

BianLian: New Ransomware variant on the rise

 blog.cyble.com/2022/08/18/bianlian-new-ransomware-variant-on-the-rise/

August 18, 2022



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.

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.

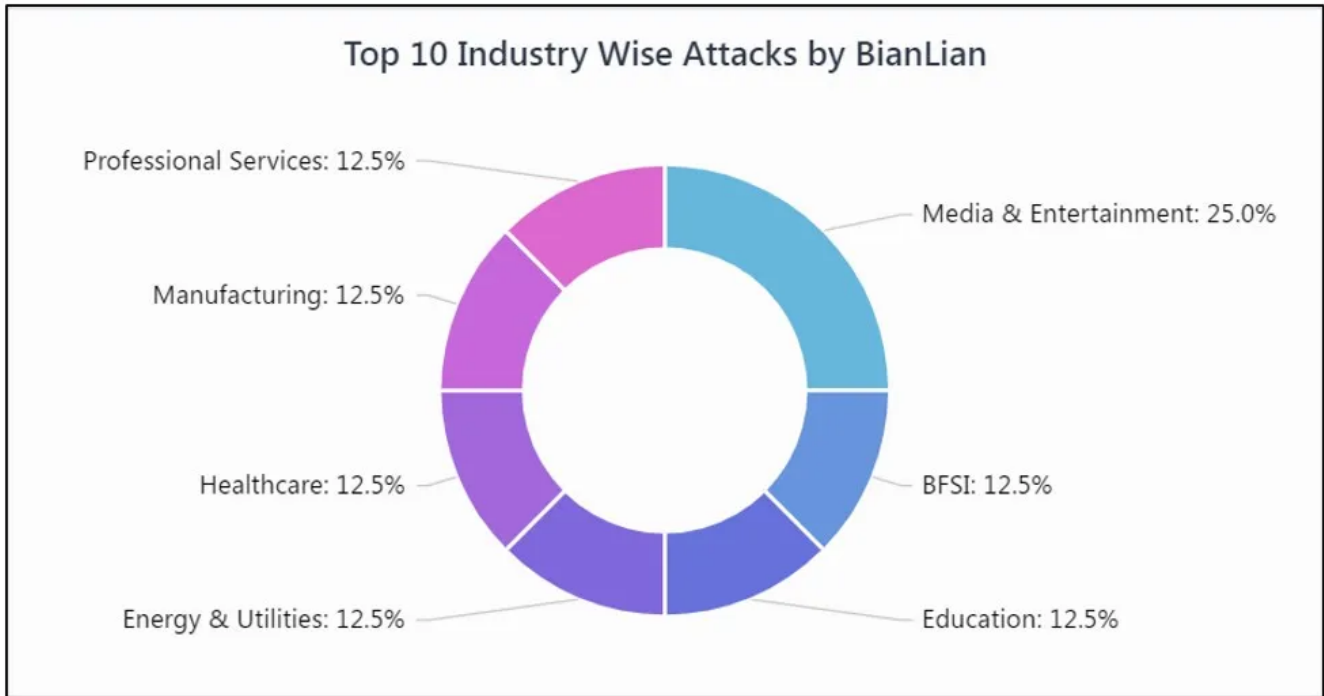


Figure 1 – Industries Targeted by the BianLian Ransomware

Technical Analysis

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

(SHA256), `eaf5e26c5e73f3db82cd07ea45e4d244ccb3ec3397ab5263a1a74add7bbcb6e2`, which is a 64-bit GoLang binary executable.

The unique build ID of the GoLang ransomware is shown below.

```

E:\ymtab
Go build ID: "H40nAXi0HAA8phzv9-cb/qCmr9jSfyS54gBjEKYHI/3NP6oNV505RosziU-nxb/ldC38qRUGilCycasAQgK"
0xpus
0xustH
0xust?
0xustH
  
```

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.

