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, <u>Stealer</u>, etc.

During our routine threat-hunting exercise, we came across a <u>Twitter</u> 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.

Burymtab	
Go build ID: "H40nAXi0HAA8phzv9-cb/qCmr9jSfyS54gBjEKYHI/3NP6oNV505RosziU-nxb/ldC38qRUGilCycasAQ	аК''
Bepu a	
Huuto	
oh.liff	
050H9	

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.

mov rcx, qword ptr ds:[rs1]	[rs1]: "MZTR"
mov rdx, gword ptr ds: [rsi+8]	[rsi+8]: "wine_get_version"
mov r8, gword ptr ds: [rsi+10]	
mov r9, qword ptr ds: [rsi+18]	
movq xmm0,rcx	
movq xmm1,rdx	
movq xmm2,r8	
movg xmm3,r9	
call rax	GetProcAddress
add rsp,150	

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	10	Entry	TEB	RIP	Suspend Count	Priority	Wait Reason	Last Error	User Time	Kernel Time	Creation Time	CPU Cycles	Name
	2052	000000000830500	0000000774485000	0000755985520590	1	Normal	Executive	00000000	00:00:00.0000000	00:00:00.0156250	16:02:12.9907702	3374556	
44	1640	0000000000830EC0	0000000774507000	00007EE98E708E24	1	Normal	Suspended	00000000	00:00:00.0156250	00:00:00.0000000	16:02:49.3405246	900901	
17	6644	0000000000830EC0	00000000774401000	00007FE98E708E24	1	Normal	Suspended	00000000	00:00:00.0000000	00:00:00.0156250	16:02:47.6762539	138F46F	
Main	1816	000000000830800	000000C7744AE000	00007FF98F708F24	1	Normal	Suspended	00000000	00:00:00.0781250	00:00:00.0468750	16:01:56.9439795	10603033	Main Thread
	3268	000000000830FC0	000000C774501000	00007FF98F708F24	1	Normal	Suspended	00000000	00:00:00.0000000	00:00:00.0000000	16:02:48.9177235	ADC112	
36	8016	000000000830FC0	000000C7744F7000	00007FF98F70E5D4	1	Normal	Suspended	00000000	00:00:00.0000000	00:00:00.0000000	16:02:48.6920536	19CCEE9	
1	8176	00007FF98F6820E0	000000C7744B1000	00007FF98F70F7F4	1	Normal	Suspended	00000000	00:00:00.0000000	00:00:00.0156250	16:02:13.9191303	865336	
2	7088	00007FF98F6820E0	000000C7744B3000	00007FF98F70F7F4	1	Normal	Suspended	00000000	00:00:00.0000000	00:00:00.0000000	16:02:13.9309926	9B33E8	
7	7180	000000000830FC0	000000C7744ED000	00007FF98F70BE24	1	Normal	Suspended	00000000	00:00:00,0000000	00:00:00.0156250	16:02:13.9854559	1848954	
40	7256	000000000830FC0	000000C7744FF000	00007FF98F70BE24	1	Normal	Suspended	00000000	00:00:00.0000000	00:00:00.0000000	16:02:48.9128486	64D028	
3	8940	000000000830FC0	000000C774485000	00007FF98F70BE24	1	Normal	Suspended	00000000	00:00:00.0000000	00:00:00.2031250	16:02:13.9653053	35FDCA6	
5	7344	000000000830FC0	000000C7744B9000	00007FF98F70BE24	1	Normal	Suspended	00000000	00:00:00.0000000	00:00:00.0000000	16:02:13.9663209	58223AB	
46	288	000000000830FC0	000000C77450B000	00007FF98F70BE24	1	Normal	Suspended	00000000	00:00:00.0000000	00:00:00.0000000	16:02:49.3498195	E9536E	
6	9160	000000000830FC0	000000C7744BB000	00007FF98F70BE24	1	Normal	Suspended	00000000	00:00:00.0156250	00:00:00.0625000	16:02:13.9841106	8597787	
4	7112	000000000830FC0	000000C7744B7000	00007FF98F70BE24	1	Normal	Suspended	00000000	00:00:00.0000000	00:00:00.0000000	16:02:13.9656547	682DF83	
9	4844	000000000830FC0	000000C7744C1000	00007FF98F70BE24	1	Normal	Suspended	00000000	00:00:00.0156250	00:00:00.0468750	16:02:13.9939187	A79681D	
10	2068	000000000830FC0	000000C7744C3000	00007FF98F70BE24	1	Norma1	Suspended	00000000	00:00:00.0156250	00:00:00.0156250	16:02:13.9974957	3CD55FA	
