KPMG Cyber Threat Intelligence Platform

BianLian Ransomware: Shifting Tactics from Encryption to Data Extortion

TLP : Clear

KPMG. Make the Difference.

BianLian, a suspected Russian-origin ransomware group active since June 2022, targets sectors like healthcare, finance, education, construction, logistics, and transportation in the United States, United Kingdom, Canada, and Australia. Initially employing a double-extortion model, they switched to data extortion by early 2023, utilizing customized, cross-platform Go-based malware and "Living off the Land" techniques.

BianLian primarily gains access using compromised RDP credentials and targets public-facing applications of both Windows and ESXi infrastructure, often via the ProxyShell exploit chain. They exploit vulnerabilities like CVE-2022-37969 on Windows 10 and 11 systems and utilize PowerShell and Command Shell to disable antivirus tools and modify the Windows Registry. They rename binaries and tasks to mimic legitimate services and pack executables with UPX for evasion. They use valid accounts for lateral movement, harvest credentials from Local Security Authority Subsystem Service (LSASS) memory and employ tools like RDP Recognizer and Impacket for credential harvesting. They also leverage tools such as Advanced Port Scanner, SoftPerfect Network Scanner, SharpShares, and PingCastle to understand the victim's environment. They employ PsExec and RDP with valid accounts for lateral movement and create domain admin accounts and Azure AD accounts for persistence. They use malware to enumerate registry values and files and copy clipboard data, and may use tools like Ngrok or a modified version of Rsocks to establish network tunnels and mask C2 traffic. Data is compressed or encrypted using PowerShell scripts and then exfiltrated via FTP, Rclone, and Mega file-sharing service.

BianLian's transition to data extortion underscores the necessity for enhanced cybersecurity defenses and strategic incident response planning.

What should you do?

- Monitor Indicators of Compromise (IoCs) in your environment to identify anomalies.
- Ensure your Windows environment is patched to the brim and is protected with multi-factor authentication.
- Conduct a comprehensive, full spectrum, threat assessment exercise to uncover blind spots and improvement areas.

KPMG Cyber Threat Intelligence Platform is an industry defining, research-based capability for enhanced visibility into cyber threats.

Our machine ingestible feeds and analysis are the result of automated, sensor-based intelligence metrics with dedicated, expert insights of each threat to provide you the appropriate context on a timely basis in industry standard formats such as STIX/ TAXII/ MISP.

These feeds are additionally co-related with our industry partners and independent research for additional context. The intelligence obtained is then curated from strategic, tactical and operational perspective to give you a wide-ranging view of cyber threats.

We also assist you with our renowned cyber incident response and threat hunting services in case you identify an active threat in your environment.

We offer a wide-range of services, including:
Strategic threat intelligence report
Machine ingestible threat intelligence feeds
Threat intelligence driven pre-emptive threat hunting exercise
Cyber Incident Response Services

KPMG in India Cyber Response Hotline: 1800 2020 502

KPMG in India contacts:

Atul Gupta
Partner
Head of Cyber Security
T: +91 98100 81050
E: atulgupta@kpmg.com

B V, Raghavendra
Partner
T: +91 98455 45202
E: raghavendrabv@kpmg.com

Sony Anthony
Partner
T: +91 98455 65222
E: santhony@kpmg.com

Chandra Prakash
Partner
T: +91 99000 20190
E: chandraprakash@kpmg.com

Manish Tembhurkar
Partner
T: +91 98181 99432
E: mtembhurkar@kpmg.com

Rishabh Dangwal
Director
T: +91 99994 30277
E: rishabhd@kpmg.com

kpmg.com/in

Follow us on:
kpmg.com/in/socialmedia

KPMG

KPMG Cyber Threat Intelligence Platform

BianLian Ransomware: Shifting Tactics from Encryption to Data Extortion

TLP : Clear

KPMG. Make the Difference.

