Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

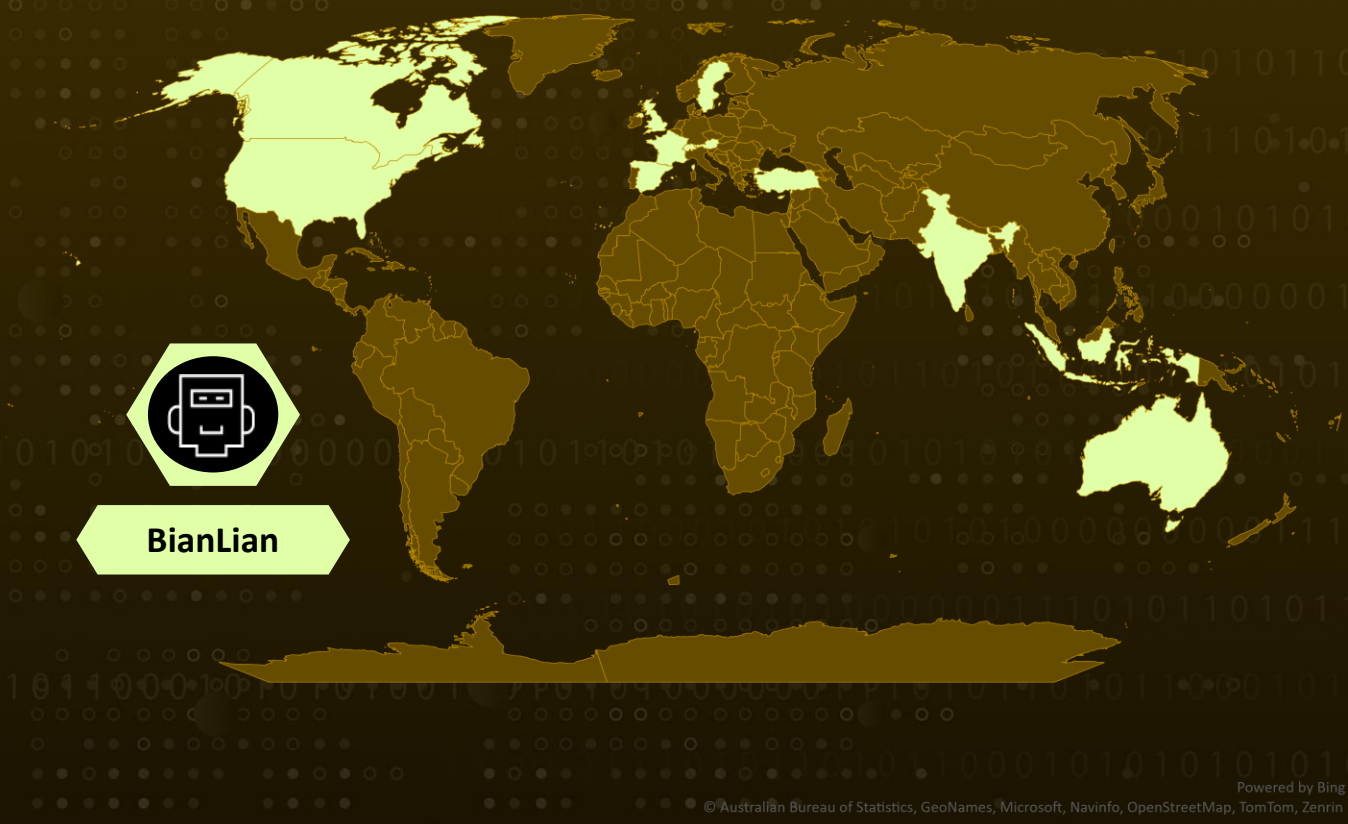
BianLian ransomware ramps up data-leak extortion and improves operational security

Date of Publication	Admiralty Code	TA Number
March 17, 2023	A1	TA2023142

Summary

Date: July 2022
Attack Region: Canada, United States, United Kingdom, India, Sweden, France, Gernamy, Spain, Austria, Switzerland, Turkey, Cyprus, Indonesia, Australia, Northern Ireland
Targeted Industries: Hospitality, Real Estate, Manufacturing, Food Products, Professional Services, Education, Construction & Engineering, Health Care, Consumer Discretionary, Diversified Telecommunication
Malware: BianLian ransomware
Attack: BianLian ransomware group is ramping up data-leak extortion to extract payments, using similar tactics & a custom backdoor, and bringing 30 new C2 servers online monthly.

