Researchers Warn of Chinese-Aligned Hackers Targeting South China Sea Countries

Date: 24th May 2024 | Severity: Medium

Summary

Cybersecurity researchers have disclosed details of a previously undocumented threat group called Unfading Sea Haze that's believed to have been active since 2018. The intrusion singled out high-level organizations in South China Sea countries, particularly military and government targets, Bitdefender said in a report shared with The Hacker News.

Attack Vectors

- "Notably, the attackers repeatedly regained access to compromised systems. This exploitation highlights a critical vulnerability: poor credential hygiene and inadequate patching practices on exposed devices and web services."
- There are some indications that the threat actor behind the attacks is operating with goals that are aligned with Chinese interests despite the fact that the attack signatures do not overlap with those of any known hacking crew.
- This includes the victimology footprint, with countries like the Philippines and other organizations in the South Pacific previously targeted by the China-linked Mustang Panda actor. Also used in the attacks are various iterations of the Gh0st RAT malware, a commodity trojan known to be used by Chinese-speaking threat actors.
- "One specific technique employed by Unfading Sea Haze – running JScript code through a tool called SharpJSHandler – resembled a feature found in the 'FunnySwitch' backdoor, which has been linked to APT41," Bitdefender said. "Both involve loading .NET assemblies and executing JScript code. However, this was an isolated similarity."
- The exact initial access pathway used to infiltrate the targets is currently known, although, in an interesting twist, Unfading Sea Haze has been observed regaining access to the same entities through spear-phishing emails containing booby-trapped archives.
- These archive files come fitted with Windows shortcut (LNK) files that, when launched, set off the infection process by executing a command that's designed to retrieve the next-stage payload from a remote server. This payload is a backdoor dubbed SerialPktdoor that's engineered to run PowerShell scripts, enumerate directors, download/upload files, and delete files.

Indicator of compromise

INDICATOR TYPE	INDICATORS
File Hash	• ed389a02b46cb203a2308aac5722176766936234 • 73daf06fed93d542af04d59a4545fab0 • 551bda0f19bf2705f5f7bd52dcbc021f • a5af41fda8ef570fda96c64a932d4247 • 93abcc4062a14ba3d3309fc5e8a910e81a4e3ce1bbbf5e6f7857779b6e76f43a • 55a246ace9630b31c43964ebd551e5e2 • 124bdaaa70da4daeacbc0513b6c0558e • 40466fd795360ac4270751d8c4500c39 • 2bf96bd44942ca8beed04623a1e19e24 • 96a43d13fd11464e9898af98cc5bb24b • 4ec62fdd3d02bc9b81a8c78910b8463a • a23704a9a673dc1de624dc80e441d18ebb0c5fb8 • 7e10d7dd09f5ee2010990701db042f11 • cb9e6fa194b8fa2ef5b6b19e0bd6873e • d9a452c1c06903fafa4dc4625b2c2d9b • b98e54d01a094bb6b83eff06a8cf49d6 • 1116efd48ca01623bf385cd612f4da1eb9eeba0329e41d0e068bcd6557a46f8f • c182b3e659a416fe59f3613c08a8cffb
IP Address	• 192[.]153.57.24 • 188[].166.224.242 • 209[.]97.167.177 • 164[.]92.146.227 • 193[.]149.129.128 • 45[.]61.137.109 • 128[.]199.66.11 • 112[.]113.112.5 • 167[.]71.199.105 • 139[.]59.107.49 • 128[.]199.166.143 • 159[.]223.78.147 • 152[.]42.198.152

Recommendation

- Submit the File Hash to the Antivirus team to update their database with the file hashes and block IPs.
- Avoid browsing the unsafe websites, clicking on suspicious links, or opening unknown email attachments.
- Update and Patch operating system, applications, and security software's up to date with latest patches.

NOTE: The recommended settings/controls should be implemented after due shall be tested on Pre-Prod or test environment before implementing. diligence and impact analysis.

Reference Links

- https://thehackernews[.]com/2024/05/researchers-warn-of-chinese-aligned[.]html
- https://www[.]bitdefender[.]com/blog/businessinsights/deep-dive-into-unfading-sea-haze-a-new-threat-actor-in-the-south-china-sea/