<pre> 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 </pre>	<pre> [rsi]: "MZ" [rsi+8]: "wine_get_version" </pre>
<pre> call rax </pre>	<pre> GetProcAddress </pre>

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	2052	0000000000830FC0	000000C77448F000	00007FF98F520C90	1	Normal	Executive	00000000	00:00:00.0000000	00:00:00.0156250	16:02:13.9907703	33745F6	
44	1640	0000000000830FC0	000000C774507000	00007FF98F70BE24	1	Normal	Suspended	00000000	00:00:00.0156250	00:00:00.0000000	16:02:49.3405246	9009C1	
44	6644	0000000000830FC0	000000C774481000	00007FF98F70BE24	1	Normal	Suspended	00000000	00:00:00.0000000	00:00:00.0156250	16:02:47.6762539	138E46E	
44	1816	0000000000830FC0	000000C7744AF000	00007FF98F70BE24	1	Normal	Suspended	00000000	00:00:00.0781250	00:00:00.0468750	16:01:56.9439795	10D03C33	Main Thread
41	3268	0000000000830FC0	000000C774501000	00007FF98F70BE24	1	Normal	Suspended	00000000	00:00:00.0000000	00:00:00.0000000	16:02:48.9177235	ADC112	
36	8016	0000000000830FC0	000000C7744F7000	00007FF98F70E5D4	1	Normal	Suspended	00000000	00:00:00.0000000	00:00:00.0000000	16:02:48.6920536	19CCCE9	
1	8176	00007FF98F6820E0	000000C774481000	00007FF98F70F7F4	1	Normal	Suspended	00000000	00:00:00.0000000	00:00:00.0156250	16:02:13.9191303	865336	
7	7088	0000000000830FC0	000000C774483000	00007FF98F70F7F4	1	Normal	Suspended	00000000	00:00:00.0000000	00:00:00.0000000	16:02:13.9309926	9833E8	
40	7180	0000000000830FC0	000000C77448D000	00007FF98F70BE24	1	Normal	Suspended	00000000	00:00:00.0000000	00:00:00.0156250	16:02:13.9854559	18A8954	
3	7256	0000000000830FC0	000000C7744F7000	00007FF98F70BE24	1	Normal	Suspended	00000000	00:00:00.0000000	00:00:00.0000000	16:02:48.9128486	64D028	
3	8940	0000000000830FC0	000000C774485000	00007FF98F70BE24	1	Normal	Suspended	00000000	00:00:00.0000000	00:00:00.0000000	16:02:13.9653033	35FD046	
5	7344	0000000000830FC0	000000C774489000	00007FF98F70BE24	1	Normal	Suspended	00000000	00:00:00.0000000	00:00:00.0000000	16:02:13.9663209	58232AB	
46	288	0000000000830FC0	000000C774508000	00007FF98F70BE24	1	Normal	Suspended	00000000	00:00:00.0000000	00:00:00.0000000	16:02:49.3498195	E95368	
48	9160	0000000000830FC0	000000C774488000	00007FF98F70BE24	1	Normal	Suspended	00000000	00:00:00.0156250	00:00:00.0625000	16:02:13.9841106	8597787	
4	7112	0000000000830FC0	000000C774487000	00007FF98F70BE24	1	Normal	Suspended	00000000	00:00:00.0000000	00:00:00.0000000	16:02:13.9655547	6820F83	
9	4844	0000000000830FC0	000000C7744C1000	00007FF98F70BE24	1	Normal	Suspended	00000000	00:00:00.0156250	00:00:00.0468750	16:02:13.9939187	A7968D8	
20	2068	0000000000830FC0	000000C7744C3000	00007FF98F70BE24	1	Normal	Suspended	00000000	00:00:00.0156250	00:00:00.0312500	16:02:13.9974957	3C055FA	
10	2352	0000000000830FC0	000000C77450F000	00007FF98F70BE24	1	Normal	Suspended	00000000	00:00:00.0000000	00:00:00.0000000	16:02:49.3538539	AC2E00	
26	8636	0000000000830FC0	000000C7744E3000	00007FF98F70BE24	1	Normal	Suspended	00000000	00:00:00.0000000	00:00:00.0312500	16:02:48.0819899	C26246	
11	9012	0000000000830FC0	000000C7744C5000	00007FF98F70BE24	1	Normal	Suspended	00000000	00:00:00.0000000	00:00:00.0312500	16:02:14.0030609	10A0E98	