Attack Regions



Attack Details

#1

BianLian is a ransomware group, that continues to add more victims, displaying a high level of operational security and skill in network penetration. Its shift of focus from ransoming encrypted files to data-leak extortion is also notable. The group has improved its ability to operate the business side of a ransomware organization while maintaining similar Tactics, Techniques, and Procedures (TTPs) to perform their initial access and lateral movement within a victim's network.

#2

In addition, BianLian appears to have found its stride in the number of command and control servers it requires to sustain its operations. The group brings close to 30 new C2 servers online each month. BianLian has been tailoring the messages delivered to specific victims to increase the pressure felt by the organizations.

#3

BianLian has also shifted its tactics to focus more on data-leak extortion as a means to extract payments from victims, rather than encrypting their data. The group promises that after they are paid, they will not leak the stolen data or otherwise disclose the fact the victim organization has suffered a breach, stating that their business depends on their reputation.

Recommendations

Security Leaders

Phishing simulations and routine education and awareness training and communications rarely account for MFA fatigue and web browser hygiene. Integrate and communicate all lessons learned.

Security Engineers

- **Uni5 Users:** This is an actionable threat advisory in HivePro Uni5. Prioritize and block all indicators attributed to the threat actors and attacks through your Command Center. Test your controls with Uni5's Breach & Attack Simulation.
- **All Engineers:** Refer to and action upon the 'Potential MITRE ATT&CK TTPs' & 'Indicators of Compromise (IoC)' on the following pages.

Potential MITRE ATT&CK TTPs

TA0007 Discovery	TA0011 Command and Control	TA0003 Persistence	TA0009 Collection
TA0005 Defense Evasion	TA0040 Impact	TA0042 Resource Development	T1027 Obfuscated Files or Information
T1219 Remote Access Software	T1584 Compromise Infrastructure	T1486 Data Encrypted for Impact	T1140 Deobfuscate/Decode Files or Information
T1102 Web Service	T1022 Data Encrypted	T1083 File and Directory Discovery	

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	076e59781d0759de35022291c3d63bbf4227bd79561d80f52c9073a6278c5077 0772fb1102685def711ffe647080e1a9b6597fe60e8f1afe7b457ac97c6ac25e 16cbfd155fb44c6fd0f9375376f62a90ac09f8b7689c1afb5b9b4d3e76e28bdf 183b28fb93db1c907b32aa9fa2f83c7b0ebcc6724de85707a89e5d03c5be5d12 1cba58f73221b5bb7930bfeab0106ae5415e70f49a595727022dcf6fda1126e9 207078c70be916bb7d2ad4d206d2dca37406f84313f88699fa57fa9745a055bb 228ef7e0a080de70652e3e0d1eab44f92f6280494c6ba98455111053701d3759 38d6ec5f93f6722c3573989f1463fb1cba1c01c3a1a0579f329e0d625c57070b 42b0606aa2c765c0b0789b47ebd3a3f43144dc0c20b2ff6db648ac5feb0a37a3 45f76c5c5126501018f907f886dd23a56dd882ee7d4f41c41d732612b2e4da88 46fa9a69989b79b56495a1ece8a45d6d5ae43c600b8a13ef88f3eb9d84efda02 487f0d748a13570a46b20b6687eb7b7fc70a1a55e676fb5ff2599096a1ca888c 4ca84be5b6ab91694a0f81350cefe8379efcad692872a383671ce4209295edc7

TYPE	VALUE
SHA256	53095e2ad802072e97dbb8a7ccea03a36d1536fce921c80a7a2f160c83366999 55016f61b9880be414cc4e1280d6bb620cfbe5e1e8e12e305a304d3dff7e209c 597c492a5af56d935d360fcfd2c1e89928dde492c86975f2c5cc33ec90b042ce 60b1394f3afee27701e2008f46d766ef466caa7711c45ddfd443a71efc39a407 61dfe2ccdc7cee55cf0530064499a52bf93bc6c3d8996ed013fcc5692e94c73a 667821f5996855bf83507fb1009f5d8d36c1258aa3c776106d453200f3bb0ed3 77617775dc6fa8b893607d52c3282ece1912bcdd0b583b418399af2eade249b8 7b15f570a23a5c5ce8ff942da60834a9d0549ea3ea9f34f900a09331325df893 93953eef3fe8405d563560dc332135bfe5874ddeb373d714862f72ee62bef518 93fb7f0c2cf10fb5885e03c737ee8508816c1102e9e3d358160b78e91fa1ebdb 96e02ea8b1c508f1ee3c1535547f9b89396f557011e61478644ae5876cdaaca5 a8e999a7a77d3b9846250a34ebda7d80ea83a79b3714b1f7ac8f92bc52a895fd a92dd4885af317d36cd62dac31d0d5c93febd367e8f4412e7593fb48c9f34256 ac1d42360c45e0e908d07e784ceb15faf8987e4ba1744d56313de6524d2687f7 adefaad2a9c449d0e9fabb5035422a6ce31d0f26b0109a7c2911f570a6c74144 afb7f11da27439a2e223e6b651f96eb16a7e35b34918e501886d25439015bf78 b4249f2effb8dd651458c831d38155346c1e2d30b191bf37197ffa5164d25f7c ba3c4bc99b67038b42b75a206d7ef04f6d8abaf87a76c373d4dec85e73859ce2 c62371f129d19707870c0f9a89b0f8a65970aed02537e358e532e4416bc8678e dcc7115496faa0797c32bb6d5d823821f19f5177e09e05dbe0151a6b9e1edfb7 dd03ea7ba369fc9df641c09f29e4abcb8378b5a8dadd3d7c14d47449525f1716 e136d635de39d23cef600cc53efd671f1e8aba7d982bde152b21ea1f7c04703e

