BianLian: New Ransomware variant on the rise

8/18/2022

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.

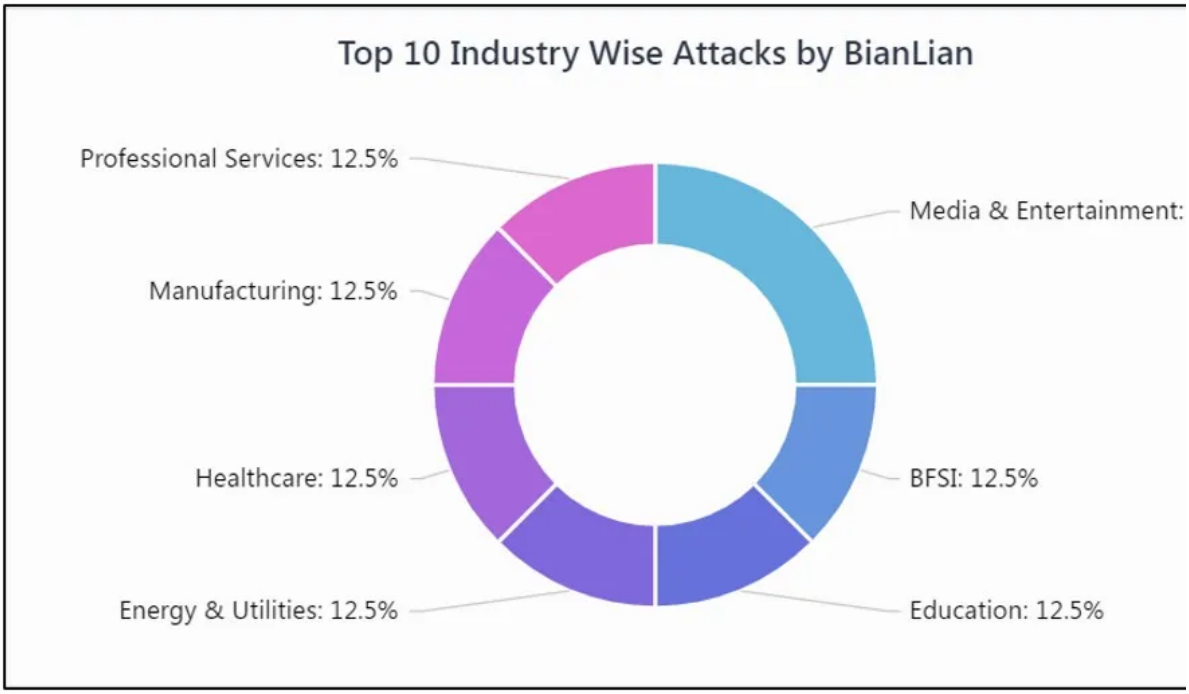


Figure 1 – Industries Targeted by the BianLian Ransomware

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.

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.

