76dd242e64bb31aec09db8464b28f	MD5	BianLian
3f3f62c33030cfd64dba2d4ecb1634a9042ba292	SHA1	Ransomware
1fd07b8d1728e416f897bef4f1471126f9b18ef108eb952f4b75050da22e8e43	Sha256	Executable

Source: <https://blog.cyble.com/2022/08/18/bianlian-new-ransomware-variant-on-the-rise/>