TYPE	VALUE
SHA256	ea5c88fe464562227f483e8fc4eb2cf43e98a897aaaa3e94de4d236d5dc6e7e7 f3a4fb09a0498e7ab3b33338ca6bc03460e43d437d9f3afbfc1a521c1029ff19 f3f3c692f728b9c8fd2e1c090b60223ac6c6e88bf186c98ed9842408b78b9f3c f6669de3baa1bca649afa55a14e30279026e59a033522877b70b74bfc000e276 f84edc07b23423f2c2cad47c0600133cab3cf2bd6072ad45649d6faf3b70ec30 117a057829cd9abb5fba20d3ab479fc92ed64c647fdc1b7cd4e0f44609d770ea 3a2f6e614ff030804aa18cb03fcc3bc357f6226786efb4a734cbe2a3a1984b6f 46d340eaf6b78207e24b6011422f1a5b4a566e493d72365c6a1cace11c36b28b 7f91e10c39e0a77c83af3ef48061cbb73194c793f9c3c8bc7fa1aa0fc75eb385 F77433e517f493ca54e6a4603e51739053ebfac03d2764ad9d1f7e00cfadefa0 e7e097723d00f58eab785baf30365c1495e99aa6ead6fe1b86109558838d294e
IPV4	104.223.0[.]85 104.234.118[.]129 104.238.35[.]26 155.94.160[.]243 173.232.2[.]41 185.99.133[.]112 192.161.48[.]51 204.152.203[.]94 208.123.119[.]100 35.157.43[.]44 45.86.163[.]228 52.53.186[.]224 54.144.145[.]126 66.85.156[.]83 102.129.214[.]35 103.199.17[.]27 103.20.235[.]122 103.20.235[.]188 104.200.67[.]156 104.200.67[.]244 104.200.67[.]31

TYPE	VALUE
IPV4	104.200.73[.]239 104.216.17[.]42 104.217.8[.]125 104.225.168[.]249 104.238.35[.]146 104.238.57[.]205 104.238.61[.]153 104.238.61[.]218 104.255.168[.]249 138.124.183[.]149 139.177.146[.]46 139.177.146[.]46 139.99.176[.]57 139.99.52[.]102 142.202.205[.]89 144.208.127[.]155 144.208.127[.]18 146.19.173[.]121 146.59.102[.]74 146.70.161[.]27 146.70.87[.]197 146.71.81[.]102 149.154.158[.]120 149.154.158[.]153 149.154.158[.]154 149.154.158[.]56 15.188.49[.]63 157.254.194[.]223 158.247.200[.]185 158.255.215[.]58 162.33.177[.]94 167.114.188[.]41 172.96.137[.]114 172.96.137[.]153 172.96.137[.]220 172.96.137[.]224 172.96.137[.]249 172.96.137[.]29 172.96.188[.]109 172.96.188[.]52 172.96.189[.]158 173.254.204[.]78 173.44.226[.]73 18.159.131[.]209

TYPE	VALUE
IPV4	185.214.10[.]116 185.243.112[.]166 185.243.115[.]30 185.56.137[.]117 188.34.155[.]224 192.161.48[.]60 192.169.6[.]79 192.52.167[.]135 194.71.227[.]52 195.201.127[.]139 198.252.101[.]244 198.252.109[.]40 198.252.109[.]57 198.252.109[.]78 206.189.128[.]5 208.123.119[.]230 208.123.119[.]240 208.123.119[.]48 209.182.225[.]124 212.46.38[.]118 216.120.201[.]107 216.146.25[.]60 217.195.153[.]177 23.163.0[.]168 23.229.117[.]247 3.134.86[.]154 35.183.14[.]149 37.220.31[.]104 37.220.31[.]17 37.235.54[.]42 37.235.54[.]52 44.212.9[.]14 45.128.156[.]10 45.128.156[.]3 45.128.156[.]43 45.145.186[.]188 45.33.119[.]19 45.56.165[.]17 45.61.136[.]152 45.66.249[.]118 45.86.230[.]64 46.246.96[.]53 5.230.70[.]23 5.230.72[.]245

