KPMG Cyber Threat Intelligence Platform

BianLian Ransomware – Smart, Fast & Stealthy

BianLian made its debut in the cyber space in July 2022 and has been targeting various sectors including media, entertainment, education, healthcare and professional services. The group is emerging as a serious threat by going cross-platform with Go(lang), adopting a fresh stealthy & faster encryption technique, alongside agile lateral movement tactics to suit various target environments. Major regions of attack include industries in Australia, North America & UK, and the group is keen on expanding its targets across the globe.

The initiation of attack is done by exploiting SonicWall VPN & Microsoft Exchange ProxyShell security flaws in order to obtain access, post which a web shell or remote access tool is dropped for further access. The group then 'lives off the land' by using native binaries for network discovery & lateral movement. LOLBins abuse include changing user rights via 'net.exe', modifying host firewall configuration via 'netsh.exe' and modifying registry for remote desktop & security policy enforcement via 'reg.exe'. Further, it lavishly uses Windows API for disk, file & directory enumeration and for numerous fast multi-threaded encryption routines, thus making it harder for analysis. BianLian stealthily encrypts files by encrypting 10-byte chunks at a time while writing into new destination file and replacing original file. It could also boot infected systems in Safe Mode to get around security solutions. Post exfiltrating data for double extortion using dropped 7-Zip & WinSCP for data compression & data transfer. As its final act, BianLian eliminates backup, snapshots and deletes itself from the system using the 'CMD' utility.

The distinctive presence of the threat actor makes it inevitable for industries across various sectors to take immediate action in order to safeguard themselves through continuous security updates.

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.

The 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

Contact us:

KPMG in India Cyber Response Hotline : +91 9176 471 471

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

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

Sony Anthony
Partner, KPMG in India
T: +91 98455 65222
E: santhony@kpmg.com

Chandra Prakash
Partner, KPMG in India
T: +91 99000 20190
E: chandraprakash@kpmg.com

Manish Tembhurkar
Associate Partner,
KPMG in India
T: +91 98181 99432
E: mtembhurkar@kpmg.com

KPMG

KPMG Cyber Threat Intelligence Platform

BianLian Ransomware – Smart, Fast & Stealthy

Indicators of Compromise: IP Addresses	
146.0.79[.]9	185.62.58[.]151
13.49.57[.]110	18.130.242[.]71
185.69.53[.]38	16.162.137[.]220
185.56.80[.]28	155.94.160[.]241
172.93.96[.]62	104.238.61[.]153
172.93.96[.]61	104.238.223[.]10
167.88.15[.]98	104.225.129[.]86
165.22.87[.]199	185.225.69[.]173
157.245.80[.]66	172.96.137[.]107
146.70.44[.]248	144.208.127[.]119
109.248.6[.]207	104.207.155[.]133
104.238.223[.]3	185.108.129[.]242

Indicators of Compromise: Hashes
e625ef18487a37a71b489d39c65a343a
36171704cde087f839b10c2465d864e1
0c756fc8f34e409650cd910b5e2a3f00
08e76dd242e64bb31aec09db8464b28f
e3baa1c3ee9aa1d5ae61187be2e20ea9cb57d538
70d1d11e3b295ec6280ab33e7b129c17f40a6d2f
3f3f62c33030cfd64dba2d4ecb1634a9042ba292
2a158d21141564af81b4877bdfe622a152449272
eaf5e26c5e73f3db82cd07ea45e4d244ccb3ec3397ab5263a1a74add7bbcb6e2
ae61d655793f94da0c082ce2a60f024373adf55380f78173956c5174edb43d49
a201e2d6851386b10e20fbd6464e861dea75a802451954ebe66502c2301ea0ed
46d340eaf6b78207e24b6011422f1a5b4a566e493d72365c6a1cace11c36b28b
3be5aab4031263529fe019d4db19c0c6d3eb448e0250e0cb5a7ab2324eb2224d
3a2f6e614ff030804aa18cb03fcc3bc357f6226786efb4a734cbe2a3a1984b6f
1fd07b8d1728e416f897bef4f1471126f9b18ef108eb952f4b75050da22e8e43
f7a3a8734c004682201b8873691d684985329be3fcdba965f268103a086ebaad
de31a4125eb74d0b7cbf2451b40fdb2d66d279a8b8fd42191660b196a9ac468f
dda89e9e6c70ff814c65e1748a27b42517690acb12c65c3bbd60ae3ab41e7aca
da7a959ae7ea237bb6cd913119a35baa43a68e375f892857f6d77eaa62aabbaf

KPMG

KPMG Cyber Threat Intelligence Platform

BianLian Ransomware – Smart, Fast & Stealthy

Indicators of Compromise: Hashes
d602562ba7273695df9248a8590b510ccd49fefb97f5c75d485895abba13418d
cd17afd9115b2d83e948a1bcabf508f42d0fe7edb56cc62f5cc467c938e45033
cbab4614a2cdd65eb619a4dd0b5e726f0a94483212945f110694098194f77095
c7fe3fc6ffdfc31bc360afe7d5d6887c622e75cc91bc97523c8115b0e0158ad6
c0fe7bfb0d1ffeb61fb9cafeeab79ffd1660ff3637798e315ff15d802a3c974e
bb2e9fd9d60f49f0fc2c46f8254e5617d4ec856f40256554087cda727a5f6019
b60be0b5c6e553e483a9ef9040a9314dd54335de7050fed691a07f299ccb8bc6
9b7a0117a27dc418fbf851afcd96c25c7ad995d7be7f3d8d888fa26a6e530221
86a9b84c6258c99b3c3c5b94a2087bc76a533f6043829ded5d8559e88b97fb2f
8592862cd28bcc23cfbcf57c82569c0b74a70cd7ea70dbdee7421f3fafc7ecaf
8084eddfdb157edf8b1c0cdf8bf4d4e4aaa332fc871c2892aa4113b5148ac63e
6d7009df2fa033f7adc30793ebd5254ef47a803950e31f5c52fa3ead1197599f
64065c29b369881ee36314c0d15e442510027186fd9087aec0f63e22a5c6f24c
5d429e05cede806ecea2e99116cac09558fcc0011095201e66c2e65c42f80fcf
50c86fb27bed1962903a5f9d155544e3fdb859ae19e967a10f0bf3a60bb8954f
3bdcc81931687abac9e6ba4c80d4d596cebb470c80f56213aa29d3da43925537
36281d02e28dd26a1db37ebe36941fc9eb1748868e96b544f227b3b59de51fea
20bab94e6d9c8ed4832ce3b58f9150b16f9e5f40ffdcb747e10366cab5a30352
1a1177363be7319e7fb50ac84f69acb633fd51c58f7d2d73a1d5efb5c376f256
001f33dd5ec923afa836bb9e8049958decc152eeb6f6012b1cb635cff03be2a2
117a057829cd9abb5fba20d3ab479fc92ed64c647fdc1b7cd4e0f44609d770ea