20	2332	0000000000830FC0	000000C774487000	00007FF98F70BE24	1	Normal	Suspended	00000000	00:00:00.0000000	00:00:00.0156250	16:02:47.6878827	DCC4D8	
12	6816	0000000000830FC0	000000C7744C7000	00007FF98F70BE24	1	Normal	Suspended	00000000	00:00:00.0000000	00:00:00.0156250	16:02:44.9971212	4200AEC	
13	4576	0000000000830FC0	000000C7744C9000	00007FF98F70BE24	1	Normal	Suspended	00000000	00:00:00.0000000	00:00:00.0312500	16:02:44.9975468	A93960A	
43	4252	0000000000830FC0	000000C774505000	00007FF98F70BE24	1	Normal	Suspended	00000000	00:00:00.0000000	00:00:00.0000000	16:02:49.1300859	8F5AE4	
10	8932	0000000000830FC0	000000C774488000	00007FF98F70BE24	1	Normal	Suspended	00000000	00:00:00.0000000	00:00:00.0000000	16:02:48.2906070	57816F	
14	4396	0000000000830FC0	000000C7744C8000	00007FF98F70BE24	1	Normal	Suspended	00000000	00:00:00.0000000	00:00:00.0000000	16:02:45.4862380	1E2422	
15	6600	0000000000830FC0	000000C7744CD000	00007FF98F70BE24	1	Normal	Suspended	00000000	00:00:00.0000000	00:00:00.0312500	16:02:45.4869292	2738D05	
16	1752	0000000000830FC0	000000C7744CF000	00007FF98F70BE24	1	Normal	Suspended	00000000	00:00:00.0000000	00:00:00.0312500	16:02:45.4933378	185E227	
37	6794	0000000000830FC0	000000C774483000	00007FF98F70BE24	1	Normal	Suspended	00000000	00:00:00.0156250	00:00:00.0156250	16:02:47.6790081	F8D2C9	
19	6252	0000000000830FC0	000000C7744D5000	00007FF98F70BE24	1	Normal	Suspended	00000000	00:00:00.0000000	00:00:00.0156250	16:02:47.6822014	1ACCF71	
21	340	0000000000830FC0	000000C7744D9000	00007FF98F70BE24	1	Normal	Suspended	00000000	00:00:00.0000000	00:00:00.0156250	16:02:47.7006434	1ED5481	
22	6472	0000000000830FC0	000000C774488000	00007FF98F70BE24	1	Normal	Suspended	00000000	00:00:00.0000000	00:00:00.0000000	16:02:47.7043146	196C951	
23	7700	0000000000830FC0	000000C7744D0000	00007FF98F70BE24	1	Normal	Suspended	00000000	00:00:00.0000000	00:00:00.0156250	16:02:47.7169393	A5CC8	
60	5920	0000000000830FC0	000000C774527000	00007FF98F70BE24	1	Normal	Suspended	00000000	00:00:00.0000000	00:00:00.0000000	16:02:49.6031775	D02D1	
24	5328	0000000000830FC0	000000C7744DF000	00007FF98F70BE24	1	Normal	Suspended	00000000	00:00:00.0000000	00:00:00.0156250	16:02:47.8763873	CF55EE	
37	3804	0000000000830FC0	000000C7744F9000	00007FF98F70BE24	1	Normal	Suspended	00000000	00:00:00.0000000	00:00:00.0000000	16:02:48.6921065	808C7A	
32	7352	0000000000830FC0	000000C7744EF000	00007FF98F70BE24	1	Normal	Suspended	00000000	00:00:00.0000000	00:00:00.0312500	16:02:48.3012354	193E16D	
25	6904	0000000000830FC0	000000C7744E1000	00007FF98F70BE24	1	Normal	Suspended	00000000	00:00:00.0000000	00:00:00.0000000	16:02:47.8772729	51905E	
27	3300	0000000000830FC0	000000C7744E5000	00007FF98F70BE24	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,rcx
0000: 6648:0F6ECA      movq xmm1,rdx
0000: 6649:0F6ED0      movq xmm2,r8
0000: 6649:0F6ED9      movq xmm3,r9
0000: FFDD            call rax
0000: 48:81C4 50010000 add rsp,150
0000: 59              pop rcx
0000: 48:8941 18      mov qword ptr ds:[rcx+18],rax
    