48	2352	000000000830FC0	000000C77450F000	00007FF98F70BE24	1	Normal	Suspended	00000000	00:00:00.0000000	00:00:00.000000	16:02:49.3538539	AC2E00	
26	8636	000000000830FC0	000000C7744E3000	00007FF98F70BE24	1	Normal	Suspended	00000000	00:00:00.0000000	00:00:00.0312500	16:02:48.0819899	C26246	
11	9012	000000000830FC0	000000C7744C5000	00007FF98F70BE24	1	Normal	Suspended	00000000	00:00:00.0000000	00:00:00.0312500	16:02:14.0030609	10A0E9B	
20	2832	000000000830FC0	000000C7744D7000	00007FF98F70BE24	1	Normal	Suspended	00000000	00:00:00.0000000	00:00:00.0156250	16:02:47.6878827	DCCAD8	
12	6816	000000000830FC0	000000C7744C7000	00007FF98F708E24	1	Normal	Suspended	00000000	00:00:00.0000000	00:00:00.0156250	16:02:44.9971212	4200AEC	
13	4576	000000000830FC0	000000C7744C9000	00007FF98F70BE24	1	Normal	Suspended	00000000	00:00:00.0000000	00:00:00.0312500	16:02:44.9975468	A93960A	
43	4252	000000000830FC0	000000C774505000	00007FF98F70BE24	1	Normal	Suspended	00000000	00:00:00.000000	00:00:00.000000	16:02:49.1300859	8F5AE4	
30	8932	000000000830FC0	000000C7744EB000	00007FF98F70BE24	1	Normal	Suspended	00000000	00:00:00.000000	00:00:00.000000	16:02:48.2906070	57816F	
14	4396	00000000830FC0	000000C7744CB000	00007FF98F70BE24	1	Normal	Suspended	00000000	00:00:00.000000	00:00:00.000000	16:02:45.4862380	1CE2422	
15	6600	000000000830FC0	000000C7744CD000	00007FF98F708E24	1	Normal	suspended	00000000	00:00:00.000000	00:00:00.0312500	16:02:45.4869292	2738605	
16	1752	000000000830FC0	00000007744CF000	00007FF98F708E24	1	Normal	Suspended	00000000	00:00:00.0000000	00:00:00.0312500	16:02:45.4933378	1856227	
18	6/04	000000000830FC0	0000000774403000	00007FF98F708E24	1	Normal	Suspended	00000000	00:00:00.0156250	00:00:00.0156250	16:02:47.6790081	F802C9	
19	6252	000000000830FC0	000000C7744D5000	00007FF98F708E24	1	Normal	Suspended	00000000	00:00:00.000000	00:00:00.0156250	16:02:47.6822014	1ACCFF1	
21	540	000000000830FC0	0000000774409000	00007FF98F708E24	1	Normal	Suspended	00000000	00:00:00.0000000	00:00:00.0156250	16:02:47.7006434	1605481	
22	64/2	000000000830FC0	00000000774408000	00007FF98F708E24	1	Normal	Suspended	00000000	00:00:00.0000000	00:00:00.0000000	16:02:47.7043146	1960951	
23	7700	000000000000000000000000000000000000000	0000000774400000	00007FF98F708E24	1	Normal	Suspended	00000000	00:00:00.0000000	00:00:00.0156250	16:02:4/./169595	ASCCC8	
24	5320	000000000000000000000000000000000000000	0000000774527000	00007FF38F708E24	1	Normal	Suspended	000000000	00.00.00.0000000	00100100.0000000	10.02.43.6031//5	CEEFEE	
27	3328	000000000000000000000000000000000000000	000000077440F000	00007755985708524	1	Normal	Suspended	000000000	00100100.0000000	00:00:00.0156250	16:02:4/.8/658/5	ROBCZA	
32	7363	000000000000000000000000000000000000000	00000007744F9000	00007FF98F708E24	1	Normal	Suspended	000000000	00:00:00.00.0000000	00100100.00000000	16:02:48 2012264	1035160	
25	6904	000000000000000000000000000000000000000	00000007744EF000	0000725985708524	1	Normal	Suspended	000000000	00:00:00.00.0000000	00:00:00.0312500	16:02:40.3012354	5190EE	
37	2200	000000000000000000000000000000000000000	0000000774461000	0000755985708534	1	Normal	Suspended	00000000	00100100.0000000	00100100.0000000	16:03:48 0830478	021520	
61	2200	COUNTRACTORSUFCO	000000L/744E5000	0000/FF38F/08E24	*	NUT TRA	suspended	000000000	00100100100000000	00.00.00.0000000	10:02:40.08204/8	031130	

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.

