Newly Detected Chinese Group Targeting Military, Government Entities

By Ionut Arghire

Published: 2024-05-23 · Archived: 2026-04-05 17:31:38 UTC

A Chinese threat actor has been targeting military and government entities in South China Sea countries for at least six years, Bitdefender reports.

Dubbed Unfading Sea Haze (PDF), focused on espionage, and capable of regaining access to the compromised environments, the hacking group has remained under the radar since 2018 using new and improved tools, tactics, and techniques (TTPs).

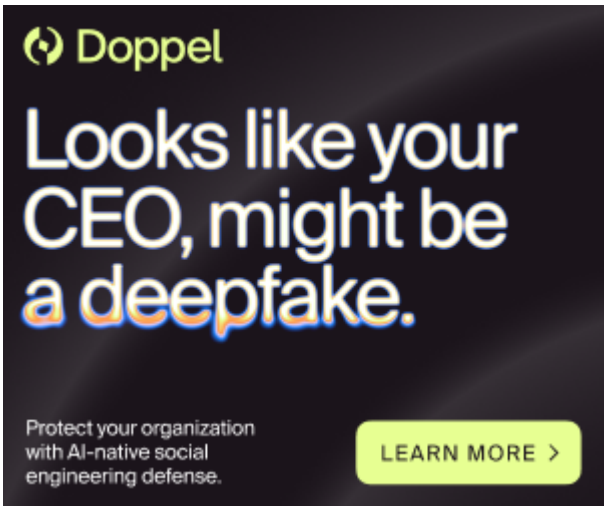
While the initial intrusion vector employed by Unfading Sea Haze is not known, the threat actor has been observed employing spear-phishing in some attacks, followed by the deployment of custom malware and tools.

Spear-phishing emails employed in attacks over the past year included malicious archives containing LNK files designed to execute malicious commands instead, leading to the deployment of malware.

For persistence, Unfading Sea Haze used scheduled tasks coupled with the manipulation of local administrator accounts. The attackers attempted to enable/disable the administrator accounts, reset its password, and hide it from the login screen.

Additionally, the threat actor has been observed using commercially available remote monitoring and management (RMM) tools, such as ITarian RMM, to gain access to the victim networks.

Advertisement. Scroll to continue reading.



“We also found evidence suggesting the attacker may have established persistence on web servers, including both Windows IIS and Apache httpd. Potential methods include web shells or malicious modules designed for these

web server platforms (IIS modules and httpd modules),” Bitdefender notes.

Between 2018 and 2023, Unfading Sea Haze relied on two Gh0st RAT variants named SilentGh0st and TranslucentGh0st, and on variants of the .NET agent SharpJSHandler, which was supported by a loader named Ps2dllLoader to execute payloads in memory.

Last year, the threat actor replaced Ps2dllLoader with a new fileless attack mechanism and switched to more modular (plugin-based) variants of Gh0st RAT, namely FluffyGh0st, InsidiousGh0st, and EtherealGh0st.

The backdoors support commands for file and folder manipulation, command execution, file download and upload, and data harvesting, but the adversary was also seen employing other custom malware and various tools for keylogging, browser data harvesting, and data exfiltration.

According to Bitdefender, Unfading Sea Haze has hit at least eight government and military organizations in the South China Sea region, and its activities appear aligned with Beijing’s interests, suggesting it could be a nation-state adversary operating out of China.

Furthermore, the use of Gh0st RAT variants has been linked to Chinese threat actors before, and the sharing of resources between Chinese hacking groups, as well as overlaps with APT41’s tooling reinforce the assumption that Unfading Sea Haze is a Chinese adversary.

Related: Chinese Hackers Have Been Probing DNS Networks Globally for Years: Report

Related: Chinese Cyberspies Targeting ASEAN Entities

Related: Chinese APT Hacks 48 Government Organizations

Source: https://www.securityweek.com/newly-detected-chinese-group-targeting-military-government-entities/