KPMG Cyber Threat Intelligence Platform

ChamelGang – The Shape-Shifting Cyber Menace

ChamelGang (aka CamoFei), a sophisticated APT group, identified in 2021 is allegedly believed to be linked to China. The group is known for its stealthy operations and cyber espionage, using advanced techniques to infiltrate and persist within networks, often disguising its activities within legitimate services and domains. It primarily targets critical infrastructure sectors such as government, energy, aviation, and healthcare across various countries including Russia, India, and the USA.

ChamelGang leverages commonly known vulnerabilities in public-facing applications such as Jboss Application Server and Microsoft Exchange to execute commands and deploy web shells. On IIS servers, they install “DoorMe v2”, a malicious backdoor disguised with modified timestamps to evade detection and achieves persistence with Cobalt Strike using a custom BeaconLoader malware, posing as OCI library files during MSDTC service restarts. They use HTTPS Beacons for connected hosts and SMB Beacons for isolated segments. Additionally, they employ their own tool, "LinuxPrivilegeElevator," for privilege escalation, supported by MGDrive malware for transferring tools during lateral movement. Utilizes the built-in Curl utility to verify command server accessibility and Fast Reverse Proxy, a public Golang tool, to route malicious traffic. Compiles system data into password-protected archive files using tools like 7zip and WinRAR. These files are then uploaded to compromised web servers and can be retrieved using wget utility or exfiltrated using MGDrive, ensuring ongoing communication with C2 servers. Finally, they deploy CatB ransomware to encrypt data across systems and demand ransom from victims.

The persistent and sophisticated attacks by ChamelGang APT emphasize the need for fortified security protocols and proactive threat intelligence to effectively mitigate and prevent future intrusions.

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

KPMG

KPMG Cyber Threat Intelligence Platform

ChamelGang – The Shape-Shifting Cyber Menace

Indicators of Compromise: IP Addresses	
45.91.24[.]73	91.204.227[.]130
42.99.116[.]14	103.80.134[.]159
185.225.19[.]61	172.104.109[.]12
115.144.122[.]8	103.151.228[.]119

Indicators of Compromise: Domains
resources.albaclass[.]com

Indicators of Compromise: Hashes
8dfeaaf7351f695024ed3604a4985e98
bd3f37243a1e4fc61a3d96cb1f47484a
4d626c627c13f4ad829ab48c2aa256d1
2643cff5746bfc546809bb29c2e57734
e6adf40a959308ea9de69699c58d2f25
88ef5955f8fa58e141da85580006b284
3ebdb5d27929f4a4f1a1adeae0894946
170c2837b98b08169ee0547215eea1ad
1208d5adf51df23a95f3104eb8aa8db0
46f15fed0162837a95c1827a25481547
7b5bbc29e6addfa1fdaea839e500f995
d30f5b6ce37f4072f46788b717f60393
9c5658ba8a8ab9e92c96f13247d3b17e
b9337830c32f71a6ecccec60ba42de00
06f80a09dae7f21401eb21431f9c6350
f86c9cbcda845027b1b6b0f775f2cd5d
edc87da8654e966bee0e5c9b92ed67cb
fdc120e54ec857017122380f29ce39a9
5a6baf931adad480b920394568c52a9d
4c573815a49c47ad453268a7a5016875
63d96f35ccb4361378a98b7d29f1528f
09959be9b5f8ca21caa55577ce620034632a3f92
0c762bff5b4a0bf5abbdf28afc15cfc6dce575b1
24eb404a8daaace36a2cf5fb0f7b8608d2a3963a