TYPE	VALUE
IPV4	5.230.73[.]234 5.230.73[.]37 51.222.96[.]1 52.87.206[.]242 54.227.224[.]229 66.85.147[.]22 72.11.134[.]215 81.17.28[.]71 85.239.52[.]96 85.239.53[.]168 96.44.135[.]76 96.44.156[.]206 96.44.157[.]203

Recent Breaches

Https://bestcarton.com
Https://parquesreunidos.com
Https://plparchitecture.com
Https://hak-graz.at
Https://thompson-safety.com
Https://anxa.com
Https://zerbesisters.com
Https://advance2000.com
Https://ggelectronics.com
Https://btbat.com
Https://woodmeister.com
Https://suburbanlabs.com
Https://fibertecinc.com
Https://nesg.org
Https://novosti-n.org
Https://novosti-n.org
Https://etisalat.a
Https://hrlt.com.au

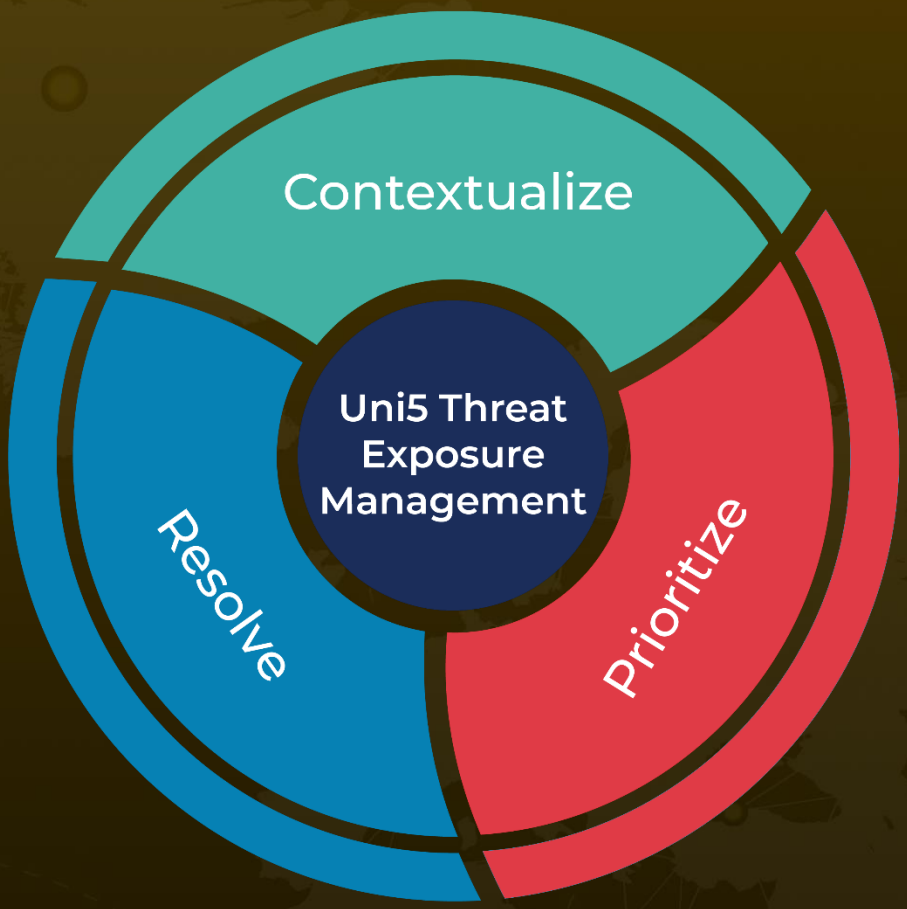
References

https://redacted.com/blog/bianlian-ransomware-gang-continues-to-evolve/
https://www.hivepro.com/multiple-industries-targeted-by-uptick-of-bianlian-ransomware/

What Next?

At **HivePro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **Hive Pro Uni5**: Continuous Threat Exposure Management Platform.



REPORT GENERATED ON

March 17, 2023 • 3:30 AM

More at www.hivepro.com