THREAT CURE

RE-ARCHITECT YOUR THREAT LANDSCAPE

Cyber Threat Advisory

BianLian

Threat Actor Ransomware

CATEGORY

Malware|Ransomware

SEVERITY

High

Platforms

Windows

IMPACT

- Targeted Sectors
- Geographical Scope
- Coercion Tactics
- Initial Access
- Swift Encryption
- Communication Channels

Description

BianLian Ransomware

The BianLian ransomware group, which emerged in late 2021, has been one of the top 10 most active groups based on leak site data we've gathered. This data shows that BianLian primarily targets the healthcare and manufacturing sectors, affecting organizations mainly in the United States (US) and Europe (EU). The group employs a multifaceted approach, coercing victims into paying for a decryptor by threatening to expose stolen data. Their targets span various sectors, including healthcare, education, and government entities. BianLian gains initial access by exploiting vulnerabilities in exposed systems and services. The encryption process is swift, often completing within minutes. Victims are instructed to communicate with the attackers via qTOX messenger or secure onionmail addresses.

Indicator of compromise

SHA-256

7981cdb91b8bad8b0b894cfb71b090fc9773d830fe110bd4dd8f52549152b448
c83870e8f4884f6653ad7fe43d43e9ab8d6c8b3c295d10f1f1921acd8f1e42a8
aee9287f835f93e6093649a826748e9b27f9921df5ce157d6fee982b8775e853
a53be1e2a6f17a5f4c22ac6fcd24fd70e04cd2c768ed83e84155e37b2a14bcbd
8738866be2f39ac05df243bbe2c82dfc6c125643cc5c75e5f199701fbacc90c9
6d0a906f3764e755d50412c58e70868db223da4a4a6ce1770f27dd9042a869bc
57379fe988e3f7072312b7c2235f13ee4df2907e3243fdec47f658ae2dc395e5
2d61625a0e63ab4491deab98c76aa02ba583b4c655b55c1672b74338c20e39dd
24f38012941211da96f82938320fdbbcb4cf72e26fbe97dc4ad8d1da63da1574
244366488f2956a7209b6f26e97927432aa71cab0c00f3cbca82c51a6706dea8
237d1bca6e056df5bb16a1216a434634109478f882d3b1d58344c801d184f95d
1efbfb8f9e441370bb3f3a316fea237564eefebbf4ba33cccdae5f853c86a7b0
0a2bb0730657fcba380c280663c5e4174586fda123f7a6c6f270a9356229ed8b
fa5d95e8a1517aab2319084cf066280fa972c982db5342b3282090450892a0b3
d70199d3f662e922363ed36d7eaf9b0dab895b9776370514b53b12099a30a802
99fc3e13f3b4d8debf1f2328f56f3810480ee2eed9271ebf413c0015c0a54c23
96e02ea8b1c508f1ee3c1535547f9b89396f557011e61478644ae5876cdaaca5
c57ca631b069745027d0b4f4d717821ca9bd095e28de2eafe4723eeaf4b062cf
1cba58f73221b5bb7930bfeab0106ae5415e70f49a595727022dcf6fda1126e9
56e63edb832fdf08d19ecfe2de1c7c6c6581cedd431215ded0c8e44ac9aed925
d0c1662ce239e4d288048c0e3324ec52962f6ddda77da0cb7af9c1d9c2f1e2eb
c775e6d87a3bcc5e94cd055fee859bdb6350af033114fe8588d2d4d4f6d2a3ae
264af7e7aa17422eb4299df640c1aa199b4778509697b6b296efa5ae7e957b40
0e4246409cdad59e57c159c7cc4d75319edf7d197bc010174c76fe1257c3a68e
ba3c4bc99b67038b42b75a206d7ef04f6d8abaf87a76c373d4dec85e73859ce2
46d340eaf6b78207e24b6011422f1a5b4a566e493d72365c6a1cace11c36b28b
2ed448721f4e92c7970972f029290ee6269689c840a922982ac2f39c9a6a838f
4c008ac5c07d1573a98eb87bffe64e9c9e946de63b40df3f686881cf0698eef7
4ca84be5b6ab91694a0f81350cefe8379efcad692872a383671ce4209295edc7
1fd42d07b4be99e0e503c0ed5af2274312be1b03e01b54a6d89c0eef04257d6e
195c11ee41f5a80d8e1b1881245545d6529671b926eb67bd3186e3ffecefe362
53095e2ad802072e97dbb8a7ccea03a36d1536fce921c80a7a2f160c83366999
23295c518f194dee7815728de15bafe07bf53b52d987c7ad2b2050f833f770f7
40126ae71b857dd22db39611c25d3d5dd0e60316b72830e930fba9baf23973ce
06f10c935fae531e070c55bde15ee3b48b6bb289af237e96eec82124c19d1049
f3f3c692f728b9c8fd2e1c090b60223ac6c6e88bf186c98ed9842408b78b9f3c
f84edc07b23423f2c2cad47c0600133cab3cf2bd6072ad45649d6faf3b70ec30
df51b7b031ecc7c7fa899e17cce98b005576a20a199be670569d5e408d21048c
73d095abf2f31358c8b1fb0d5a0dc9807e88d44282c896b5033c1b270d44111f
f6669de3baa1bca649afa55a14e30279026e59a033522877b70b74bfc000e276
d3574cc69a5974a32a041d1dc460861fe1cef3c1f063171c5fc890ca0e8403c4
7ba40902dc495d8da28d0c0788bcfb1449818342df89f005af8ce09f2ee01798
91ffe0ee445b82bd3360156feeecf8112d27c9333f9796caffcfda986fd7e9b4
60b1394f3afee27701e2008f46d766ef466caa7711c45ddfd443a71efc39a407

