KPMG Cyber Threat Intelligence Platform

Gelsemium APT - Deceptive Web Shells Unveiled

Gelsemium APT is a well-known and sophisticated Chinese-origin cyberespionage group that has been operating since 2014. The group has been very stealthy and operated covertly for many years, demonstrating their expertise and advanced technology while remaining under the radar. This threat actor targets a wide range of entities, including government institutions, electronics manufacturers, universities, and religious organizations, primarily in Southeast Asia and the Middle East. A recent campaign observed in the wild also featured multiple failed attempts of deploying IIS backdoor is believed to be linked to Gelsemium APT.

Initial access is achieved by conducting basic reconnaissance, exploit internet-facing servers, and deploy web shells like China Chopper, reGeorg & AspxySpy. Multiple unsuccessful attempts to deliver IIS backdoor were also observed during analysis. The web shells facilitate internal recon, conduct lateral movement via SMB and download additional tools. Before proceeding with further exploitation, threat actor checks internet connectivity by pinging Chinese websites. In recent campaigns, an executable is used to save an embedded OwlProxy DLL on compromised systems, enabling direct command execution through a hidden HTTP service. In case OwlProxy fails, the group switches to EarthWorm, a publicly accessible SOCKS tunneler that establishes a tunnel between the compromised network & an external C2. Proof-of-concept scripts like SpoolFool along with Potato Suite are used to exploit a Print Spooler vulnerability (CVE-2022-21999) to create a local administrator user and elevate privileges. Run-of-the-mill command and control infra is used by leveraging Cobalt Strike.

In the face of adversaries like Gelsemium, it is evident that relying on a single layer of security is insufficient. To effectively mitigate the threat, organizations should adopt a multi-layered defense approach.

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

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

KPMG Assurance and Consulting Services LLP, Lodha Excelus, Apollo Mills Compound, NM Joshi Marg, Mahalaxmi, Mumbai - 400 011 Phone: +91 22 3989 6000, Fax: +91 22 3983 6000.

This document is for e-communication only.

#KPMG josh

home.kpmg/in

Follow us on home.kpmg/in/socialmedia

KPMG

KPMG Cyber Threat Intelligence Platform

Gelsemium APT - Deceptive Web Shells Unveiled

Indicators of Compromise: IP Addresses
27.124.26[.]83
27.124.26[.]86

Indicators of Compromise: Hashes
1b167409f594ce3cac5dc0bb516743e8
31eb70dc11af05ec4d5cda652396970c
acdae8914ed98213f10518fe657f87bb
12b5f256f015a67753dc2c70c1c8e80a
3cbea05bf7a1affb821e379b1966d89c
ab9091f25a5ad44bef898588764f1990
4bafbdca775375283a90f47952e182d9
b8458d393443ca9b59f4d32a5d31e4f7
29274ca90e6dcf5ae4762739fcbadf01
056b431e7d1837728d5262fd4c5fe291
7b21a76c955b0eec20b1e181d9189b64
cf56cb65c4e5b4d7794147daeed0bf66
19afd572720b56cada666600945a4b75
0a55fea4cd5676ffda440f5b6909df8b
3915b9b2e55f9faf8d1a78bda2bbd9a8
7fe429afcd33e0528498ea238f865d6e
a0900cd756a056535e7326b4390160c8
b35d10caedd701bf1a502e377a09173f
11be56784340af177b9155c33c1184b4
11be56784340af177b9155c33c1184b4
e222758869452afcd795a798cdf6cffa4ad4a642
2aee1f5306e38d080d16a96b6c23895ffc6ee2fc
8f18618ca9084506d26b84330629c844a226f2ff
183a2bb4baa18461e47a21c2b4b62ef44187c374
95f90554fb2ef20a64be9f6e81ff35c353392093
c822f6100333e84bd0ec87675ca79d65cb01a01e
663a254350fbc379d8d7f69c50ead3117ee8b634
613efd1d13d461c7f0833c8c9410e0ccf414e7d9
e007edd4688c5f94a714fee036590a11684d6a3a

Indicators of Compromise: Hashes
e095249f9fe185a40f70be528e1cccab436d7946
8b8bc1708bc9bd19edd3a2424752401ef5f9b40e
c3f5d5d52890fe72bd2fc4c08aaf538da73016d7
7f7bd5ab5a608e68f7e14af926fc6505990effcc
9193e83d6faf1e43e75565337efd8409133a9fa7
52ab5645503ae1d5edd0b365e1128c96f2c5d40a
99d384721d29307e5dc67a743082867b96b08f69
3e5bb0354812935dc82ec1835c8f724daa58594b
9672f131f5837d4c7cf6ca9f786c21dabb4803e7
92106dca5459dd987a5d121671771e33314a7610
92106dca5459dd987a5d121671771e33314a7610
c254dc53b3cf9c7d81d92f4e060a5c44a4f51a228049fd1e2d90fafa9c0a44ee
c0a7a797f39b509fd2d895b5731e79b57b350b85b20be5a51c0a1bda19321bd0
b9a9e43e3d10cf6b5548b8be78e01dc0a034955b149a20e212a79a2cf7bee956
527063cb9da5eec2e4b290019eaac5edd47ff3807fec74efa0f1b7ddf5a1b271
fd0b9f09770685ed6f40ecabcd31bc467fa22801164b52fdc638334009b7c06f
77e82c3d5fea369f6598339dcd97b73f670ff0ad373bf7fc3a2d8586f58d9d32
f0761ad307781bdf8da94765abd1a2041ac12a52c7fdde85f00b2b2cab6d6ce8
29cc79a451f73bac43dbe9455d2184770beae69f4e6bc2d824abd2cfbedf53f1
3268f269371a81dbdce8c4eedffd8817c1ec2eadec9ba4ab043cb779c2f8a5d2
4dcdce3fd7f0ab80bc34b924ecaa640165ee49aa1a22179b3f580b2f74705dd9
17392669a04f17fda068d18ae5850d135f3912d08b4e2eee81fce915849887b3
3be95477e1d9f3877b4355cff3fbcdd3589bb7f6349fd4ba6451e1e9d32b7fa6
181feef51991b162bdff5d49bb7fd368d9ec2b535475b88bc197d70d73eef886
ff7485d30279f78aba29326d9150b8c302294351e716ece77f4a3b890008e5fe
2f3abc59739b248ee26a575700eef93b18bd2029eb9f8123598ffdd81fa54d8b
c7bd78b9a68198b8787d28ba5094827eb99a0798719bcb140f3afb695925566c
24eb9c77448dda2d7cfecc60c804a378e89cbd450fbf7f4db875eb131cd4510a
96bc4853d5a0c976fb7a02d747cd268fb2dfc8c2361d68bb4ffcc16adec5ea19
ac115bfa8d36cf31046b8ccce30e9ebcede899395d56400955f95e242d5c9c75
61de79db5ed022ee9376e86a2094a51cf3b31fa6bce126cbcdacad33469c752f
29e78ca3cb49dd2985a29e74cafb1a0a15515670da0f4881f6095fb2926bfefd
552388d74478a84b8e64e3ee2316331740a0d060f322e92b5c608ea745adba90
fe71b66d65d5ff9d03a47197c99081d9ec8d5f6e95143bdc33f5ea2ac0ae5762