Hive Pro

Threat Level

Amber

Hiveforce Labs

# THREAT ADVISORY

## ATTACK REPORT

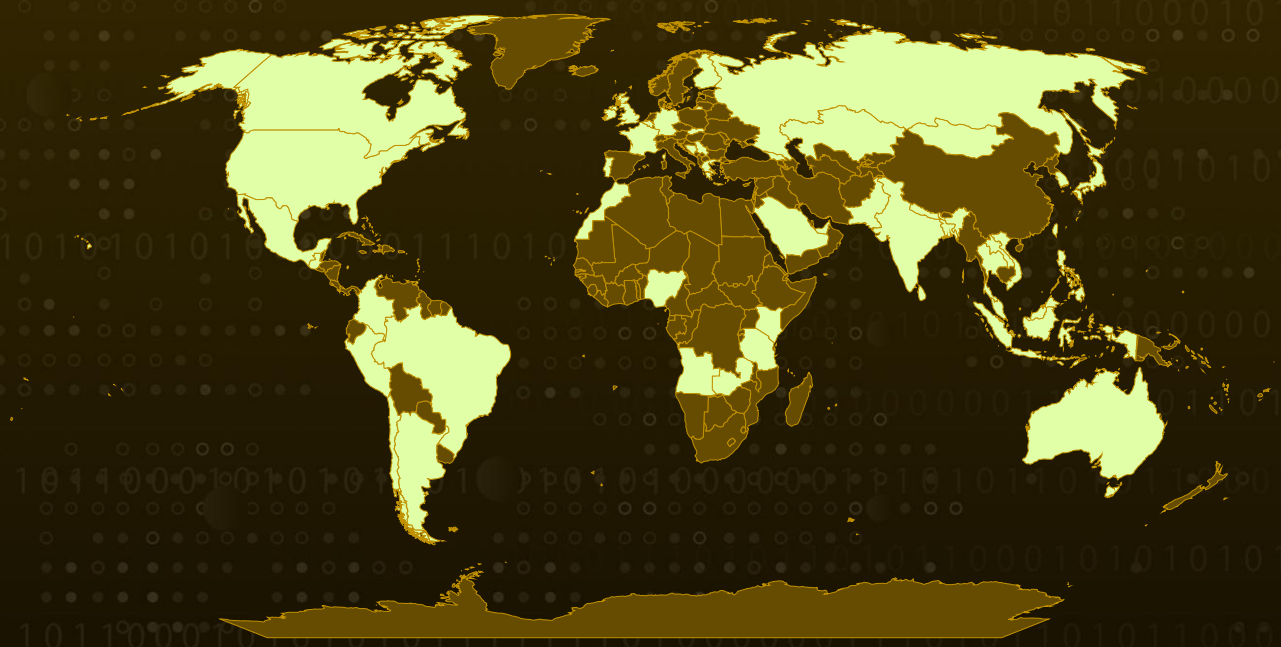
# Hidden in Plain Sight: The Abuse of Nezha and the Ghost RAT That Followed

| Date of Publication | Admiralty Code | TA Number |
| --- | --- | --- |
| October 10, 2025 | A1 | TA2025312 |

# Summary

**Attack Discovered:** August 2025
**Targeted Countries:** Taiwan, Japan, South Korea, Hong Kong, Singapore, Malaysia, India, United Kingdom, United States of America, Colombia, Laos, Thailand, Australia, Indonesia, France, Canada, Argentina, Sri Lanka, Philippines, Ireland, Kenya, Macao, Mainland China, Russia, Saudi Arabia, Nepal, Mongolia, Finland, Tanzania, Zambia, Angola, Nigeria, Morocco, Portugal, Greece, Serbia, Bosnia and Herzegovina, Slovakia, Mexico, Peru, Brazil, Vietnam, Pakistan, Trinidad and Tobago, Chile, Guatemala, Kazakhstan, Germany, Georgia, Bangladesh, Belgium, United Arab Emirates
**Affected Platform:** Windows
**Malware:** Ghost RAT
**Attack:** A stealthy cyberattack that began with a simple phpMyAdmin misconfiguration quickly escalated into a full-scale operation. The attacker cleverly used log poisoning to plant a hidden web shell, then repurposed the legitimate Nezha monitoring tool to control systems and deploy Ghost RAT malware secretly. By turning everyday admin tools into weapons, the attacker managed to infiltrate over a hundred machines across Taiwan, Japan, South Korea, and Hong Kong. The campaign highlights how easily overlooked configurations and trusted open-source utilities can be exploited to create powerful intrusion tools.

