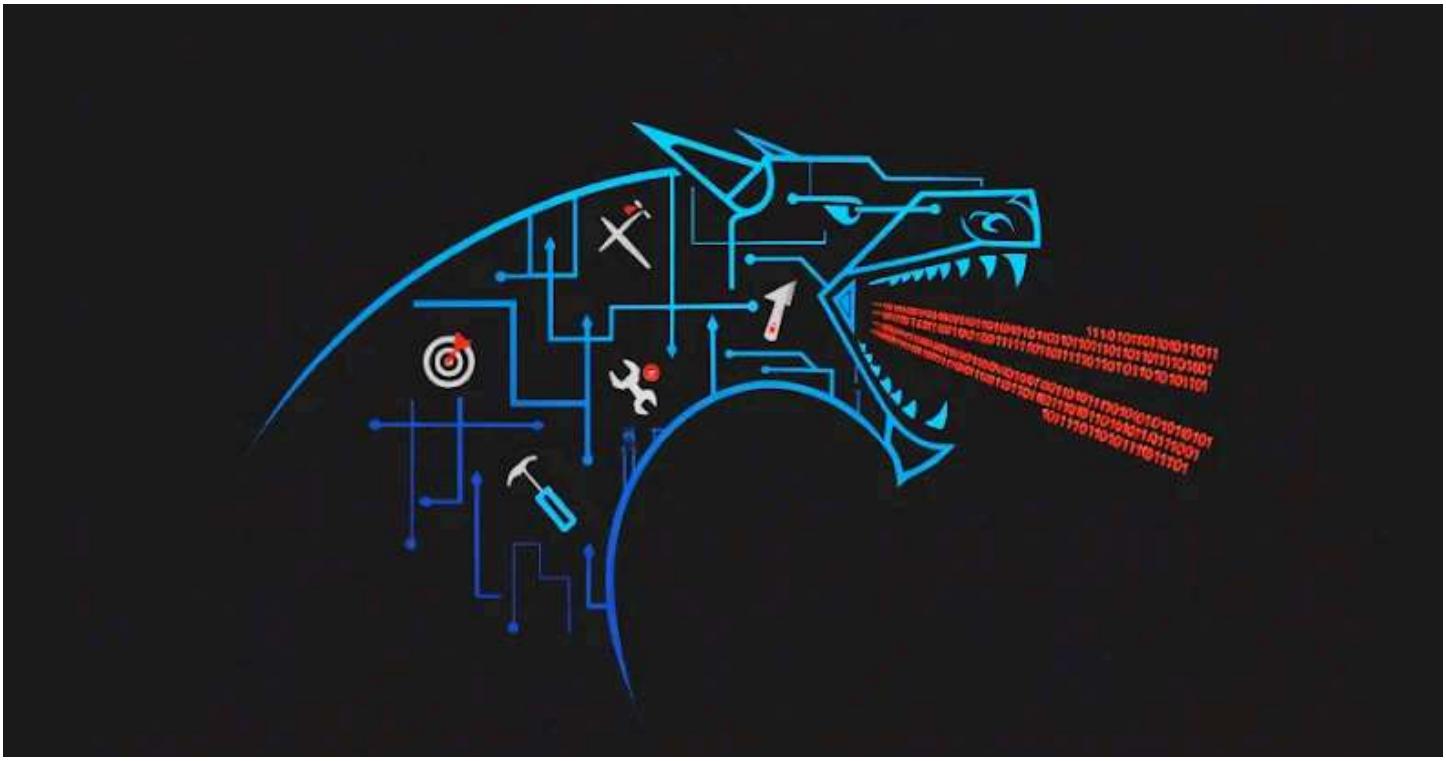
Chinese Hackers Weaponize Open-Source Nezha Tool in New Attack Wave

Oct 08, 2025 Ravie Lakshmanan



Threat actors with suspected ties to China have turned a legitimate open-source monitoring tool called Nezha into an attack weapon, using it to deliver a known malware called Gh0st RAT to targets.

The activity, observed by cybersecurity company Huntress in August 2025, is characterized by the use of an unusual technique called log poisoning (aka log injection) to plant a **web shell** on a web server.

"This allowed the threat actor to control the web server using **ANTSWORD**, before ultimately deploying Nezha, an operation and monitoring tool that allows commands to be run on a web server," researchers Jai Minton, James Northey, and Alden Schmidt **said** in a report shared with The Hacker News.

