KPMG Cyber Threat Intelligence Platform

Evasive Panda - Unmasking China's Geopolitical Cyber Spy

TLP : Clear

KPMG. Make the Difference.

Evasive Panda, also known as Bronze Highland, Daggerfly, or StormBamboo, is a China-affiliated APT group specializing in cyber espionage. Active since 2012, it targets individuals, government entities, and organizations opposing China's geopolitical interests. The group is known for advanced techniques, persistent intelligence gathering, supply chain compromises, and custom malware deployment. The countries targeted by the group include India, China, Tibet, Taiwan, Hong Kong, South Korea, Myanmar, Australia, the USA, and Vietnam.

Initial access to victims is achieved through the use of compromised websites to conduct watering-hole attacks and through supply-chain compromise. When a target navigates to an affected URL, they are redirected to a fake HTML page with a crash pop-up and are prompted to download a fix. Pressing this prompt triggers a script that downloads the payload, which includes the Evasive Panda backdoor, MgBot, and a newer variant, Nightdoor. These communicate with their C2 server to fetch further functionalities (e.g., Gmck.dll, Olck.dll), which are part of the CloudScout utilities that steal data from cloud services. These functionalities are dropped at a hardcoded path disguised as legitimate. The Gmck.dll and Olck.dll files contain the modules CGM and COL, which target Gmail and Outlook, respectively. These .dll files provide CGM and COL browser cookies from web browser database files in the form of a .dat configuration file, which is RC4 encoded using a key common to all CloudScout modules. Upon authentication, these modules extract email headers, bodies, and attachments from compromised accounts. The stolen data is encrypted, compressed, and exfiltrated in ZIP archives.

Evasive Panda's use of custom malware and supply chain exploits increases risks, highlighting the need for strong security and constant threat monitoring.

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

Evasive Panda - Unmasking China's Geopolitical Cyber Spy

TLP : Clear

KPMG. Make the Difference.

Indicators of Compromise: IP Addresses

122.10.90[.]12	122.10.88[.]226
103.96.128[.]44	

Indicators of Compromise: Hashes

011f7a50fd410bfa0666f1150b2c3351
13546e9d36effa74f971d90687b60ea6
b2a36442e68848944365d3d1b8b7554a
889a7ae42fb44390ab99af071dd3d6b0
07df8d223f8a370cd703d177d7e93a36
ae5d92ef69074050a822f6669fe267b6
f553ea019b79742eabcbacd387231623
cc6e4be68c511637a5727a2cc02c1161
166b0d75858ec81744921b133d72ab2d
624d58a9a56c0f0a5c4923557a99f808
c643ef13ab7d1f78c8a1fba2143311c0
963f9805fa2867df5d3d328c863f9dfa
c02b6a7cc4f4da2d6956049b90ff53ba
be17d056039267973e36043c678a5d56
678df4d276bea90b62036d47a7166a69
4c504e0ef91fc66a6d6c4e3d6b10fa18
d5cd5877cdeef31a0a1631057a14fa45
fe387599de816d6c8d7588bd18189930
3f3a560d8ee98df9c63ddf5c25c3aa38
60346e35e66e904ebedc8e7d67f5813d
bb3f710885a178523b284a5e07c0f37f
9c9d6a30bd4addf6ce5386c19bb234f3

Follow us on:
kpmg.com/in/socialmedia

KPMG

KPMG Cyber Threat Intelligence Platform

Evasive Panda - Unmasking China's Geopolitical Cyber Spy

TLP : Clear

KPMG. Make the Difference.

Indicators of Compromise: Hashes
8bd980204d5b27aec0f128fb6ad730ce
766bbadfce62075ab12b7cc5bbbf103a
b75c6f0c5863c00baef1b4dba7498a43
d7a70062736c8d34823cfb835cf5c34c
0e5b7dd17bea6fbb04d9372caa84f6e9
437c8066b76978ee963883e137eef57e
9f27e0798271b590a01463d4543df2ea
f29e438050cf287c2018d3f78d473ce3
4e1f5425d498d5088842ce4b7fe47529
652c96dd649c26b07752a6322056252f
b14d66dec5ab42df524739a168689be0
0d533b3902f1e50b8429a3383419197a
84f6b9f13cdcd8d9d15d5820536bc878cd89b3c8
c70c3750ac6b9d7b033addef838ef1cc28c262f3
812124b84c5ea455f7147d94ec38d24bdf159f84
ad6c84859d413d627ac589aedf9891707e179d6c
3dd958ca6eb7e8f0a0612d295453a3a10c08f5fe
547bd65eee05d744e075c5e12fb973a74d42438f
59aa9be378371183ed419a0b24c019ccf3da97ec
fa78e89ab95a0b49bc0663f7ab33aaf1a924c560
52fe3fd399ed15077106bae9ea475052fc8b4acc
1c7df9b0023fb97000b71c7917556036a48657c5
944b69b5e225c7712604efc289e153210124505c
82b99ad976429d0a6c545b64c520be4880e1e4b8
5748e11c87aeab3c19d13db899d3e2008be928ad
f0f8f60429e3316c463f397e8e29e1cb2d925fc2

KPMG

KPMG Cyber Threat Intelligence Platform

Evasive Panda - Unmasking China's Geopolitical Cyber Spy

TLP : Clear

KPMG. Make the Difference.