SHA-256

c5fa6a7a3b48a2a4bbcbbbb1ca50c730f3545e3fbb03fa17fb814ad7a400a21f
93fb7f0c2cf10fb5885e03c737ee8508816c1102e9e3d358160b78e91fa1ebdb
ac1d42360c45e0e908d07e784ceb15faf8987e4ba1744d56313de6524d2687f7
4e92b73a17e0646876fb9be09c4ee6f015f00273932d2422b69339e22b78b385
93953eef3fe8405d563560dc332135bfe5874ddeb373d714862f72ee62bef518
228ef7e0a080de70652e3e0d1eab44f92f6280494c6ba98455111053701d3759
bd41ac2686beadc1cb008433960317b648caae37c93d8c0d61ad40fe27b5b67e
90f50d723bf38a267f5196e22ba22584a1c84d719b501237f43d10117d972843
188e95d6ed0810c216ab0043ecc2f54f514e624ca31ed1eec58cfc18cc9ac75e
5162fd73cbe8f313d2b0e4180bab4cbe47185f73a3ffc3d1dcccc36bc2865142
9413ba4a33ea77326b837ba538f92348e1909d5263ca67a86aa327daa8fbba30
e7e097723d00f58eab785baf30365c1495e99aa6ead6fe1b86109558838d294e
3106e313f6df73b84acd8d848b467ac42c469ffabbad19e4fdcc963639cfff8c
ac14946fd31ca586368c774f3a3eed1620bf0f0b4f54544f5d25e87facf18d82
3a2f6e614ff030804aa18cb03fcc3bc357f6226786efb4a734cbe2a3a1984b6f