```

rdx: "MZ锈"

writeFile


```

.rax=1
.txt:0000000000830D1C_new_one.exe:$60D1C #6031C
    
```

Addr:	Hex	ASCII
000000	59 6F 75 72 20 6E 65 74 77 6F 72 68 20 73 79 73	Your network systems were attacked and encrypted.
000000	74 65 6D 73 20 77 65 72 65 20 61 74 74 61 63 68	Contact us in order to restore your data. Don't make any changes in your file structure: touch no files, don't try to recover by yourself, that may lead to it's complete loss.... To contact us you have to download "tox" malware: https://qt0x.github.io/
000000	6E 64 20 61 6E 64 20 65 6E 63 72 79 70 74 65 64	
000000	2E 20 43 6F 6E 74 20 75 73 20 69 6E 20	
000000	6F 72 64 65 72 20 74 6F 20 72 65 73 74 6F 72 65	
000000	20 79 6F 75 72 20 64 61 74 61 2E 20 44 6F 6E 67	
000000	74 20 61 68 65 20 61 6E 79 72 20 66 69 6C 65 20	
000000	65 73 20 69 6E 20 79 6F 77 72 20 66 69 6C 65 20	
000000	73 74 72 75 63 74 75 72 65 3A 20 74 6F 75 63 68	
000000	20 6E 6F 20 66 69 6C 65 73 2C 20 64 6F 6E 27 74	
000000	20 74 72 79 20 74 6F 20 72 65 63 6F 76 65 72 20	
000000	62 79 20 79 6F 75 72 73 65 6C 66 2C 20 74 68 61	
000000	74 20 6D 61 79 20 6C 65 61 64 20 74 6F 20 69 74	
000000	27 73 20 63 6F 6D 70 6C 65 64 65 20 6C 6F 73 73	
000000	2E 0D 0A 0D 0A 54 6F 20 63 6F 6E 74 61 63 74 20	
000000	75 73 20 79 6F 75 20 68 61 76 65 20 74 6F 20 64	
000000	6F 77 6E 6C 6F 61 64 20 22 74 6F 78 22 20 6D 65	
000000	73 73 65 6E 67 72 3A 20 68 74 74 70 73 3A 2F	
000000	2F 71 74 6F 78 2E 67 69 74 68 75 62 2E 69 6F 2F	

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.

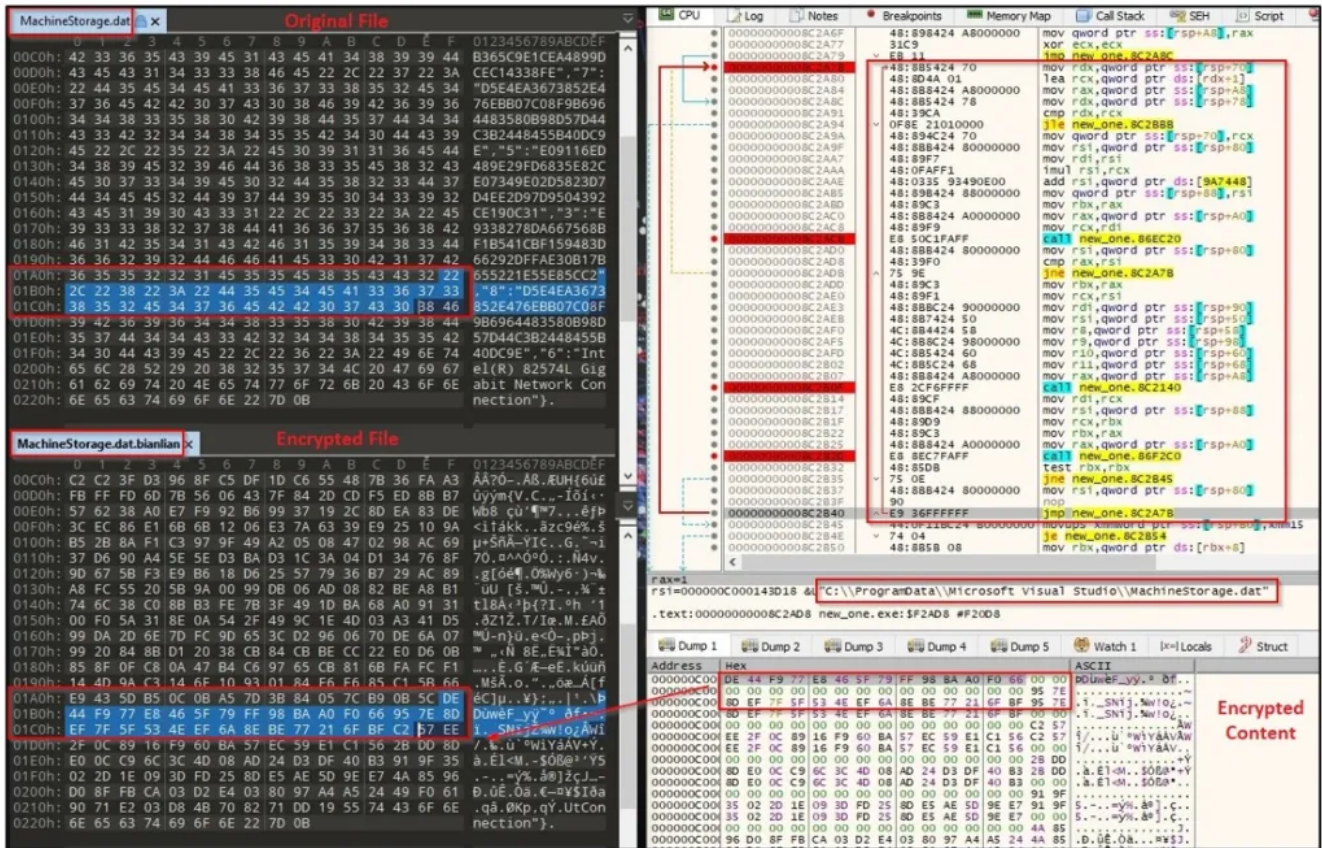


Figure 7 – Encryption routine and Original/Encrypted file content

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.