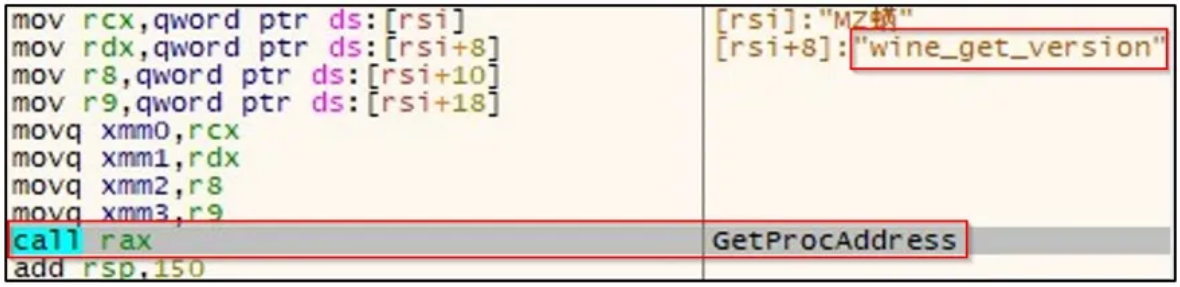
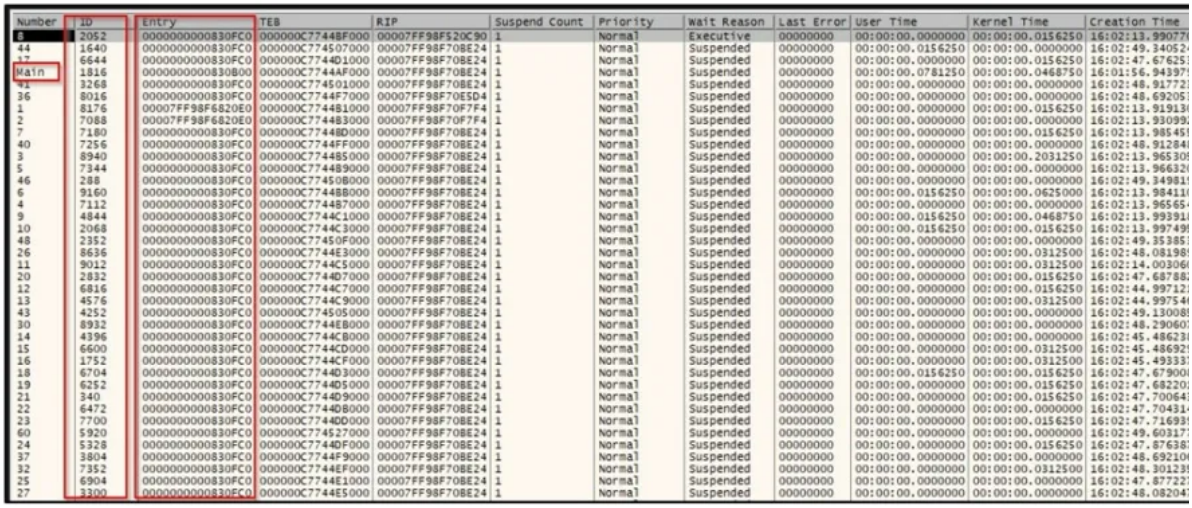