Indicators of Compromise: IP Addresses	
146.0.79[.]9	185.62.58[.]151
5.2.79[.]138	192.169.6[.]232
66.135.0[.]42	91.199.209[.]20
172.93.96[.]61	83.136.180[.]12
172.93.96[.]62	85.13.117[.]213
185.69.53[.]38	104.225.129[.]86
45.9.150[.]132	104.238.223[.]10
64.52.80[.]120	185.225.69[.]173
104.238.223[.]3	192.145.38[.]242
109.248.6[.]207	185.108.129[.]242

Indicators of Compromise: Hashes
08e76dd242e64bb31aec09db8464b28f
ad5fbd52096e8bdc76d4052a5d8975a2
e245f8d129e8eadb00e165c569a14b71
bc292d6f5c3ed8bf4165eb5b2c88fede
cf13f947009af3e28528dfa3baaa7d10
026a7d53db504daa1aba3a941ee90a5d
09fe88cbc094d5b8999e6f576c6fed2a
df786efbc445ae590b7a19c21002fcf9
aa42a333887b605f721bf7f6eac736f4
19565d20e8ef1d3c42b20fdbb3bd3963
457f7ba6c9c5c6ae0cc76fa98c801a2b
4d76c5753e61b8fffdb5beffbece6f35
b2dd304aff345a84979336d2ffc97014
6564ffc14ab803a961453a118a33830e

Follow us on:
kpmg.com/in/socialmedia

KPMG

KPMG Cyber Threat Intelligence Platform

BianLian Ransomware: Shifting Tactics from Encryption to Data Extortion

TLP : Clear

KPMG. Make the Difference.

Indicators of Compromise: Hashes
d4db6316686e26ad99d1a9ec2d449a59
0cc30238204a3d3da6d588640e054af6
0c756fc8f34e409650cd910b5e2a3f00
14da9c0c4e3ac3b9abb2c48b37bece19
97abffeaa7bdfaa81532bd6028498225
e625ef18487a37a71b489d39c65a343a
e3baa1c3ee9aa1d5ae61187be2e20ea9cb57d538
3f3f62c33030cfd64dba2d4ecb1634a9042ba292
3477a173e2c1005a81d042802ab0f22cc12a4d55
8aff38ec1949981ab8e9f2f6d7a2c1b0cb665ab4
c9bed711b33c9177aedb4363e8f7257433229bcf
ace070500fcb2a5a568014cd797dd17d87b2c11b
23fb3022ce7e94db2be7d1eea803fc299a0af26b
2d2be679772386bd2d2428ae01c6a2ffaecd41de
281b2d0b444d2db7931747a5afd73d3a38c10f64
02d1c9bc2d5a448ce15e82a41bc5a03851d521d0
3f6f09baea2507134255588feed3b7b7990f3bfb
8490fd0a801dda3f4fbd0f99b8efaaeb6e3f6577
3a0a139def1de0d366a3ed3e5eb2af1f41685fcd
b301bdb7c4f9104b0965640e32560bb03c45cae3
5bbc3ca6d806a2bd7e7121137de318870c1673fe
6eb8398e33b4b09b852834420c35e5521075db94
5a1df6ea72b1a22ab48c547898bb0e8710c1d771
76493a78f17e4aae568b9fc88ea7fd6e2ad498db
44718c5e078f58ae18b41a6eccd68e44128f3786
83635e26940f29055d7fdc481ff215c764b6b6a3

KPMG

KPMG Cyber Threat Intelligence Platform

BianLian Ransomware: Shifting Tactics from Encryption to Data Extortion

TLP : Clear

KPMG. Make the Difference.

