KPMG

KPMG Cyber Threat Intelligence Platform

Unfading Sea Haze – Maneuvers Across the South China Sea

Unfading Sea Haze, a cyber threat group that emerged in 2018, has been actively targeting high-level military and government entities in countries surrounding the South China Sea. While the group's origins and affiliations remain undisclosed, their activities bear resemblance to those aligned with Chinese interests, evident from victimology patterns and the utilization of Gh0st RAT malware commonly associated with Chinese-speaking threat actors.

The group gains initial access through undisclosed methods, including spear-phishing emails with malicious archives. These archives conceal LNK files that trigger PowerShell commands, initiating a fileless attack using MSBuild.exe. The attack halts if ESET's "ekrn.exe" is detected. Malicious code from a remote SMB share activates 'SerialPktdoor', granting remote control over the compromised system without leaving traces. Persistence is established through scheduled tasks mimicking legitimate Windows files, combined with DLL sideloading techniques to execute malicious payloads. The attackers manipulate local Administrator accounts, enabling and resetting passwords while hiding the accounts from the login screen. In a departure from typical nation-state actor tactics, the group incorporates commercially available Remote Monitoring and Management (RMM) tools like ITarian RMM for network access. The attackers employ a variety of custom and off-the-shelf tools for data collection, including keyloggers, browser data stealers, and USB/WPD monitors. Data exfiltration initially relies on a custom tool named DustyExfilTool but transitions to curl and FTP with dynamically generated credentials for improved operational security.

The Unfading Sea Haze group's use of modular tactics shows their determination to bypass traditional security, hence necessitating a proactive and adaptable defense strategy from organizations.

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

Sony Anthony
Partner, KPMG in India
T: +91 98455 65222
E: santhony@kpmg.com

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

B V, Raghavendra
Partner, KPMG in India
T: +91 98455 45202
E: raghavendrabv@kpmg.com

Chandra Prakash
Partner, KPMG in India
T: +91 99000 20190
E: chandraprakash@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

Unfading Sea Haze – Maneuvers Across the South China Sea

Indicators of Compromise: IP Addresses	
45.61.137[.]109	128.199.66[.]11
192.153.57[.]24	139.59.107[.]49
112.113.112[.]5	167.71.199[.]105
159.223.78[.]147	164.92.146[.]227
209.97.167[.]177	152.42.198[.]152
188.166.224[.]242	128.199.166[.]143
193.149.129[.]128	

Indicators of Compromise: Domains
bitdefenderupdate[.]org

Indicators of Compromise: Hashes
6a0933d08d8d27165f72c53df8f1bf04
1dbcd8d2f5718fa7654f8b5f34b88d43
1ce17f0e2a000a889b3f81e80b95f19f
2e4055e16c1a9274caa182223977eda1
1e55bda0b7eb0aea78577a21f51e8f5c
b3dc2dcb0f2a5661aed1f4e6d9e88bc6
124bdaaa70da4daeacbc0513b6c0558e
e7433f8a0943a6025d43473990ec8068
cb95ad8fad82eac1c553cd2d7470100b
19dbf2d82f6f95a73f1529636e775295
ac7b8524098cbb423619706ff617b6a6
95701a74b6b3de68fc375cd08ae8d2c2
7e10d7dd09f5ee2010990701db042f11
a5af41fda8ef570fda96c64a932d4247
5421e3cef32e534fa74a26df1c753700
4d99127e4b1d27a56f7c4b198739176b
5bd1eb1166da401c470af2b9e204b2d1
2c45c1c35c703bb923b558343f00ea34
70773eb54234c486c46048ade57db45b
69310040e872806cb2b00d3addb321a7