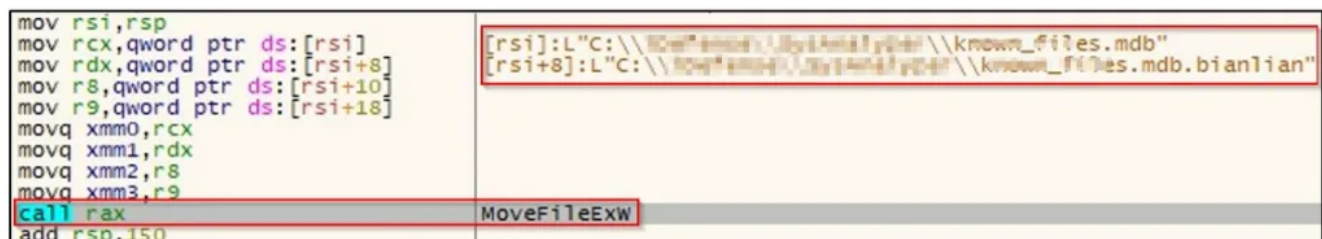


Figure 8 – MoveFileExW() API

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\\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
...py.bianlian	BIANLIAN File	4 KB
...py.bianlian	BIANLIAN File	4 KB
...py.bianlian	BIANLIAN File	3 KB
...py.bianlian	BIANLIAN File	3 KB
...py.bianlian	BIANLIAN File	5 KB
...c.bianlian	BIANLIAN File	4 KB
...o.bianlian	BIANLIAN File	4 KB
...py.bianlian	BIANLIAN File	103 KB
...c.bianlian	BIANLIAN File	56 KB
...o.bianlian	BIANLIAN File	56 KB
Look at this instruction.txt	Text Document	1 KB
...py.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.

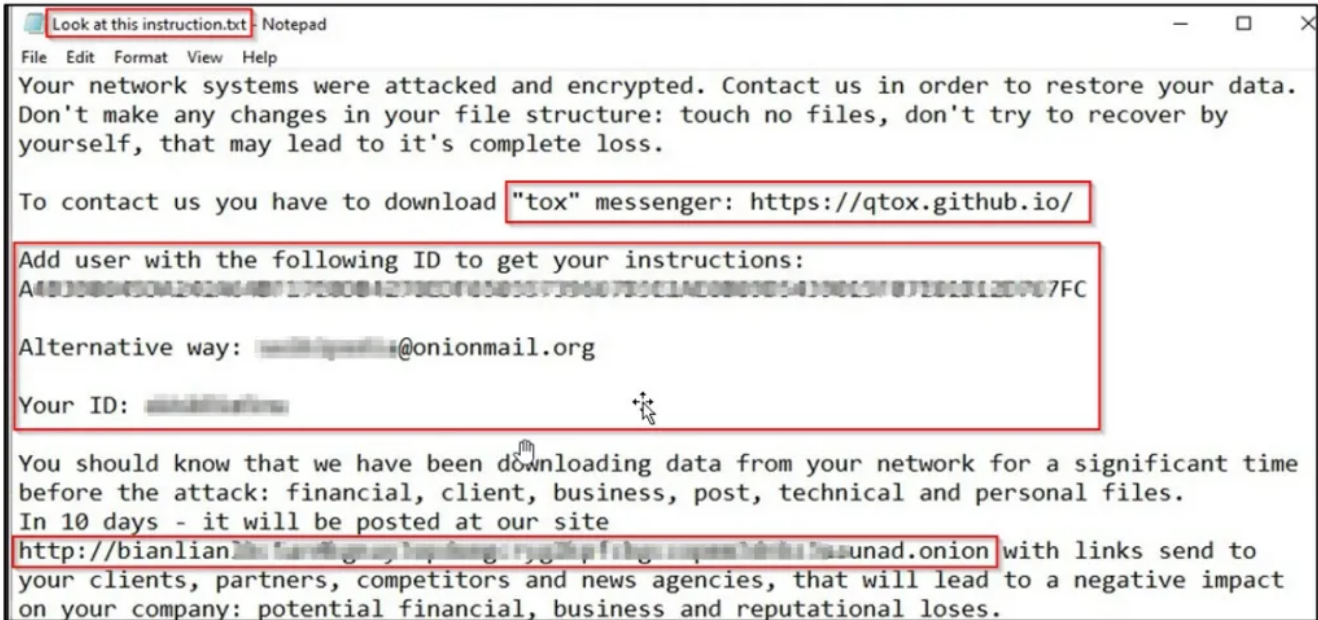


Figure 10 – Ransom note

The figure below shows the BianLian ransomware Onion leak home page and the affected company's extortion objects.

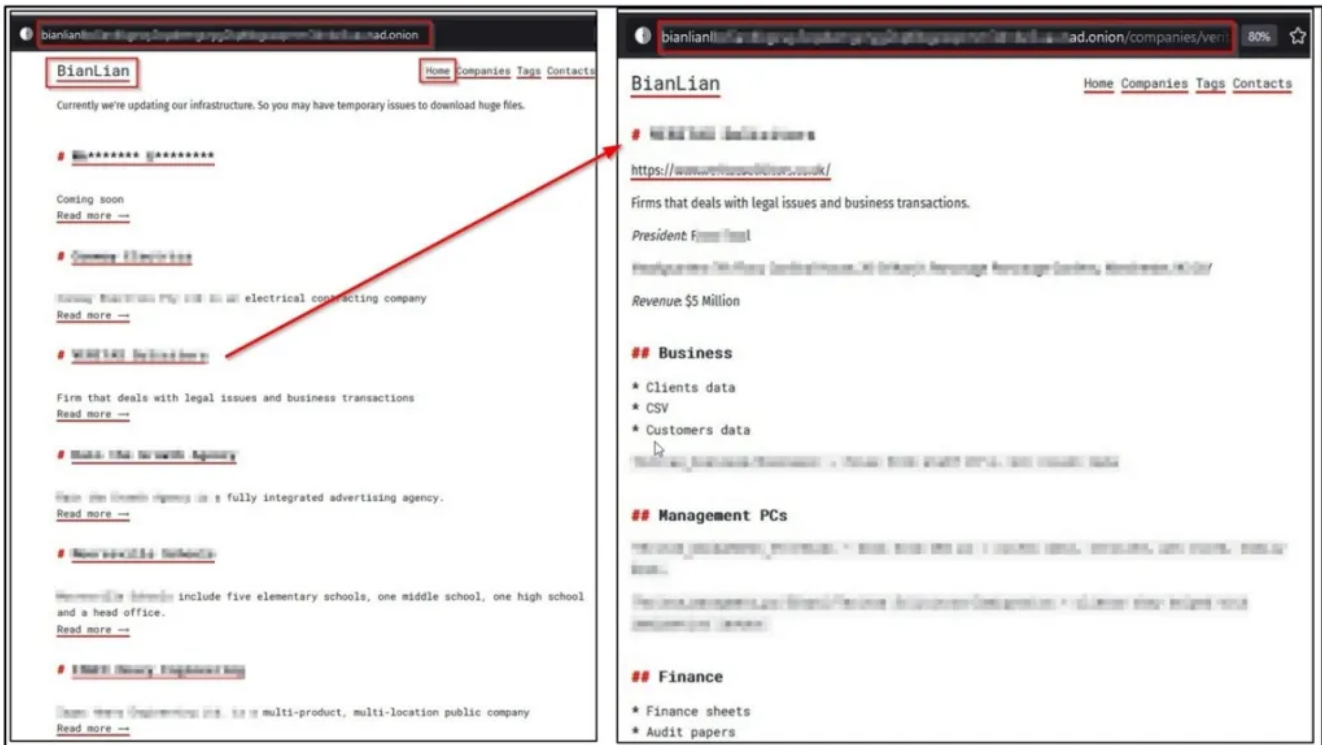