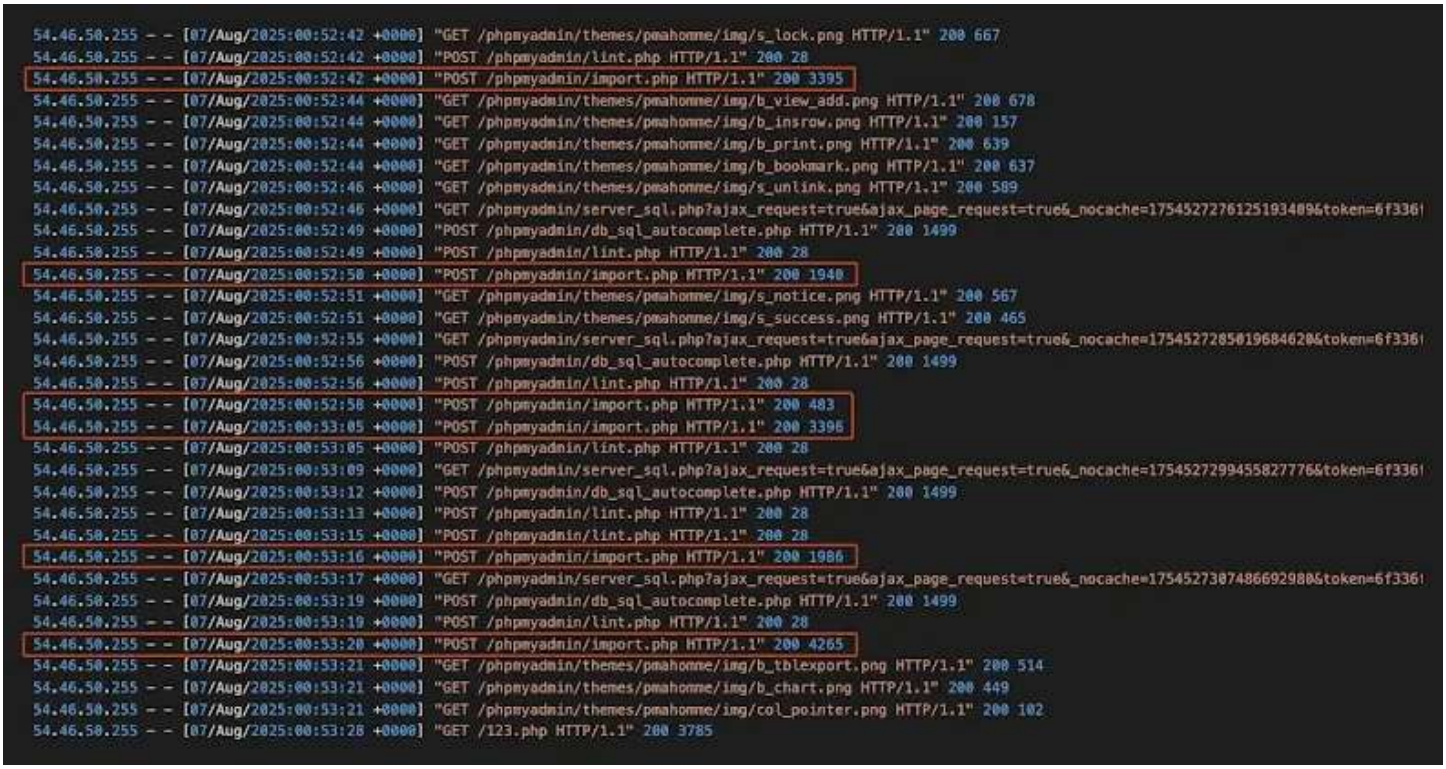
In all, the intrusion is said to have likely compromised more than 100 victim machines, with a majority of the infections reported in Taiwan, Japan, South Korea, and Hong Kong.

"The activity has been going on since at least June of 2025 but it may have been longer," Minton, principal security operations analyst at Huntress, told The Hacker News. "This is assessed based on the first seen timestamps of systems connecting back to the threat actor's Nezha dashboard which is also a good indication of when the individual systems were breached."

The attack chain pieced together by Huntress shows that the attackers, described as a "technically proficient adversary," leveraged a publicly exposed and vulnerable phpMyAdmin panel to obtain initial access, and then set the language to simplified Chinese.

The cybersecurity company said, while it has not observed other initial access vectors, it assessed with high confidence that there are other methods the threat actors are using to break into networks of interest. "This is assessed based on the metadata of the diverse systems which the threat actors Nezha agent was installed on which indicate some systems we wouldn't necessarily expect to be running a phpMyAdmin panel," it said.

The threat actors have been subsequently found to access the server SQL query interface and run various SQL commands in quick succession in order to drop a PHP web shell in a directory accessible over the internet after ensuring that the queries are logged to disk by enabling general query logging.



"They then issued a query containing their one-liner PHP web shell, causing it to be recorded in the log file," Huntress explained. "Crucially, they set the log file's name with a .php extension, allowing it to be executed directly by sending POST requests to the server."

The access afforded by the ANTSWORD web shell is then used to run the "whoami" command to determine the privileges of the web server and deliver the open-source Nezha agent, which can be used to remotely commandeer an infected host by connecting to an external server ("c.mid[.]al").

An interesting aspect of the attack is that the threat actor behind the operation has been running their Nezha dashboard in Russian, with over 100 victims listed across the world. A smaller concentration of victims is scattered across Singapore, Malaysia, India, the U.K., the U.S., Colombia, Laos, Thailand, Australia, Indonesia, France, Canada, Argentina, Sri Lanka, the Philippines, Ireland, Kenya, and Macao, among others.

The Nezha agent enables the next stage of the attack chain, facilitating the execution of an interactive PowerShell script to create Microsoft Defender Antivirus exclusions and launch Gh0st RAT, a malware widely used by Chinese hacking groups. The malware is executed by means of a loader that, in turn, runs a dropper responsible for configuring and starting the main payload.

"This activity highlights how attackers are increasingly abusing new and emerging publicly available tooling as it becomes available to achieve their goals," the researchers said.

"Due to this, it's a stark reminder that while publicly available tooling can be used for legitimate purposes, it's also commonly abused by threat actors due to the low research cost, ability to provide plausible deniability compared to bespoke malware, and likelihood of being undetected by security products."

(The story was updated after publication to include additional insights from Huntress.)

Found this article interesting? Follow us on Google News, Twitter and LinkedIn to read more exclusive content we post.