KPMG

KPMG Cyber Threat Intelligence Platform

ChamelGang – The Shape-Shifting Cyber Menace

Indicators of Compromise: Hashes
33009aaea3d58d8f72dfaf45dd8016707599d6c0
374882c4752a05ec52e41943d7e3de8c1cccef10
44759a6597bad3a287a7b82724a763208c599135
5c15b0ad93f2a4ae08a2a8e070afb99795855e0f
5d43ee1f75781033cd5accf298583529bdd12fa1
65867d738ee978811a098a766810726e39d1391e
782b157e901326d67a783e3e7dac9694a87dc7c2
951e603af10ec366ef0f258bf8d912efedbb5a4b
a2a81d5fcc0012e78fe4fe1b681a82c3158ce2bf
a566e410144d5972a92dc21de37e2b8617bfc347
a79bc5e91761c98d99dc028401cd284c3b340474
bd22ce42492bdad203ce1c712e075d422f70bbd3
c1eb7d5b772635d519cb6f4f575ada709d626c1a
db99fc79a64873bef25998681392ac9be2c1c99c
dcd3f2a8ec1e63cb1bfcaa622ae48373ce0a01ce
dfab55758b195d1d30d89ba9175da3a49dc180be
e7ee9c41a1137b50d81238ae35b927f6ebbaae83
efa16441d95984bb5b278aa510e9942a40356f84
f4529b672eec3f629184fa4c62c3743ae5354f95
15b0a25b4e55241b12d09633465d3109c324fb98
de8bf4153bd72ef668b9a60419794ccabbe87c4f
d4828b63b596cf8d069b97a8a9396928ec3ad216
19114f25a5681149ae3950fb0c52d59a69d031dc
1e12b053a643895e071be3538bb9950667134563
1fa6de645e7146a0a1b64e17d260546e598acd17
398c4c0ba6f5ea78175dd2846067f10d3864a2cc
57373d25527b3adf54eefcbfb69b41a513605af0
19114f25a5681149ae3950fb0c52d59a69d031dc
1e12b053a643895e071be3538bb9950667134563
1fa6de645e7146a0a1b64e17d260546e598acd17
57373d25527b3adf54eefcbfb69b41a513605af0
608c2a64c9d41b891c18cb682a01eabf035a7f50
398c4c0ba6f5ea78175dd2846067f10d3864a2cc
57373d25527b3adf54eefcbfb69b41a513605af0

KPMG

KPMG Cyber Threat Intelligence Platform

ChamelGang – The Shape-Shifting Cyber Menace

Indicators of Compromise: Hashes
608c2a64c9d41b891c18cb682a01eabf035a7f50
8052fcd408d9bd9e7594accdabb161ba8c4a9bd7
882efb1b8093c46223e71e2be353b6a95dc24e7a
8ce96c0eb64db6856908fde2a1e9bcc387ce2744
8e76a2cc57fa5390462839c0471f522db3882c66
9d1076b58f30142fe1c693b4edcec9816b3cb3c6
cf2b73f77761f4441f9c31512d58709f5d9d59eef6514857a5e37b8c4e956c3a
d80a112dbf9ccbf4ca8bcf7d34bc33840246dfce2da64d2bfbbdd8994173ba7e
0299ae439023fd43cf0459170b330b1686b76c5e2080c685ae82dd3a9f331632
f450c74a27c1a639bdafe04a0c542c68fa11927bfd8991e7c16e7d8840c2642d
66657c07c5fbdb807a3b8de77145c0f060eb32d3d91b6c8ec304b491af1e49d2
806761850d19f0cc9f41618e74db471e85c494e952f900f827c1779f2d1c4d31
f9d394a785d2f9475334d4c39e9d88a16b88b10bf0899327ce9a353a742113f7
fb26d7871c1e78a339327da930f88412de3eeb14b2b048b6163c3107bc75c84d
f93a822ebb5b246287cfc285e96d5f50e4a65b9f9ea6f5b998904bbfcd7567ec
2682c0b5cca25043b1ef1536cd234275d1c2ef653ba8162bb5a5ec199a88067e
49292dd838429bcf4aaf77ff6960156edaf1ec094ee4e6b9863c5d5fc9d32279
a9ac99942eea11a3a710d6e63284b9d1c0694b3340350be60f3c278a13178dc2
751a0c3cf357b48c4a4733d482f8ee92166a7abf6e3236719691a870dd767421
7604e9ecedf298907e537e50b9c74006640561b32265c3ebba38e587166f67ab
c700c772dc070c09dc380dc69803a0d93122bb70309ee4fbb04c41d8e18dbee9
4edfeba94d06ad9532088e32d27b044c72ab8555cccdaa4a06f9661994a6b55b
9990388776daa57d2b06488f9e2209e35ef738fd0be1253be4c22a3ab7c3e1e2
c2cce705c53c5d0d72b318a432e89a9fa5bbbe2780715b5662365dafbc2da3d8
8679c9e96394c39fa5eeb277a7e28313ef502be5d8401c43fa9955820962add0
c283ceb230c6796d8c4d180d51f30e764ec82cfca0dfaa80ee17bb4fdf89c3e0
da4698e14cd543721213ee240ab847d375b94494c5a7969ad31390f4ed7656df