00000 00000 00000 00000	6648:0F6EC1 6648:0F6ECA 6649:0F6ED0 6649:0F6ED9 FFD0 48:81C4 50010000	movq xmm0,rcx movq xmm1,rdx movq xmm2,rs movq xmm2,rs call rax	rdx:"MZ鳞" WriteFile	
00000	59 48:8941 18	pop rcx mov gword ptr ds:[rcx+18].rax		
<		and divid by and and the set		
rax=1 .text:000	0000000830D1C new_one	e.exe:\$6001C #6031C	Eile Home Share View Drive Tools	
Dump 1	1 Dump 2 Dum	p 3 📖 Dump 🖓 📖 Dump 5 🧐 Watch 1 🛙 🕬		
Addr e: He: 000000 59 000000 74 000000 65 000000 2E 000000 6F 000000 20	X 6F 75 72 20 6E 65 74 65 6D 73 20 77 65 72 64 20 61 6E 64 20 65 20 43 6F 6E 74 61 63 72 64 65 72 20 74 6F 79 6F 75 72 20 64 61	ASCII 77 GF 72 GB 20 73 73 73 Your network sys 65 20 61 74 74 61 63 68 tems were attack 6E 63 72 79 70 74 65 64 ed and encrypted 74 20 75 73 20 69 6E 20. Contact us in 20 72 65 73 74 6F 72 65 order to restore 74 61 2E 20 44 6F 6E 27 your data. Don'	Image: Second system Image: Second system <td>Lename</td>	L ename
000000 74 000000 65 000000 73	20 6D 61 6B 65 20 61 73 20 69 6E 20 79 6F 74 72 75 63 74 75 72	6E 79 20 63 68 61 6E 67 t make any chang 75 72 20 66 69 6C 65 20 es in your file 65 3A 20 74 6F 75 63 68 structure: touch	← → ∽ ↑ 📥 → This PC → Local Disk (C:)	
00000C 20 00000C 20 00000C 62	6E 6F 20 66 69 6C 65 74 72 79 20 74 6F 20 79 20 79 6F 75 72 73	73 2C 20 64 6F 6E 27 74 no files, don't 72 65 63 6F 76 65 72 20 try to recover 65 6C 66 2C 20 74 68 61 by yourself, tha	^ Name Size Type	
000000 27	73 20 63 6F 6D 70 6C	61 64 20 74 6F 20 69 74 t may lead to it 65 74 65 20 6C 6F 73 73 's complete loss	Look at this instruction.txt 1 KB Text Do	cument
000000 75	73 20 79 6F 75 20 68	61 76 65 20 74 6F 20 64 us you have to d	Python27 File fold	der
000000 6F 000000 73	77 6E 6C 6F 61 64 20 73 65 6E 67 65 72 3A	20 68 74 74 70 73 3A 2F ssenger: https:/	Program Files File fold	der
000000 2F 000000 0D	71 74 6F 78 2E 67 69 0A 0D 0A 41 64 64 20	74 68 75 62 2E 69 6F 2F /qtox.github.io/ 75 73 65 72 20 77 69 74Add user wit	Windows File fold	der

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.

crypto/cipher.newCBC	
crypto/cipher.dup	
crypto/cipher.NewCBCEncrypter	
crypto/cipher.(*cbcEncrypter).BlockSize	
crypto/cipher.(*cbcEncrypter).CryptBlocks	
crypto/internal/subtle.lnexactOverlap	
crypto/internal/subtle.AnyOverlap	
crypto/cipher.xorBytes	
crypto/cipher.init	
crypto/cipher.xorBytesSSE2	
crypto/aes.encryptBlockGo	
encoding/binary.bigEndian.Uint32	
encoding/binary.bigEndian.PutUint32	Figure 6 – Hardcoded Strings of "Crypto"
crypto/aes.expandKeyGo	
crypto/aes.rotw	
crypto/aes.subw	
crypto/aes.KeySizeError.E3ror	
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	

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.