Figure 3 – Anti-analysis Technique

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
8	2052	00000000830FC0	000000C7744BF000	00007FF98F520C90	1	Normal	Executive	00000000	00:00:00.0000000	00:00:00.0156250	16:02:13.990770
44	1640	00000000830FC0	000000C774507000	00007FF98F70BE24	1	Normal	Suspended	00000000	00:00:00.0156250	00:00:00.0000000	16:02:49.340524
17	6644	00000000830FC0	000000C7744D1000	00007FF98F70BE24	1	Normal	Suspended	00000000	00:00:00.0000000	00:00:00.0156250	16:02:47.676253
Main	1816	00000000830B00	000000C7744AF000	00007FF98F70BE24	1	Normal	Suspended	00000000	00:00:00.0781250	00:00:00.0468750	16:01:56.943975
41	3268	00000000830FC0	000000C774501000	00007FF98F70BE24	1	Normal	Suspended	00000000	00:00:00.0000000	00:00:00.0000000	16:02:48.917723
36	8016	00000000830FC0	000000C7744F7000	00007FF98F70E5D4	1	Normal	Suspended	00000000	00:00:00.0000000	00:00:00.0000000	16:02:48.692053
1	8176	00007FF98F6820E0	000000C7744B1000	00007FF98F70F7F4	1	Normal	Suspended	00000000	00:00:00.0000000	00:00:00.0156250	16:02:13.919130
2	7088	00007FF98F6820E0	000000C7744B3000	00007FF98F70F7F4	1	Normal	Suspended	00000000	00:00:00.0000000	00:00:00.0000000	16:02:13.930992
7	7180	00000000830FC0	000000C7744BD000	00007FF98F70BE24	1	Normal	Suspended	00000000	00:00:00.0000000	00:00:00.0156250	16:02:13.985455
40	7256	00000000830FC0	000000C7744FF000	00007FF98F70BE24	1	Normal	Suspended	00000000	00:00:00.0000000	00:00:00.0000000	16:02:48.912846
3	8940	00000000830FC0	000000C7744B5000	00007FF98F70BE24	1	Normal	Suspended	00000000	00:00:00.0000000	00:00:00.2031250	16:02:13.965305
5	7344	00000000830FC0	000000C7744B9000	00007FF98F70BE24	1	Normal	Suspended	00000000	00:00:00.0000000	00:00:00.0000000	16:02:13.966320
46	288	00000000830FC0	000000C7745080000	00007FF98F70BE24	1	Normal	Suspended	00000000	00:00:00.0000000	00:00:00.0000000	16:02:49.349815
6	9160	00000000830FC0	000000C7744BB000	00007FF98F70BE24	1	Normal	Suspended	00000000	00:00:00.0156250	00:00:00.0625000	16:02:13.984110
4	7112	00000000830FC0	000000C7744B7000	00007FF98F70BE24	1	Normal	Suspended	00000000	00:00:00.0000000	00:00:00.0000000	16:02:13.965654
9	4844	00000000830FC0	000000C7744C1000	00007FF98F70BE24	1	Normal	Suspended	00000000	00:00:00.0156250	00:00:00.0468750	16:02:13.993918
10	2068	00000000830FC0	000000C7744C3000	00007FF98F70BE24	1	Normal	Suspended	00000000	00:00:00.0156250	00:00:00.0156250	16:02:13.997495
48	2352	00000000830FC0	000000C7745080F000	00007FF98F70BE24	1	Normal	Suspended	00000000	00:00:00.0000000	00:00:00.0000000	16:02:49.353851
26	8636	00000000830FC0	000000C7744E3000	00007FF98F70BE24	1	Normal	Suspended	00000000	00:00:00.0000000	00:00:00.0312500	16:02:48.081985