29a14cb63a1900fe185fad1c1b2f2efb85a058ac3c185948b758f3ce4107e11e
8b65c9437445e9bcb8164d8557ecb9e3585c8bebf37099a3ec1437884efbdd24
1fd07b8d1728e416f897bef4f1471126f9b18ef108eb952f4b75050da22e8e43
af46356eb70f0fbb0799f8a8d5c0f7513d2f6ade4f16d4869f2690029b511d4f
4f4a2adc7ecc41f12defe864c78ad6bbf708355affac4115dcd5065b38198109
bd57af28c94c3b7f156511c48f4b62cd1b4c29a1a693f4dc831e0a928691cc56
7dabe5d40c13c7c342b7182eaf7c63fbb5e326300316f6f6518b527d57e79ac8
afb7f11da27439a2e223e6b651f96eb16a7e35b34918e501886d25439015bf78
d3fc56b98af9748f7b6dd44e389d343781ff47db9ed3d92ae8fadc837f25f6ed
eaf5e26c5e73f3db82cd07ea45e4d244ccb3ec3397ab5263a1a74add7bbcb6e2
16cbfd155fb44c6fd0f9375376f62a90ac09f8b7689c1afb5b9b4d3e76e28bdf
16b0f643670d1f94663179815bfac493f5f30a61d15c18c8b305b1016eece7ef
c592194cea0acf3d3e181d2ba3108f0f86d74bcd8e49457981423f5f902d054b
487f0d748a13570a46b20b6687eb7b7fc70a1a55e676fb5ff2599096a1ca888c

SHA-1

1af5616fa3b4d2a384000f83e450e4047f04cb57

be359ef3f2a7962dfbdbc705c4f532d6b2f440a5

b6f7f5f4e3a3e510529379d1aee5fed0be65d566

43707fcff6b4aace232f26fe3d07c30d3b40e1a6

2a4062e10a5de813f5688221dbeb3f3ff33eb417

007dcff13f36583843db1c4130d4255e33284f86

02d1c9bc2d5a448ce15e82a41bc5a03851d521d0

047124d79f0483f62fdb92921af77f800dd269b7

0d0da202a53e9f95575ced832489859888b9e9f8

26ab576a0abf7085ecf6321a311a7b3088ee48ae

281b2d0b444d2db7931747a5afd73d3a38c10f64

2d2be679772386bd2d2428ae01c6a2ffaecd41de

35f8f47c6e4af82c671e30105c24ab1f6ff37639

3a0a139def1de0d366a3ed3e5eb2af1f41685fcd

3f6f09baea2507134255588feed3b7b7990f3bfb

41c236c2e9722c88314b286352062addebf30df0

44718c5e078f58ae18b41a6eccd68e44128f3786

76493a78f17e4aae568b9fc88ea7fd6e2ad498db

7b65797644c746da3d8f033b7b40011aa56e3199

83635e26940f29055d7fdc481ff215c764b6b6a3

8490fd0a801dda3f4fbd0f99b8efaaeb6e3f6577

8aff38ec1949981ab8e9f2f6d7a2c1b0cb665ab4

974e2f27797c471e332326e3673685501b439fea

a5bad0998601a18a1259350599a9a1ec707a299f

ace070500fcb2a5a568014cd797dd17d87b2c11b

b301bdb7c4f9104b0965640e32560bb03c45cae3

c4d3a4e6be4275e48f9bb82fac7ef0b53531e97d

c9bed711b33c9177aedb4363e8f7257433229bcf

4b70350e6c66f238774a20bfc5f15f2a4560803e

4dba35652a91b78d92744970c59f37fcc8aa8bb7

5409bd072cd857d94ff24cb8ede0c758689fbbf1

56aecf816c478d18179aa78baaafb35ada5cd1e2

5bbc3ca6d806a2bd7e7121137de318870c1673fe

6eb8398e33b4b09b852834420c35e5521075db94

MD-5

d25a5b444336b66cc5f36437701b896b
c56b5f0201a3b3de53e561fe76912bfd
54654b346e7425ca1d586f418743dafc
5d9a13a7cac144013d8a985efd0a6658
00bdc543e75222df8cb30324f285d885
08e76dd242e64bb31aec09db8464b28f
0c756fc8f34e409650cd910b5e2a3f00
146229561a3746053f85aa8a11559eac
14da9c0c4e3ac3b9abb2c48b37bece19
214c2e995c87b94e7302d1cab9063314
215a7c28d07eb446eaee352ac2af62a3
22c04e4bec172e22d25d52a8d28af897
2b5db2277171dc9e45677b0a4b6ac4a7
318249067514a04331bde3d08785e7b5
36171704cde087f839b10c2465d864e1
4a432dac581e5ebf31008f8f7041e96e
4e8f9792dd5abeb31acdb7850e1feb31
4f4a826dc77e591b5679bd3d1052d52e
f2f4756ac33399925d32ae49a0098e5e
f454c52f40d1de3e7f0c9763e21d7d05
f890c89f8d78599d724cb14eeb0e0198