MachineStorage.dat	× Original File		CPU	Log Notes	Breakpoints Memory	Map 🔲 Call Stack 🗠 SEH 🔟 Script 🔮
	2 4 5 6 7 9 9 4 9 6 9 5			0000000008C2A6F	48:898424 A8000000	mov qword ptr ss:[rsp+A8],rax
00C0b 42 33 36 39	35 43 39 45 31 43 45 41 34 38 39 39	4 B365C9F1CFA4899D		000000000008C2A77 0000000008C2A79	× EB 11	imp new one. BC2ABC
0000h: 43 45 43 31	31 34 33 33 38 46 45 22 20 22 37 22	A CEC14338EE" = 7":		TOXADOOROO BCZAT B	P48: 885424 70	mov rdx, qword ptr ss: rsp+70
00E0h: 22 44 35 45	45 34 45 41 33 36 37 33 38 35 32 45	4 "D5F4FA3673852F4		00000000008C2A80	48:8D4A 01 48:888474 A8000000	lea rcx, qword ptr ds: [rdx+1]
00F0h: 37 36 45 42	42 42 30 37 43 30 38 46 39 42 36 39	6 76FBB07C08F9B696		00000000000000000000000000000000000000	48:885424 78	mov rdx, gword ptr ss: rsp+78
0100h: 34 34 38 33	33 35 38 30 42 39 38 44 35 37 44 34	4 4483580B98D57D44		0000000008C2A91	45:39CA	cmp rdx,rcx
0110h: 43 33 42 32	32 34 34 38 34 35 35 42 34 30 44 43	9 C3B2448455B40DC9		000000000008C2A94	48:894C24 70	mov gword ptr ss: rsp+70 .rcx
0120h: 45 22 2C 22	22 35 22 3A 22 45 30 39 31 31 36 45	4 E","5":"E09116ED		0000000008C2A9F	48:888424 80000000	mov rs1, qword ptr ss: [rsp+80]
0130h: 34 38 39 45	45 32 39 46 44 36 38 33 35 45 38 32	3 489E29FD6835E82C		00000000008C2AA7	48:89F7 48:0EAEE1	imul rsi.rcv
0140h: 45 30 37 33	33 34 39 45 30 32 44 35 38 32 33 44	7 E07349E02D5823D7		0000000008C2AAE	48:0335 93490E00	add rsi, gword ptr_ds: [9A7448]
0150h: 44 34 45 45	45 32 44 39 37 44 39 35 30 34 33 39	2 D4EE2D97D9504392		00000000008C2AB5	48:898424 88000000	mov gword ptr ss:[rsp+88],rs1
0160h: 43 45 31 39	39 30 43 33 31 22 2C 22 33 22 3A 22	15 CE190C31","3":"E		00000000008C2AC0	48:888424 A0000000	mov rax, gword ptr ss:[rsp+A0]
0170h: 39 33 33 38	38 32 37 38 44 41 36 36 37 35 36 38	2 9338278DA667568B	d •	0000000008C2AC8	48:89F9	mov rcx,rdi
0180h: 46 31 42 35	35 34 31 43 42 46 31 35 39 34 38 33	4 F1B541CBF159483D		00000000000SC2AD0	48: 888424 8000000	mov rsi, gword ptr ss: [rsp+80]
0190h: 36 36 32 39	39 32 44 46 46 41 45 33 30 42 31 37	2 66292DFFAE30B17B	•	0000000008C2AD8	48:39F0	cmp rax,rs1
01A0h: 36 35 35 32	32 32 31 45 35 35 45 38 35 43 43 32	2 655221E55E85CC2*		00000000008C2AD8	^ 75 9E	jne new_one.sc2A78
01B0h: 2C 22 38 22	22 3A 22 44 35 45 34 45 41 33 36 37	3 , "8": "D5E4EA3673		00000000008C2AE0	48:89F1	mov rcx,rs1
01C0h: 38 35 32 45	45 34 37 36 45 42 42 30 37 43 30 88	6 852E476EBB07C08F		00000000008C2AE3	48:8BBC24 90000000	mov rd1, qword ptr ss: rsp+90
01001: 39 42 36 39	39 36 34 34 38 33 35 38 30 42 39 38	4 986964483580898D		00000000000000000000000000000000000000	4C:884424 58	mov r8, gword ptr ss: [rsp+58]
01505: 34 30 44 44	34 34 43 33 42 32 34 34 38 34 33 33	2 57044C3B2448455B		0000000008C2AF5	4C:8B8C24 98000000	mov r9, gword ptr ss: [rsp+98]
02000 65 66 28 55	43 39 43 22 20 22 30 22 3A 22 49 0E	4 40DC9E , 0 : INC		00000000008C2802	4C:885424 60	mov r11, qword ptr ss: rsp+68
02100: 61 62 69 74	74 20 4E 65 74 77 6E 72 6P 20 42 6E	E shit Network Con		0000000008C2807	48:888424 A8000000	mov rax, gword ptr ss: rsp+A8
0220h: 6F 65 63 74	74 69 6E 6E 22 7D 0B	nection")		0000000000sC2B14	48:89CF	mov rd1.rcx
011011 01 03 03 13		nección ji	•	0000000008C2B17	48:888424 88000000	mov rsi, qword ptr ss:[rsp+88]