11	9012	00000000830FC0	000000C7744C5000	00007FF98F70BE24	1	Normal	Suspended	00000000	00:00:00.0000000	00:00:00.0312500	16:02:14.003060
20	2832	00000000830FC0	000000C7744D7000	00007FF98F70BE24	1	Normal	Suspended	00000000	00:00:00.0000000	00:00:00.0156250	16:02:47.687862
12	6816	00000000830FC0	000000C7744C7000	00007FF98F70BE24	1	Normal	Suspended	00000000	00:00:00.0000000	00:00:00.0156250	16:02:44.997123
13	4576	00000000830FC0	000000C7744C9000	00007FF98F70BE24	1	Normal	Suspended	00000000	00:00:00.0000000	00:00:00.0312500	16:02:44.997546
43	4252	00000000830FC0	000000C774505000	00007FF98F70BE24	1	Normal	Suspended	00000000	00:00:00.0000000	00:00:00.0000000	16:02:49.130085
30	8932	00000000830FC0	000000C7744EB000	00007FF98F70BE24	1	Normal	Suspended	00000000	00:00:00.0000000	00:00:00.0000000	16:02:48.290603
14	4396	00000000830FC0	000000C7744CB000	00007FF98F70BE24	1	Normal	Suspended	00000000	00:00:00.0000000	00:00:00.0000000	16:02:45.486238
15	6600	00000000830FC0	000000C7744CD000	00007FF98F70BE24	1	Normal	Suspended	00000000	00:00:00.0000000	00:00:00.0312500	16:02:45.486929
16	1752	00000000830FC0	000000C7744CF000	00007FF98F70BE24	1	Normal	Suspended	00000000	00:00:00.0000000	00:00:00.0312500	16:02:45.493337
18	6704	00000000830FC0	000000C7744D3000	00007FF98F70BE24	1	Normal	Suspended	00000000	00:00:00.0156250	00:00:00.0156250	16:02:47.679000
19	6252	00000000830FC0	000000C7744D5000	00007FF98F70BE24	1	Normal	Suspended	00000000	00:00:00.0000000	00:00:00.0156250	16:02:47.682202
21	340	00000000830FC0	000000C7744D9000	00007FF98F70BE24	1	Normal	Suspended	00000000	00:00:00.0000000	00:00:00.0156250	16:02:47.700643
22	6472	00000000830FC0	000000C7744DB000	00007FF98F70BE24	1	Normal	Suspended	00000000	00:00:00.0000000	00:00:00.0000000	16:02:47.704314
23	7700	00000000830FC0	000000C7744DD000	00007FF98F70BE24	1	Normal	Suspended	00000000	00:00:00.0000000	00:00:00.0156250	16:02:47.716935
60	5920	00000000830FC0	000000C774527000	00007FF98F70BE24	1	Normal	Suspended	00000000	00:00:00.0000000	00:00:00.0000000	16:02:49.603171
24	5328	00000000830FC0	000000C7744DF000	00007FF98F70BE24	1	Normal	Suspended	00000000	00:00:00.0000000	00:00:00.0156250	16:02:47.876382
37	3804	00000000830FC0	000000C7744F9000	00007FF98F70BE24	1	Normal	Suspended	00000000	00:00:00.0000000	00:00:00.0000000	16:02:48.692106
32	7352	00000000830FC0	000000C7744EF000	00007FF98F70BE24	1	Normal	Suspended	00000000	00:00:00.0000000	00:00:00.0312500	16:02:48.301239
25	6904	00000000830FC0	000000C7744E1000	00007FF98F70BE24	1	Normal	Suspended	00000000	00:00:00.0000000	00:00:00.0000000	16:02:47.877223
27	3300	00000000830FC0	000000C7744E5000	00007FF98F70BE24	1	Normal	Suspended	00000000	00:00:00.0000000	00:00:00.0000000	16:02:48.082047