fdeccb927db95a038e0934564282044d
08bdf000031bbad1a836381f73adace5
0c0195c48b6b8582fa6f6373032118da
42a80cc2333b612b63a859f17474c9af
7b68bc3dd393c2e5273f180e361f178a
9e88c287eb376f3c319a5cb13f980d36
bfd36fd6a20ccd39f5c3bb64a5c5dd8b
c12f54a3f91dc7bafd92cb59fe009a35
ec74a5c51106f0419184d0dd08fb05bc
e245f8d129e8eadb00e165c569a14b71
e5f1be8d5b7b33096e8f9ebb413b0466
e625ef18487a37a71b489d39c65a343a
e630ace786fcdf6caa4c231957129ebb
53cefec60084a9c4e0355d9387840373
55d87f659e61d135b9f52966715df05c
5b415a56214972c7d81494fca32f13bf
5cb3f287494a8086148f5d08c1ac49a4
609554db75e2068d1e1d49b202ae92da
6149c2af9d66c017eb126150d1e30106
65d3a8dbd5a5ee902fee141f467b325a
681d2e6fca521c29ac8bf056e5473c4a

MD-5

fdce2762c69cf4a5e4cb9f6caeb508b8
b55f4147ac49e2bf4be8cad18a7d2e1d
bd0a4dbb3913263b840e4c0e04e67825
be5361057039c171e2870f727c930a35
be8303c908486cf992550822d0619ffe
c1f44396f46e508b30eb8af4733131b7
c5af959e620a6641f5e9965a1be215e0
d21978539ddac2857b80b6cf762dabc5
d29810036078d3294223a14f2adb9508
d638b545c3e3bfc1e72470e7ce1d510e
d72edd6eb0b0cabada93db36ec007352
d94b066171548e027b6de4a64837a303
ded60c35e28c3c0ea30823cca0b212ce
ebc8fdafb45e7e383e527f18d1828bd6

68d8a369cdf2e92c0f7ac2310f633b45
6a58b52b184715583cda792b56a0a1ed
6cc6e89b244e9b27ab4c43c9ab434f8f
6cca2573c8c65aadbfb14548974cde30
752a495b34b244acc86aba16b6353343
7cc78f1b6c65c6b0cdc57e8a01c7b235
8019a453dc321006280bdc6759ebfffc
8054bcc0a3e2cda7179e6dafb28b108a
84c4769c1a2bfa2105199e4c1784851b
88e332e259b78210bbf56ee417dce6c3
8a2e26ab771132300b56478fee1dd634
97abffeaa7bdfaa81532bd6028498225
98835e4259e89a70bfacd979e11938f9
b0623af1c22682ae58ab1ff8324a33cd

Remediation

1. Regular Vulnerability Scans: Identify and patch exposed systems promptly.
2. Data Backups: Perform regular, offline backups of critical data.
3. Security Updates: Keep all software and systems up to date.
4. Employee Training: Educate staff on phishing and safe online practices.
5. Network Segmentation: Limit the spread of ransomware by segmenting networks.
6. Access Controls: Use multi-factor authentication and enforce least privilege access.
7. Incident Response Plan: Maintain and update a ransomware-specific response plan.
8. Endpoint Protection: Deploy solutions to detect and respond to suspicious activities.
9. Block all IOCs on your XDR, EDR and other security tools.

THREAT CURE

RE-ARCHITECT YOUR THREAT LANDSCAPE

Cyber Threat Advisory

Secure your byte world

+1 (832) 271 2738

info@threatcure.net

https://threatcure.net/