	Environment of File			000000000008C2B1F	48:8909 48:8903	mov rbx, rbx
MachineStorage.dat.biar	anlian × Encrypted File			0000000008C2825	48:888424 A0000000	mov rax, qword ptr ss:[rsp+A0]
0 1 2 3	3456789ABCDÉ	F 0123456789ABCDEF		00000000008C2832	48:85DB	test rbx,rbx
00C0h: C2 C2 3F D3	D3 96 8F C5 DF 1D C6 55 48 7B 36 FA	∖3 ÅÅ?ÓÅß.ÆUH{6ú£ ≚	s	0000000008C2B35	~ 75 OE	jne new_one.8C2845
00D0h: FB FF FD 60	5D 7B 56 06 43 7F 84 2D CD F5 ED 8B	37 ûÿým{V.C."-Íõí‹· 🚞		00000000000000000000000000000000000000	48:888424 8000000 90	nop
00E0h: 57 62 38 A0	A0 E7 F9 92 B6 99 37 19 2C 8D EA 83	DE Wb8 çù′¶™7.,.êfÞ		0000000008C2840	ALE9 36FFFFFF	jmp new_one. SC2A7B
00F0h: 3C EC 86 E1	E1 6B 6B 12 06 E3 7A 63 39 E9 25 10	A <itákkāzc9é%.š th="" 🚬<=""><th>(</th><th>00000000008C2845</th><th>* 74 04</th><th>1e new one, 8C2854</th></itákkāzc9é%.š>	(00000000008C2845	* 74 04	1e new one, 8C2854
0100h: B5 2B 8A F1	F1 C3 97 9F 49 A2 05 08 47 02 98 AC	9 µ+SnA-YICG. ¬1		0000000008C2850	48:8858 08	mov rbx, gword ptr ds: [rbx+8]
0110h: 37 D6 90 A4	A4 5E 5E D3 BA D3 1C 3A 04 D1 34 76	F 70.440°0.:.N4V.		<		
0120h: 49 57 55 20	T3 E9 B0 T8 D0 23 37 79 30 B7 29 AC	9 gloen owyo') h	rax=1			
0140b: 74 6C 38 CO	CO &R R3 FF 7R 3F 49 1D RA 68 A0 91	1 +18A(3b/2T %h 1	FS1=000000	C000145018 & C: 11	Programbata/(Microsoft v	isual scudio/(Machinescorage.dat
0150h: 00 F0 5A 31	31 8E 0A 54 2F 49 9C 1E 4D 03 A3 41	5 .ðZ1Ž.T/Iœ.M.£AÕ	.text:0000	0000008C2AD8 new_0	ne.exe:\$F2AD8 #F20D8	
0160h: 99 DA 2D 68	5E 7D FC 9D 65 3C D2 96 06 70 DE 6A)7 ™Ú-n}ü.e<ÒpÞj.	-			
0170h: 99 20 84 88	BB D1 20 38 CB 84 CB BE CC 22 E0 D6	B ™ "<Ň 8Ë"Ë%Ì"àÔ.	Dump 1	Dump 2 Dump 2	ump 3 📲 Dump 4 📲 Dum	np 5 🐨 Watch 1 💷 Locals 🖉 Struct
0180h: 85 8F OF C8	C8 0A 47 B4 C6 97 65 CB 81 6B FA FC	1È.GʻÆ—eE.kúuñ	Address	Нех		ASCII
0190h: 14 4D 9A C3	C3 14 6F 10 93 01 84 F6 F6 85 C1 5B	6	000000000	DE 44 F9 77 E8 46	5F 79 FF 98 BA A0 F0 66	00 00 DDUWEF_yy.* OT
01A0h: E9 43 50 B5	B5 OC OB A5 7D 3B 84 05 7C B9 OB 5C	DE eC]µ¥};".[1.\Þ	0000000000	80 EF 7F 5F 53 4E	EF 6A 8E BE 77 21 6F BF	95 7E .1SNIJ. SWIDZ .~ Encrypted
U180h: 44 F9 77 E8	E8 46 5F 79 FF 98 BA A0 F0 66 95 7E	D DuweF_yy * at	0000000000	80 EF 7F 5F 53 4E	EF 6A SE BE 77 21 6F BF	C2 57
UTCON: EF /F SF 53	53 4E EF 6A 8E BE 77 21 6F BF C2 57	LE 1. Shigzww.ozAwi	0000000000	EE 2F OC 89 16 F9	60 BA 57 EC 59 E1 C1 56	c2 57 1/u ewiyaAvAw Content
01E0h; E0 0C C0 50	50 20 4D 08 4D 24 D2 DE 40 D2 01 05	S à ÉLAN SÓRONYES	000000000000000000000000000000000000000	EE 2F 0C 89 16 F9	60 BA 57 EC 59 E1 C1 56	00 00 1/u •wiYaAV
01E0h: 02 2D 1E 00	00 30 ED 25 80 E5 AE 50 9E E7 44 85		00000000000	8D E0 OC C9 6C 3C	4D 08 AD 24 D3 DF 40 B3	28 DD . a. E1 <m sob@*+y<="" th=""></m>
0200h: D0 8F FR C	CA 03 D2 E4 03 80 97 A4 A5 24 49 E0	1 Đ ÚÊ Ôā €-¤¥\$Tāa	0000000000	SD E0 0C C9 6C 3C	4D 08 AD 24 D3 DF 40 B3	00 00 .a. £1.4\$0E0*
0210h: 90 71 E2 03	03 D8 48 70 82 71 DD 19 55 74 43 6F	E .gâ.ØKp.gÝ.UtCon	00000000000	35 02 2D 1E 09 3D	FD 25 80 E5 AE 50 9E E7	91 9F 5=ý%.å0].ç
0220h: 6E 65 63 74	74 69 6F 6E 22 7D 0B	nection"}.	0000000000	35 02 2D 1E 09 3D	FD 25 80 E5 AE 50 9E E7	00 00 5=ý%.å*].¢
			00000000000	96 DO 85 58 CA 02	D2 E4 02 80 97 44 45 34	44 PE D 00 05 05 WYCT

