KPMG Cyber Threat Intelligence Platform

Blind Eagle - Exploiting Cloud Services for Cyber Espionage

TLP : Clear

KPMG. Make the Difference.

Blind Eagle (aka APT-C-36, AguilaCiega, APT-Q-98) is an advanced persistent threat group targeting government, financial, and critical infrastructure sectors in Colombia and Ecuador since 2018. The group has expanded its malware arsenal with a variant of PureCrypter and is possibly leveraging a packer-as-a-service (HeartCrypt) to enhance obfuscation and evasion. Additionally, Blind Eagle appears to have increased its adaptability by frequently rotating command-and-control (C2) infrastructure and potentially using compromised cloud storage services such as Google Drive for malware distribution, indicating an evolving threat landscape in the region.

Blind Eagle initiates its attack with spear-phishing emails containing a malicious .URL file designed to exploit CVE-2024-43451, an NTLMv2 hash disclosure vulnerability patched by Microsoft in November 2024. On vulnerable systems, the .URL file triggers a WebDAV request automatically, alerting attackers even before any user interaction. On patched systems, the infection only progresses when the user manually clicks the .URL file, leading to malware download. The malicious .URL file downloads a variant of PureCrypter, which executes payloads directly in-memory to evade detection. PureCrypter retrieves and deploys multiple remote access trojans (RATs), including Remcos RAT, NjRAT, and AsyncRAT, from Bitbucket, GitHub, or compromised Google Drive accounts. Remcos RAT establishes persistence by modifying Windows registry keys and creating scheduled tasks to ensure execution after system reboots. The malware communicates with command-and-control (C2) servers, allowing Blind Eagle to exfiltrate credentials, emails, and system data, as well as execute remote commands.

Blind Eagle's exploitation of legitimate file-sharing platforms constitutes a significant cybersecurity threat, demanding proactive defenses and constant vigilance.

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

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

Blind Eagle - Exploiting Cloud Services for Cyber Espionage

TLP : Clear

KPMG. Make the Difference.

Indicators of Compromise: IP Addresses

62.60.226[.]64

Indicators of Compromise: Domains

elyeso.ip-ddns[.]com

Indicators of Compromise: Hashes

35382198a1419bbc2eee2e193cc43c5d
ff4ce8c6f894f47c6f284ac6d19492ad
854c8933557334cb2f0e5dbe8ede11cb
16b605009baf2002cdab88ca597f22ee
21d52d07f0f04e0934011978a85e6a15
bb2acd12aef6bd62c14962b64da5a9bd
6f21738f94daf7b7a839d072852460e8
65458b9921380297e2ef212515f26948
d630835afafe3493e8d120210d56ce95
cc7a9d80a31e2e0d7811f5f83557735a
76a6a7d2ab9e95b28876139cd6a887ee
f22dd67bcd7aa0c59e841fa912fee583
51b5d48c1cb5c0e921622cf61889f031
e95b50d462bec50ead081c4e2b94202b
6df47a9484d9133d19da7de2479e0ce5
4b19fd700069414aef438426752ca3ee
290400014dd47271d6ed315d488f4b62
97de421bd63480e7e355155b622e2f54
8da55dfac2aa99abfaf63b35707cbc6a

Follow us on:
kpmg.com/in/socialmedia

KPMG

KPMG Cyber Threat Intelligence Platform

Blind Eagle - Exploiting Cloud Services for Cyber Espionage

TLP : Clear

KPMG. Make the Difference.

Indicators of Compromise: Hashes
af607da780ff1643acff911077859c2f
a29c364348da95d46906a3cd97d5d812
61f4ef2333a35bf80f1847bc9ed81688
9bf79297f1cb4d4558df34df6543629c
8f51f6f5288c7f7c5d25d2f978cb05c89c92fb40
e105142651cf7489bcf7caa7c4b29e0b247870ca
e82637a13fb2f791dc9c53416d3c7db942c900e1
82b3eedc49bfa287ca0debd41c9834b79eb4c185
bdcc654d04706ce9132b6ec88fcec6f1890ebf4c
06610beb1023ef579bc7505a70d4ac4d62becfdb
be3081db22763d3264bea34165e684e018bbb9dc
d140ebce995ff2a212ca507e82195a9c5633ea11
3df1878271206aa4d722aa32fa1803c8130e4059
ea5795d34522b6af9966497ba8385ed2da08f7b0
9ad312d7e13109329032a96116d496aa46528438
c6d673f1678cd9ac5f35b9203949a30e6476e986
93773632d065436990bec5c67cf06bd552149dd7
1d1e007a9d8939bee7a0333522cc4f7480d448cc
133bc4304057317b0b93f5ff44f20d153b985b50
1fcc44d3b20381acce66f5634743917e8f22dae7
a0338654304b6f824bdc39bbb482a0e114f8a3a1
07647f0eddf46d19e0864624b22236b2cdf561a1
08daf84d9c2e9c51f64e076e7611601c29f68e90
83c851f265f6d7dc9436890009822f0c2d4ba50a
33ddaedc98991435f740f7a5a8a931a8cadd5391
758c73ab9706ae6977f9b4601c20b3667836d3ef

Follow us on:
kpmg.com/in/socialmedia

KPMG

KPMG Cyber Threat Intelligence Platform

Blind Eagle - Exploiting Cloud Services for Cyber Espionage

TLP : Clear

KPMG. Make the Difference.