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.

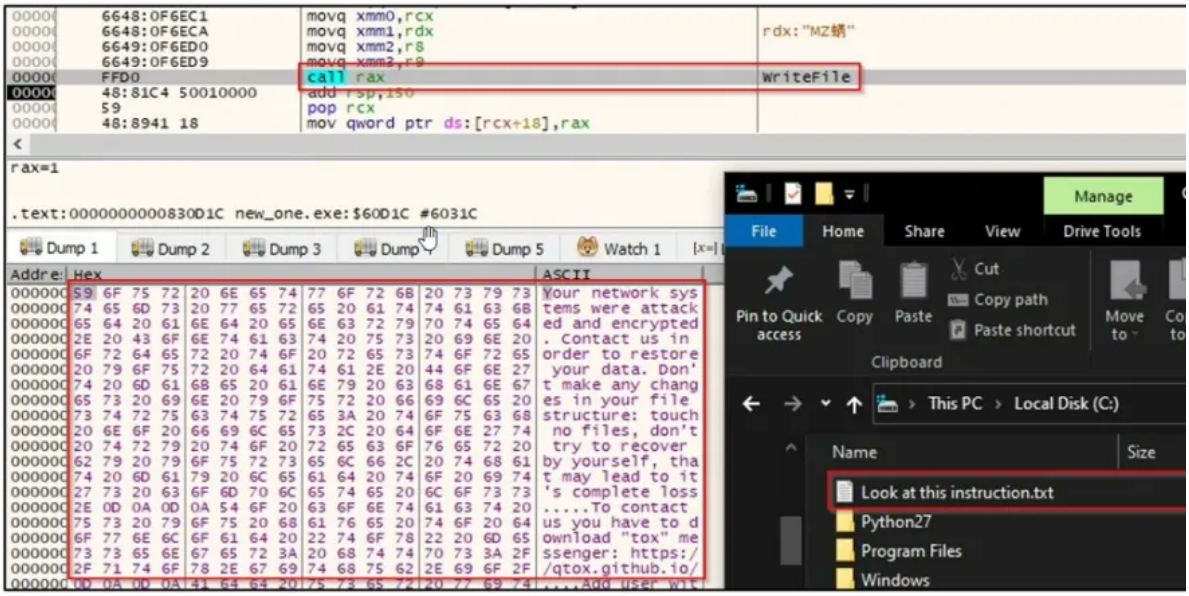


Figure 5 – Malware Writing Ransom Notes

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 usesGoLang Packages such as “*crypto/cipher,” “crypto/aes” and “crypto/rsa”* for file encryption on the victim machine.

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.

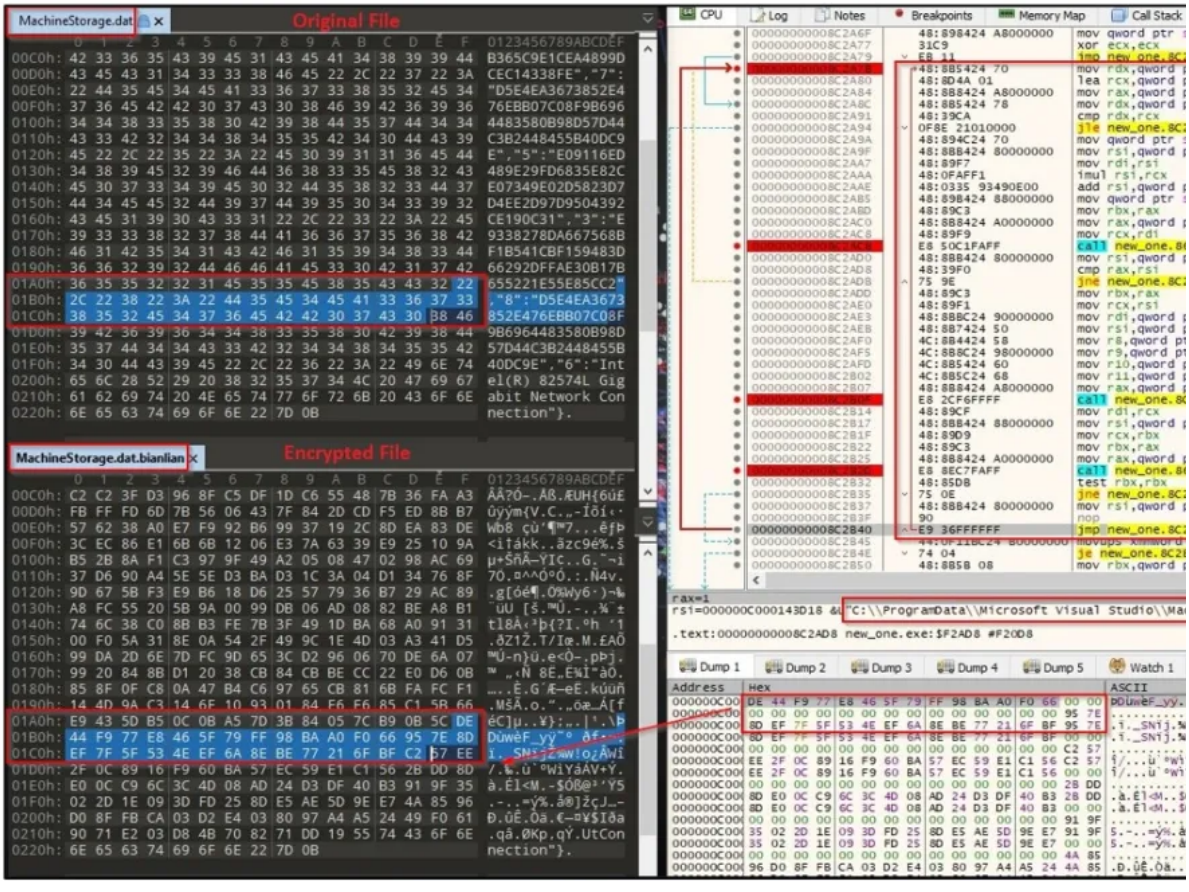


Figure 7 – Encryption routine and Original/Encrypted file content

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.