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.

<pre>mov rsi,rsp 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</pre>	[rsi]:L"C:\\ Confirmation of the logic of the second of th
call rax	MoveFileExW
add rsp.150	

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	Туре	Size
bianlian	BIANLIAN File	20 KB
y.bianlian	BIANLIAN File	49 KB
📄 🛲 y.bianlian	BIANLIAN File	4 KB
📄 🔤 y.bianlian	BIANLIAN File	26 KB
ingent gy.bianlian	BIANLIAN File	44 KB
yc.bianlian	BIANLIAN File	39 KB
in an Inian	BIANLIAN File	4 KB
📄 🖦 🚛 Linenlian	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
bianlian	BIANLIAN File	56 KB
Look at this instruction.txt	Text Document	1 KB
📄 marputh pylitianlian	BIANLIAN File	7 KB
jy.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.

O Dianianing and an and a second s	mad.onion companies/		→ C 🌒 bianlian	Ne sunadorios contacts/	\$ O \$
BianLian	Home Companies		BianLian	Home Company	ies Tags Contacts
# All companies	→ C ● blanfailli Bianl ian	Hone Cones	# Contacts		
* manuar 6 watting Jul 8, 2022 * Manuar 6 watting Jul 8, 2022 * Watting Jul 8, 2022	# All tags		# Tox		
 Internet input y Jun 28, 2822 Internet in Internet S Jun 21, 2822 	图 insurance		And Manager dates	n and a statement and a statement of the	
BALT Henry Toyl Law Big Jun 21, 2822 Bala Flow Forticity Jun 28, 2822 Address Insurance description Jun 28, 2822	education engineering		# Mail	-il	
* Fantana in Kabiral Jun 5, 2822	聞 law 聞 marketing		gonionia Manailizto	r.com	
2022 e Riani ian	I new				
LARK C SAMILARITY		•••••••••••••••••	2022 o BianLian		

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