KPMG

KPMG Cyber Threat Intelligence Platform

Unfading Sea Haze – Maneuvers Across the South China Sea

Indicators of Compromise: Hashes
35623ba9f8fcbcf0fce96aa2465b0b66
828faccaaf8e70be1c32ae5588d3df12
4ec62fdd3d02bc9b81a8c78910b8463a
cff31de1b28f6b00d13d15c2be08a982
7ff8a134c1ee44c915339a74e4a2d3ca
0dd4603f7c3a80a2408e458fe58b2e60
11c7f264184ed52df4a3836a623845c8
55a246ace9630b31c43964ebd551e5e2
8c31532f73671995d7f3b6d5814ba726
5268206fb6c96f614f67cd5d686f42af
cf2f7331a04bb9cd47b58a5c80d4c242
3d87f0bd243cff931bb463fce1d115e3
98de3eeda1adefec31d3e3f00079dd2d
b04d9dba3bc922a33c1408d4fbf80678
35a307b73849a3d7a7cd603a0c4698f2
3d879bc2fb28c5abbcd6e08b6e5dc762
7aba74bfbf5cb068fb52e8813c40f4cd
510c36c9061778d166e23177a191df35
b6cd3d88a6d6886718b6113147a99901
1179f589791c2eaa1ae33f38e62753d0
0b744f9d38e125cd4fe14289272ac0e2
960a964cab127c4f3c726612fdeaeb08
1d2185c956a75a8628e310a38dea4001
7169179cc18e6aa6c2c36e4bee59f63d
cf398f9780de020919daad9ca4a27455
96a43d13fd11464e9898af98cc5bb24b
14a88779c7e03ecfc19dd18221e25105
2bf96bd44942ca8beed04623a1e19e24
fabdf1094b49673bc0f015cbb986bad5
00bcbeb6ffdadc50a931212eff424e19
e5fc13c39dd81e6de11d1c211f4413ba
9425f9f7cc393c492deb267c12d031c5
551bda0f19bf2705f5f7bd52dcbc021f
654163ab9002bd06f68a9f41123b1cd4

KPMG

KPMG Cyber Threat Intelligence Platform

Unfading Sea Haze – Maneuvers Across the South China Sea

Indicators of Compromise: Hashes
fda22f52f0d3a81f095a00810a3dd70a
cf5f2e3e1ce82e75a2d0885af5efa1ef
3631001b60bdf712e6294d40ec777d87
4e470ea6d7d7da6dd4147c8e948df7c8
73daf06fed93d542af04d59a4545fab0
100c461d79471c96eba20c8eae35c5ba
40466fd795360ac4270751d8c4500c39
cb9e6fa194b8fa2ef5b6b19e0bd6873e
af215f4670ae190e699c27e5205aadee
39d43f21b3c2b9f94165f5257b229fb4
3dc8d8a70cc60a2376ce5c555d242cf3
6f01bed0b875069ec5b9650e6d8c416f
5f8f9269bcd52ef630bc563b83059b77
fa93aec0018c5e3d1d58b76af159bb82
846838327cda19b4415afd5b352c95df
17303b1a254abb9ed0795f7d9b51b462
3decde2a91f52255dd97eaafc2666947
b98e54d01a094bb6b83eff06a8cf49d6
b1a886f8904d90ad28fce0dc0dc9df93
5800fff782c36df785dad1d0a34ad418
a23704a9a673dc1de624dc80e441d18ebb0c5fb8
fb308d20f5321b1217de2d92fc84dc0536a1437a
d421830cc2c1a04dd89c94bee0714ef805fa6c4c
ed389a02b46cb203a2308aac5722176766936234
d353bb3f4ce1e25e6f641013ee1db442140fc130
7c1a3c5c016209a502fe5157b7c525c6b079d79b
4df94ae575587d83bc4cd977761d3530370da191
1116efd48ca01623bf385cd612f4da1eb9eeba0329e41d0e068bcd6557a46f8f
530101bcf9aa5de8aa28d383d1b7c84cd9f7b7e4a3a9cffd12a2912c9ac01adf
6b5b8b12af21700a212d5ece27f065f8f9ed38b2969ad5dfaa790bc76754de6c
93abcc4062a14ba3d3309fc5e8a910e81a4e3ce1bbbf5e6f7857779b6e76f43a
9fc446be8d03a135f901ba77cce1f39bb609d8e9ee3101399fa7e9e73299d379
7587ca6b8163e3e5b05e4a9fc79ec19deee9c971e6f76adadc4d970c99cad4f3
87a547e50c9f8c08b49410131cf96213910a238ae2dd81815902fd5b5002fe52