Indicators of Compromise: Hashes
10fb52e4a3d5d6bda0d22bb7c962bde95b8da3dd
e5214ab93b3a1fc3993ef2b4ad04dfcc5400d5e2
d60ee17418cc4202bb57909bec69a76bd318eeb4
2ac41ffcde6c8409153df22872d46cd259766903
0781a2b6eb656d110a3a8f60e8bce9d407e4c4ff
9d1ecbbe8637fed0d89fca1af35ea821277ad2e8
62b72607762e6b67e5bb66a5febadda72ff4fce88f996861b978a58cd418eeb1
ee6a3331c6b8f3f955def71a6c7c97bf86ddf4ce3e75a63ea4e9cd6e20701024
2c0cfe2f4f1e7539b4700e1205411ec084cbc574f9e4710ecd4733fbf0f8a7dc
d9eec27bf827669cf13bfdb7be3fdb0fdf05a26d5b74adecaf2f0a48105ae934
174a62201c7e2af67b7ad37bf7935f064a379f169cf257ca16e912a46ecc9841
cb7d9feda7d8ebfba93ec428d5a8a4382bf58e5a70e4b51eb1938d2691d5d4a5
b9f44273a1993d32c0dfbae59946e5e0811eb71dcb8924afbe9c5756693384db
6062e6f44c235bb4b0c22f6c473b2781ae381f38fcbee71e7bd51a2764875305
1f34527a01bd3c05affe6c90aeaea926f57efa2fac06859f8427988865ccd310
420700a96c1c0a136cff5445e4160b58316b5f837975bbd00f67007849af9459
73d50eabd0b377e22210490a06ecf2441191558d97ce14ba79517c0e7696318b
c55dc6adb0f8faa94650d379814c568ca55db3d50f8fb8c5b075a21955f76daf
eb540cf9833ab8bd901b48ef258c0e14eb91fb3118fa967a40cd64d8ab417fa9
88b0ee7273a91d92c3570dbc67896e15b53ca118d2b45e49a3489605cc26bf24
419311167faeee927763b67ce00dbd4491f18bb0dbac9236621faec9e6422fa9
115036c379d083cde6f1ad89bd02a90cbc2ee046cb576b830c1dffb1cb0a7f1f
3e92f35c3818be05033b9f6716fe4fc30d5a68f6e412422ad7c68c85d4451ae4
a0fe56ec6eb5cc433fdc9e3537e49b45c90ffe8df409a0f1b5844bc253d209ba
7294b1ceb43381845e2c836737b81970db87d43ed3a5b6d65a252a496efb2f25
8ebce3ceaf166fe2edab157b88aa84349d2d848242ff305cdc7edb6a34e5b72f

KPMG

KPMG Cyber Threat Intelligence Platform

Evasive Panda - Unmasking China's Geopolitical Cyber Spy

TLP : Clear

KPMG. Make the Difference.

Indicators of Compromise: Hashes
c449846edfd7dc49ca59e9c0af719c46eb73ee474ec18f9860db70599e50992e
a0b5863db12d6a77d51909803b1b89b606df748a3f053b5f324e30900cdcdbf4
e34edeb60c4cc90057d99c9faa6d85b6246f2d70c60cd1b74a61317df1cb7ee9
b9a14f62f6a84dc7bdfa518d6e41611e4301e913aca92a9e79462d47d8d5fe38
3a91d0b140fb39fc74dc3cee1dd506bad13ee1500cc4e554744afb8336a4e54d
77d88603c7d05c447229eb688717e93034098f7168a00b5075a35c2bbbc6277e
f18bca0882958d243abd1939ff2c693392cf6fd6256367b47feb5a415d99030b
50abc37272a0579cd1636ba9db09feca76a06ff66fd84ead444c26fdb49d4a23
ee4044364bf6b4ac0d2e7a9805a4d0f281af0fd5797bf2ff879ddf18f297f00d
2fe6ebc590c1bd7b84c28d1e429288930e182c5147b1a6e49e1a5d08450411ed
9d134fc0d1bad6de3e16ec99d5bc73574e8d48ce41cffa565c551c42b7eab344
c4372ea0411c4d42e28edd01b0777632786fea765b0162c64a027c0bf3fc6daf
11714fb1750bac7a0e27137b8d912906501a8a82a516344ed9c0ea7f72be272a
9bbd602fb6e583832d309a293ae3a51bbaaab008655e18bf5082761c80bd8341
2c5e6ebbad199c28f1375841165bca0a310aa78ad11168bfdd53c13fff78733a
539d0a317815953d0d0caaf2077251c4bb0107fd7af9dffc3dacef4428ff97b1
6248d68e6636d4769e66ec4be0b08e601b1a05c63bfa7457c508d7278c0d84a2
19590e6e92dffaa21ccce3f4123f6f854361c699185d058ea929e7e441bddfe8
88f29b4f7e23458da966553a637ef05a45869ec4df4fd3c19736ebb4449d19da
d91c95100288668e321bc04305f896c3038f46404b8ca7da4427f9bec4b25878
866134587921cf465cf92fc9385239fadd27cd412c5eadf5ba017086630fc8b1
b32bbc5767cdfa8ff481f3523e391d2e6e025d549298617b79eaeb83f3612dd3
f92a60d772da631dd0e925e36be12c6632b23fad993e3d23f97967352e0cb05c
f021a0e571ead8d43b6d9bdd0e90424ccf399276ce0b3b5e33332d12be902236
1bf43b48462ab6bf92989ba3b804df224c1d594fcecc99bc9f673f88c3698265
81044813cf55c2398d7e2179e75c06ed8bcbcfc0328f9e0e2cc0b67e2e3d2e4a