KPMG

KPMG Cyber Threat Intelligence Platform

Mango Sandstorm - Rapidly Leveraging Latest Exploits

Mango Sandstorm, aka MERCURY, UNC3313, Muddy Water, Earth Vetala, Static Kitten and Seedworm operates as an Iranian APT group affiliated with the Iranian Ministry of Intelligence and Security (MOIS). Active since 2012, Mango Sandstorm has been keen on including newly released POC exploits as part of their attack chain. Having exploited multiple Microsoft Exchange vulnerabilities and Apache log4j in the past, the group is currently targeting the recently reported Papercut vulnerabilities. Targeted regions of interest includes Pakistan, UAE, Israel, Turkey and US, impacting sectors such as education, energy, healthcare and finance.

Initial access by exploiting unpatched papercut vulnerabilities (CVE-2023–27350, CVE-2023–27351) recently or via phishing emails with links to drop web shells or various malware loaders respectively. Post gaining initial access, performs basic system and network discovery and looks for Active Directory information to pivot to. Utilizes SimpleHelp remote access tool to covertly access the victim machine, maintain persistent access and to execute commands. Creates new local admin user account and copies malware tools to the startup folder while modifying registry keys to ensure persistence on reboot. Executes malicious binaries via DLL side-loading to avoid any alert and dumps credentials using Mimikatz. Also, leverages WMI utility or pre-deployed remote service tools if any, to move laterally within the environment. Modifies security settings via Group Policy Objects & uses PowerShell scripts to evade defenses. Known to leverage tools such as Ligolo, eHorus, etc. and DNS tunnelling for data exfiltration.

With threat groups proactively leveraging newly disclosed vulnerabilities, it’s becoming highly important to be on the lookout for the same and prioritize patch updates for better defense.

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

Mango Sandstorm - Rapidly Leveraging Latest Exploits

Indicators of Compromise: IP Addresses	
95.181.161[.]81	5.199.133[.]149
185.118.164[.]195	185.183.97[.]25
178.32.30[.]3	88.119.170[.]124

Indicators of Compromise: Hashes
a0421312705e847a1c8073001fd8499c
51bc53a388fce06487743eadc64c4356
b6b0edf0b31bc95a042e13f3768a65c3
52299ffc8373f58b62543ec754732e55
d68f5417f1d4fc022067bf0313a3867d
c0c2cd5cc018e575816c08b36969c4a6
37fa9e6b9be7242984a39a024cade2d5
0431445d6d6e5802c207c8bc6a6402ea
5f71191ca2aff4738d9ca86e884e9afa
cb84c6b5816504c993c33360aeec4705
e1f97c819b1d26748ed91777084c828e
e182a861616a9f12bc79988e6a4186af
b3504546810e78304e879df76d4eec46
69ff29b86ab5444197aeb0cf5eba0967
887f345dce4426b9c841c7fde581b18f
218d4151b39e4ece13d3bf5ff4d1121b
6c084c8f5a61c6bec5eb5573a2d51ffb
a65696d6b65f7159c9ffcd4119f60195
4a022ea1fd2bf5e8c0d8b2343a230070
0ac499496fb48de0727bbef858dadbee
a16f4f0c00ca43d5b20f7bc30a3f3559
8344f2c1096687ed83c2bbad0e6e549a71b0c0b1
81f46998c92427032378e5dead48bdfc9128b225
6c55d3acdc2d8d331f0d13024f736bc28ef5a7e1
28e799d9769bb7e936d1768d498a0d2c7a0d53fb
61608ed1de56d0e4fe6af07ecba0bd0a69d825b8
570f7272412ff8257ed6868d90727a459e3b179e
89df0feca9a447465d41ac87cb45a6f3c02c574d

Indicators of Compromise: Hashes
483cd5c9dd887367793261730d59178c19fe13f3
94e26fb2738e49bb70b445315c0d63a5d364c71b
3204447f54adeffb339ed3e00649ae428544eca3
b9e6fc51fa3940fb632a68907b8513634d76e5a0
5168a8880abe8eb2d28f10787820185fe318859e
ca97ac295b2cd57501517c0efd67b6f8a7d1fbdf
2f6dd6d11e28bf8b4d7ceec8753d15c7568fb22e
47a4e0d466bb20cec5d354e56a9aa3f07cec816a
0211569091b96cffab6918e18ccc97f4b24d88d4
3765c1ad8a1d936aad88255aef5d6d4ce24f94e8
fa73bee345b6f5d214917b5425bb2a6bd9b45de7
9f212961d1de465c20e84f3c4d8ac0302e02ce37
4209a007fcf4d4913afad323eb1d1ae466f911a6
69840d4c4755cdab01527eacbb48577d973f7157
d02d93b707ac999fde0545792870a2b82dc3a238
4808cae5e9684e691490a652a93a56005d603643
59ae2ee86e7f9f90fc3c5737355e88b59b00fa2a
12db8bcee090521ecf852bf215ce3878737517a22ef1f2ff9bdec7cba8d0d3aa
dd7ee54b12a55bcc67da4ceaed6e636b7bd30d4db6f6c594e9510e1e605ade92
9d50fcb2c4df4c502db0cac84bef96c2a36d33ef98c454165808ecace4dd2051
2471a039cb1ddeb826f3a11f89b193624d89052afcbee01205dc92610723eb82
7e7545d14df7b618b3b1bc24321780c164a0a14d3600dbac0f91afbce1a2f9f4
b5b1e26312e0574464ddef92c51d5f597e07dba90617c0528ec9f494af7e8504
e7baf353aa12ff2571fc5c45184631dc2692e2f0a61b799e29a1525969bf2d13
255e53af8b079c8319ce52583293723551da9affe547da45e2c1d4257cff625a
5bcdd422089ed96d6711fa251544e2e863b113973db328590cfe0457bfeb564f
9cb79736302999a7ec4151a43e93cd51c97ede879194cece5e46b4ff471a7af7
9ec8319e278d1b3fa1ccf87b5ce7dd6802dac76881e4e4e16e240c5a98f107e2
b6133e04a0a1deb8faf944dd79c46c62f725a72ea9f26dd911d6f6e1e4433f1a
ce9bd1acf37119ff73b4dff989f2791eb24efc891a413df58856d848f0bcaee9
e7f6c7b91c482c12fc905b84dbaa9001ef78dc6a771773e1de4b8eade5431eca
b1e30cce6df16d83b82b751edca57aa17795d8d0cdd960ecee7d90832b0ee76c
42ca7d3fcd6d220cd380f34f9aa728b3bb68908b49f04d04f685631ee1f78986
3098dd53da40947a82e59265a47059e69b2925bc49c679e6555d102d1c6cbbc8

Indicators of Compromise: Hashes
d77e268b746cf1547e7ed662598f8515948562e1d188a7f9ddb8e00f4fd94ef0
ed988768f50f1bb4cc7fb69f9633d6185714a99ecfd18b7b1b88a42a162b0418
c2badcdfa9b7ece00f245990bb85fb6645c05b155b77deaf2bb7a2a0aacbe49e
f10471e15c6b971092377c524a0622edf4525acee42f4b61e732f342ea7c0df0
cc67e663f5f6cea8327e1323ecdb922ae8e48154bbf7bd3f9b2ee2374f61c5d6
a500e5ab8ce265d1dc8af1c00ea54a75b57ede933f64cea794f87ef1daf287a1
fb69c821f14cb0d89d3df9eef2af2d87625f333535eb1552b0fcd1caba38281f