Figure 11 – BianLian Leak site home page

The BianLian Leak site contains the list of all companies affected by the ransomware and the TA's contact details for ransomware data recovery.

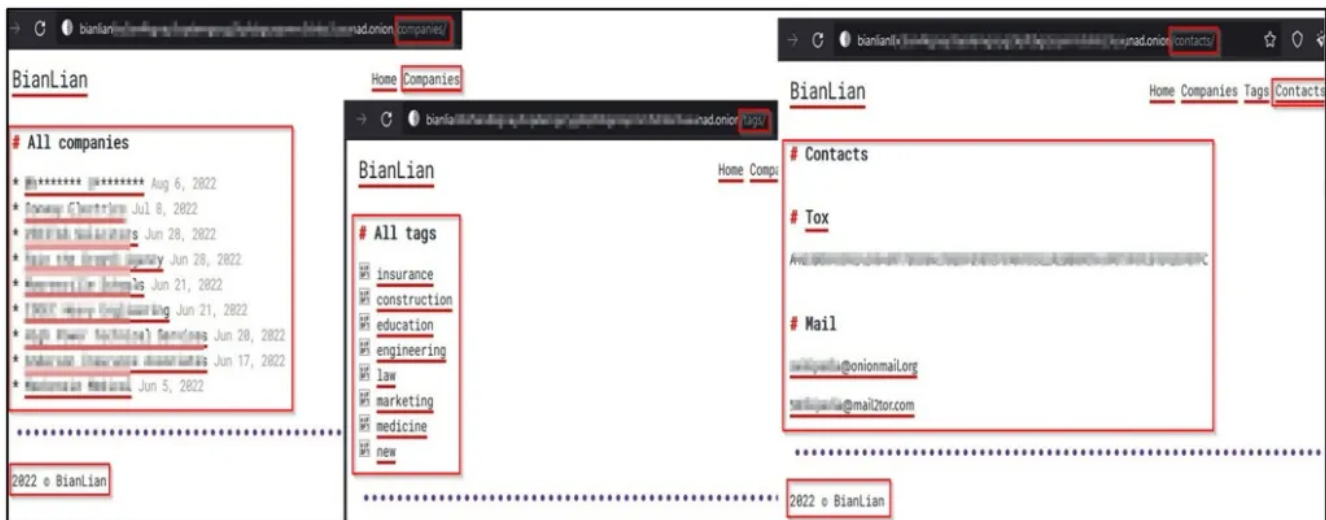


Figure 12 – BianLian Leak site affected companies list & TAs contact details

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	T1204 T1059	User Execution Command and Scripting Interpreter
Defense Evasion	T1497 T1027 T1036	Virtualization/Sandbox Evasion Software Packing Masquerading
Discovery	T1082 T1083 T1518 T1120	System Information Discovery File and Directory Discovery Security Software Discovery Peripheral Device Discovery
Impact	T1486	Data Encrypted for Impact
Lateral Movement	T1091	Replication Through Removable Media

Indicator Of Compromise (IOCs)

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