Indicators of Compromise: Hashes
b79de10cd30caadd4478064ae9d3ace4f20ff6de
4f82f428738e331cefd979be27e307b75c3290cf
e456762fd9366c34b848ff82e94604bc5b5f236f
ce327468e3b2748ca7dfabbd6e761e8dd8635c9e
d9328eabc7af75231c02757500ee1625b9db4c93
0c495951b812524b0d92c98755d7498fd87424f2
deb2f36614cb763e26482cb12318d29987292d0c
df5ab53da8c2913ea72dfe3bd31122d418c800a6
9da0d9124565af63d097e20cbb1946fe39d0986aceea180680d35ec03033cdca
9f4c9dda304fd58054423451e240ac61e8ce597a39cfd882351b8cd556f91331
a1f614bd8ce64fe9b165b0919eadbc626b34c21a64655f29da426ed65d5d12ca
a3dabca21d1b11071f6075269dae98942d9412d8914793d9a621007bafb9b52d
c9bb768c709927fee739b229deaa11c3713c8db00b9d6583b352226c01f770f9
eaa172d3c2d41f31fde710a9fcecef69a575c3b28d320189169d4e3ecc519d0b
efc7977c746ee61b576953513a0dc05fc9ae8e0490166bd03421121b60edce32
fd14da859c0f7fde6527db8c2b712737585a604f7606f961b4728a8c4701d329
021fb223e024f2e97a5bdde7ee0c669e581af3f7db63c2ec6db461178c1dfaa5
05184813ce52dd1d86d808e444e87f1e1ac6e0bf34460208b52852b963b86607
09c886ca2943a82bfdd9b86436747363467f019234f682b73827d8481dc08b03
13ad84b1c893f6b628c622b74bd1e300ff0b4a561ed4d5341c67cf5646a1a628
3019a38dc320ab563b3628f4c94363a2289d07d567bb72f15b1dd50b840ddefe
3f5aebcd4b96e70ce93a7e2de86559564850a9c425f7727ed480236e94b5893f
4ba7c0d32f870a1cea7ae630fc171a0f4c9b844a1f5f08bb322ee5e75713b93a
5c66a382f171162422ac869a48d2a2903a2c3a36280f4056da354b0706072f30
5f709b4c46af41aa77f59a486b95e6297d43c5e87984bf4cac7ffacff03bc4ec
63483c47375452defc26bc75fdae6f9e7054877a182dc9ab18eaa9921b910c9c

KPMG

KPMG Cyber Threat Intelligence Platform

Blind Eagle - Exploiting Cloud Services for Cyber Espionage

TLP : Clear

KPMG. Make the Difference.

Indicators of Compromise: Hashes
68ffe5e10f64256e4303a67d8174fae4e34b276626abca5a49268fb4a2ca1afa
6bf7e095fefd4540be63e3d630e45460be59eb9dfb2e97df2be60798b1796e58
6f3e81a2a2732b60736cf98ac192d48ac735c021ed4fc65e49a9f49bc2a21c4b
74ab680c1b6fd0daeb503c916258c22186e4f2c75325bf132c9c75bc3196b1c7
7790daa6919363d95e44145128c67d1002cd598746ae3daf7dc6d7dc781d5247
78c02913c8655b31c69c35d510ea9d925421964b56d225ae9e6704e5cd7b5e6d
81adb71ca743d1e8dfa2e56d9a049bf722276e129acd6c684d9d6c85dd02af89
96b279e1d8074821392b8f01c40981b7d4dc061eadad98305208000afba130ef
a091503006e3ba89247ea55799771c0a43a61713bd167256571a3f6f44655939
a56cb0647d59967ea6b49e76f870a4d9b315ad9aa6b982d9bbad14bccd61df35
a7358bb72d70cb4e90011f26b15ede41af271e63fe584635d8b638ec6e7babda
ab7719d622a3254ed7ea59f6ac88d472416bd31dbdc51066b6fcb4644406eb47
afe75789e1b12c98e308092b5dbc18b22fc2ea5db386015dd8f8f696bbc024fb
b06c94d478de44a5e27322852b3b497edaec55c87821de6af4e19edd32fd1ec5
cbadf79a7756da6f000fab3b9dd9bf17f799d35a019174ad2921f23b93b51f17
d1cd2ff5ce6946bfe36812f787b4ce4e5d4c133a085ccbe981fd2f16e75032f3
e32944abfe4d11cb0cf3f05d5d259520590e1ba4992919ecd08deec9de1b62a0
e6218c7793859bc7058ad00abb9e615dca0da896a6ccb53b0fef870e11166394
e6e6798be705f555d2346a7cff81c067a6e942b1d60a17f8e68b067602bebc56
ec1a6afb0f7ea668259e3f6872bda4da654d53f78c1baccb39071fa25988ddb3
f1feef1c385560a964aa32529e75dabc4a41893a0d098c37bb5b96598802a799
f694e70bdc4a10261ca5b8bcd65dfb5fbf60a56ad0401dd39b469a3d84f3848e
fa3de61fc30653fff80dfe10c644957ba3465ce28d1cc9dddde19f4b97ddf89
fbfbc78b2c47385a222e53ac5d24003155d73ca172f2967640f3541183c47d9a
9438c974f3cdefd5a097e55bde4734a2db9438be7c8012fa455d4d8bceb537ca
5cada311c0db4a8fe87a377b82f4ba9f686953ae98b59dd493d66da8927d9e68