Indicators of Compromise: Hashes
35f8f47c6e4af82c671e30105c24ab1f6ff37639
7b65797644c746da3d8f033b7b40011aa56e3199
56e63edb832fdf08d19ecfe2de1c7c6c6581cedd431215ded0c8e44ac9aed925
3106e313f6df73b84acd8d848b467ac42c469ffabbad19e4fdcc963639cfff8c
7ba40902dc495d8da28d0c0788bcfb1449818342df89f005af8ce09f2ee01798
06f10c935fae531e070c55bde15ee3b48b6bb289af237e96eec82124c19d1049
23295c518f194dee7815728de15bafe07bf53b52d987c7ad2b2050f833f770f7
d3fc56b98af9748f7b6dd44e389d343781ff47db9ed3d92ae8fadc837f25f6ed
c5fa6a7a3b48a2a4bbcbbbb1ca50c730f3545e3fbb03fa17fb814ad7a400a21f
16b0f643670d1f94663179815bfac493f5f30a61d15c18c8b305b1016eece7ef
188e95d6ed0810c216ab0043ecc2f54f514e624ca31ed1eec58cfc18cc9ac75e
4f4a2adc7ecc41f12defe864c78ad6bbf708355affac4115dcd5065b38198109
99fc3e13f3b4d8debf1f2328f56f3810480ee2eed9271ebf413c0015c0a54c23
d3574cc69a5974a32a041d1dc460861fe1cef3c1f063171c5fc890ca0e8403c4
4c008ac5c07d1573a98eb87bffe64e9c9e946de63b40df3f686881cf0698eef7
90f50d723bf38a267f5196e22ba22584a1c84d719b501237f43d10117d972843
0e4246409cdad59e57c159c7cc4d75319edf7d197bc010174c76fe1257c3a68e
228ef7e0a080de70652e3e0d1eab44f92f6280494c6ba98455111053701d3759
f6669de3baa1bca649afa55a14e30279026e59a033522877b70b74bfc000e276
f3f3c692f728b9c8fd2e1c090b60223ac6c6e88bf186c98ed9842408b78b9f3c
93953eef3fe8405d563560dc332135bfe5874ddeb373d714862f72ee62bef518
f84edc07b23423f2c2cad47c0600133cab3cf2bd6072ad45649d6faf3b70ec30
487f0d748a13570a46b20b6687eb7b7fc70a1a55e676fb5ff2599096a1ca888c
1cba58f73221b5bb7930bfeab0106ae5415e70f49a595727022dcf6fda1126e9
ac1d42360c45e0e908d07e784ceb15faf8987e4ba1744d56313de6524d2687f7
96e02ea8b1c508f1ee3c1535547f9b89396f557011e61478644ae5876cdaaca5

KPMG

KPMG Cyber Threat Intelligence Platform

BianLian Ransomware: Shifting Tactics from Encryption to Data Extortion

TLP : Clear

KPMG. Make the Difference.

Indicators of Compromise: Hashes
e7e097723d00f58eab785baf30365c1495e99aa6ead6fe1b86109558838d294e
ba3c4bc99b67038b42b75a206d7ef04f6d8abaf87a76c373d4dec85e73859ce2
60b1394f3afee27701e2008f46d766ef466caa7711c45ddfd443a71efc39a407
16cbfd155fb44c6fd0f9375376f62a90ac09f8b7689c1afb5b9b4d3e76e28bdf
53095e2ad802072e97dbb8a7ccea03a36d1536fce921c80a7a2f160c83366999
afb7f11da27439a2e223e6b651f96eb16a7e35b34918e501886d25439015bf78
93fb7f0c2cf10fb5885e03c737ee8508816c1102e9e3d358160b78e91fa1ebdb
4ca84be5b6ab91694a0f81350cefe8379efcad692872a383671ce4209295edc7
8b65c9437445e9bcb8164d8557ecb9e3585c8bebf37099a3ec1437884efbdd24
73d095abf2f31358c8b1fb0d5a0dc9807e88d44282c896b5033c1b270d44111f
264af7e7aa17422eb4299df640c1aa199b4778509697b6b296efa5ae7e957b40
2ed448721f4e92c7970972f029290ee6269689c840a922982ac2f39c9a6a838f
df51b7b031ecc7c7fa899e17cce98b005576a20a199be670569d5e408d21048c
c592194cea0acf3d3e181d2ba3108f0f86d74bcd8e49457981423f5f902d054b
c57ca631b069745027d0b4f4d717821ca9bd095e28de2eafe4723eeaf4b062cf
c775e6d87a3bcc5e94cd055fee859bdb6350af033114fe8588d2d4d4f6d2a3ae
1fd07b8d1728e416f897bef4f1471126f9b18ef108eb952f4b75050da22e8e43
7b15f570a23a5c5ce8ff942da60834a9d0549ea3ea9f34f900a09331325df893
40126ae71b857dd22db39611c25d3d5dd0e60316b72830e930fba9baf23973ce
20bab94e6d9c8ed4832ce3b58f9150b16f9e5f40ffdcb747e10366cab5a30352
50c86fb27bed1962903a5f9d155544e3fdb859ae19e967a10f0bf3a60bb8954f
64065c29b369881ee36314c0d15e442510027186fd9087aec0f63e22a5c6f24c
8592862cd28bcc23cfbcf57c82569c0b74a70cd7ea70dbdee7421f3fafc7ecaf
c0fe7bfb0d1ffeb61fb9cafeeab79ffd1660ff3637798e315ff15d802a3c974e
c7fe3fc6ffdfc31bc360afe7d5d6887c622e75cc91bc97523c8115b0e0158ad6
cd17afd9115b2d83e948a1bcabf508f42d0fe7edb56cc62f5cc467c938e45033