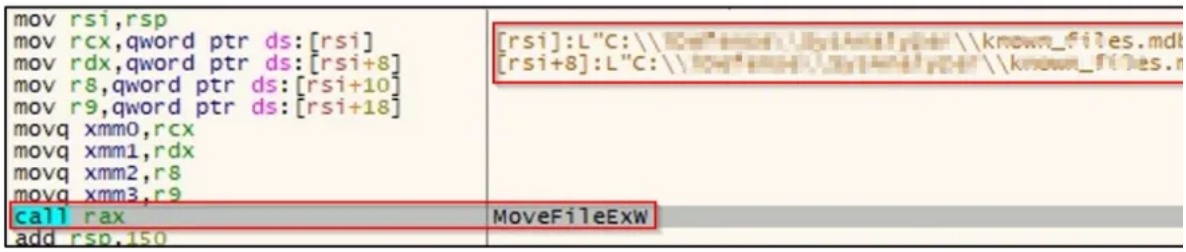


Figure 8 – MoveFileExW() API

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.

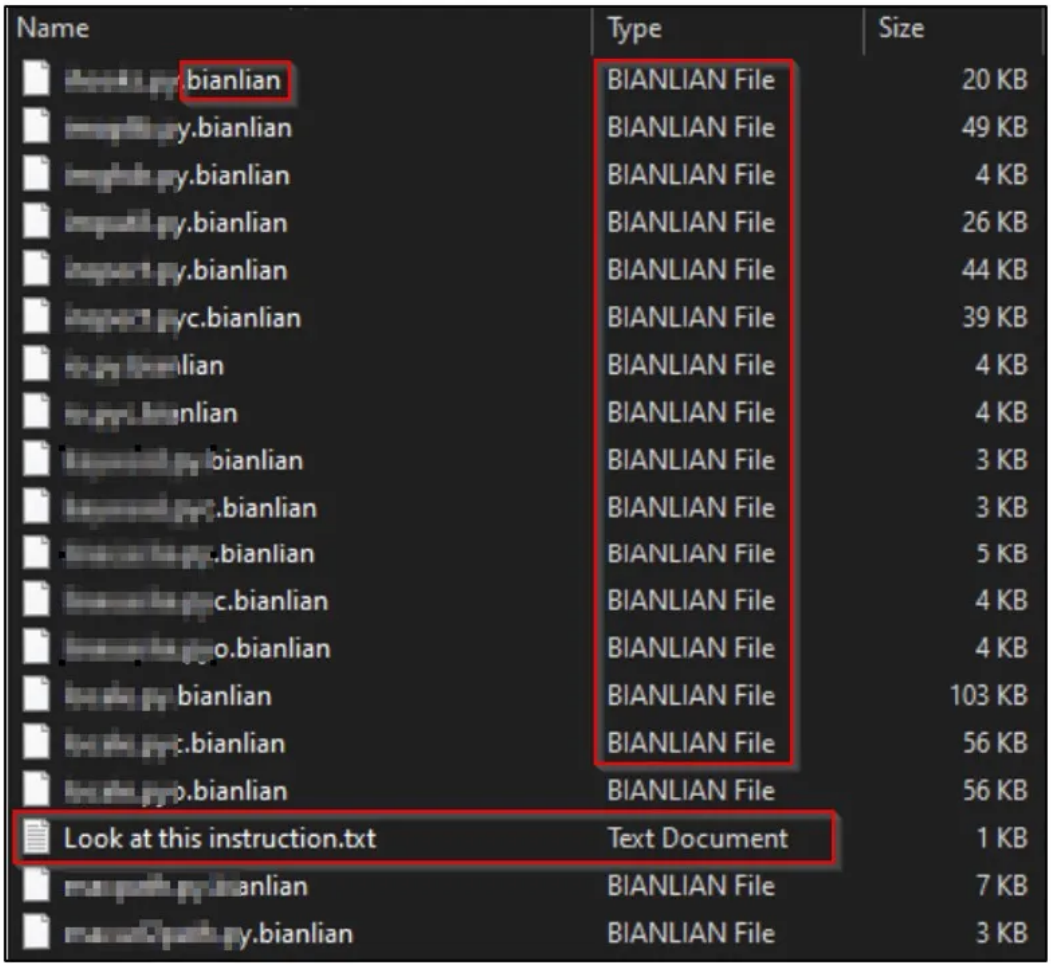


Figure 9 – Files encrypted by BianLian Ransomware

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.

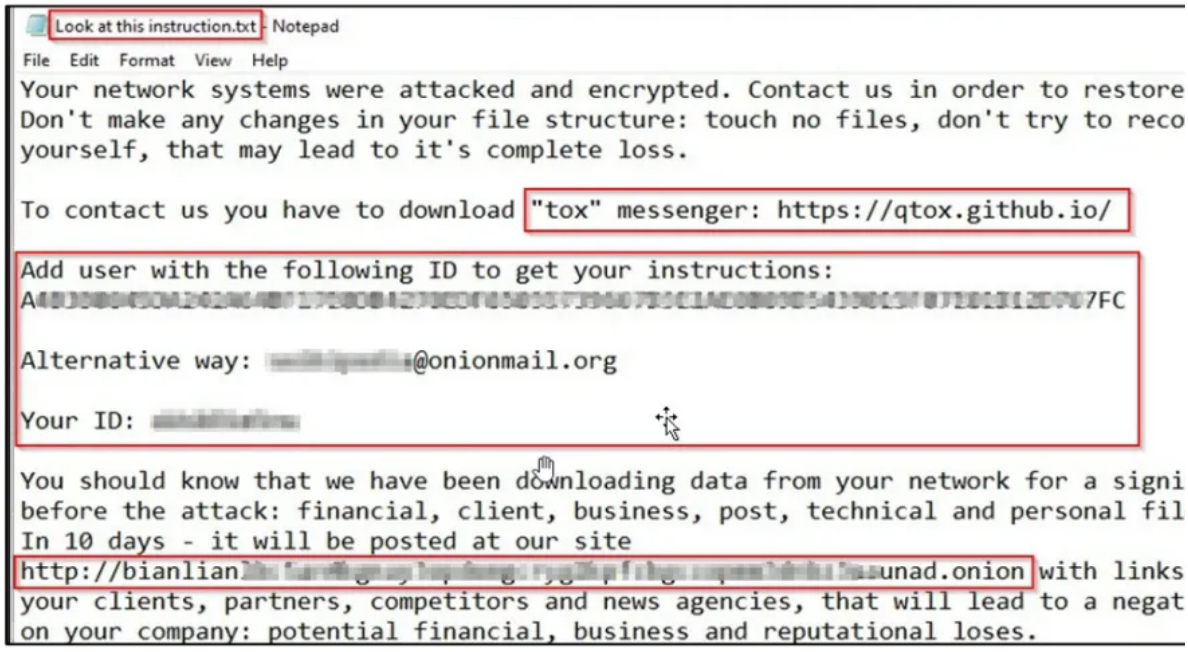


Figure 10 – Ransom note

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

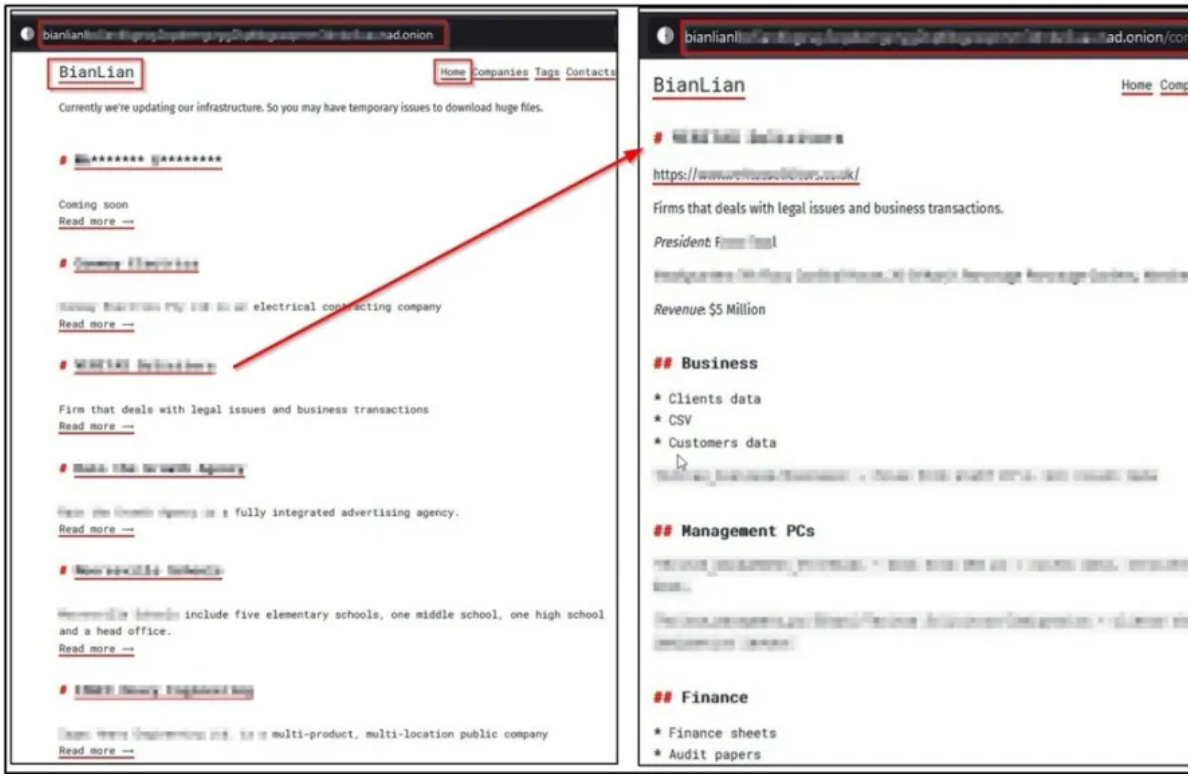


Figure 11 – BianLian Leak site home page

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	User Execution
	T1059	Command and Scripting Interpreter
Defense Evasion	T1497	Virtualization/Sandbox Evasion
	T1027	Software Packing
	T1036	Masquerading
Discovery	T1082	System Information Discovery

	T1083	File and Directory Discovery
	T1518	Security Software Discovery
	T1120	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	MD5	BianLian
70d1d11e3b295ec6280ab33e7b129c17f40a6d2f	SHA1	Ransomware
eaf5e26c5e73f3db82cd07ea45e4d244ccb3ec3397ab5263a1a74add7bbcb6e2	Sha256	Executable
08e76dd242e64bb31aec09db8464b28f	MD5	BianLian
3f3f62c33030cfd64dba2d4ecb1634a9042ba292	SHA1	Ransomware
1fd07b8d1728e416f897bef4f1471126f9b18ef108eb952f4b75050da22e8e43	Sha256	Executable