## Attack Regions



# Attack Details

**#1** In August 2025, a well-coordinated web intrusion began with the planting of a simple web shell on a compromised web server. The attacker used a tool called AntSword to gain remote control and later deployed Nezha, a legitimate server monitoring program that was repurposed for malicious use, to install Ghost RAT, a remote access trojan. The campaign affected more than a hundred systems, mostly in Taiwan, Japan, South Korea, and Hong Kong.

**#2** The attack started when a phpMyAdmin panel, used for managing databases, was accidentally left open to the internet after a DNS misconfiguration disabled authentication. Logs from the Apache server revealed that the attacker accessed the panel from an AWS IP address in Hong Kong and quickly changed the interface language to Simplified Chinese. Within seconds, they executed several SQL commands, proving they had strong technical skills. By taking advantage of a misconfigured logging feature and a directory traversal flaw, the attacker managed to inject a PHP web shell directly into the MariaDB logs. This clever technique, known as log poisoning, allowed them to execute PHP code remotely and establish a hidden backdoor on the system.

**#3** Once the web shell was active, the attacker tested it to confirm access, then switched IP addresses, likely to cover their tracks or pass control to another operator. Further investigation revealed that the server had exposed Windows management services to the internet, which allowed its information to appear on reconnaissance tools like Shodan. The attacker's infrastructure was linked to MoeDove LLC, a small hosting provider connected to suspicious domains and past malicious activity. Though seemingly small, this provider's recurring presence across multiple malicious domains hinted at a well-organized operation rather than random hacking attempts.

**#4** Telemetry from the infected systems showed that the attacker downloaded and installed the Nezha agent using an executable named live.exe hosted on Cloudflare. While Nezha is typically used for legitimate remote monitoring, it was configured here to connect to a command server hosted in Dublin under HostPapa. The Nezha dashboard used by the attacker was set to Russian and lacked authentication, exposing system data without restriction.

**#5** The final stage involved deploying Ghost RAT, which gave the attacker full remote control over the infected systems. The malware used multiple stages, a loader, a dropper, and the main payload, each designed to hide its activity and resist analysis. It maintained persistence by disguising itself as a Windows service named "SQLlite" and operated under system folders. Ghost RAT communicated with domains tied to MoeDove LLC, and its infrastructure was traced back to Chinese operators with a track record of registering fake or malicious domains. The attack's complexity and precision point to a skilled and well-funded actor.

# Recommendations

- **Secure All Admin Panels and Management Interfaces:** Always protect tools like phpMyAdmin or remote management consoles with strong passwords and multi-factor authentication. Never leave them exposed to the internet without proper access controls.
- **Keep Your Software Updated:** Regularly patch web servers, database tools, and any third-party software to close known vulnerabilities that attackers can exploit.
- **Separate Service Accounts:** Avoid running web and database services under the same user account. Using separate accounts with minimal privileges reduces the damage attackers can cause if one service is breached.
- **Limit Access to Monitoring Tools:** If you use legitimate remote monitoring or management software like Nezha, make sure it's configured securely with proper authentication and encryption.
- **Enhance Endpoint Protection:** Deploy next-generation antivirus (NGAV) and endpoint detection & response (EDR) solutions to identify and block malware. Leverage behavioral analysis and machine learning-based detection to spot suspicious activity.

## Potential MITRE ATT&CK TTPs

| | | | |
|---|---|---|---|
| **TA0001** Initial Access | **TA0002** Execution | **TA0003** Persistence | **TA0004** Privilege Escalation |
| **TA0005** Defense Evasion | **TA0007** Discovery | **TA0011** Command and Control | **T1190** Exploit Public-Facing Application |
| **T1505** Server Software Component | **T1505.003** Web Shell | **T1059** Command and Scripting Interpreter | **T1071** Application Layer Protocol |
| **T1071.001** Web Protocols | **T1543** Create or Modify System Process | **T1036** Masquerading | **T1036.004** Masquerade Task or Service |

| | | | |
|---|---|---|---|
| **T1078** Valid Accounts | **T1046** Network Service Discovery | **T1105** Ingress Tool Transfer | **T1082** System Information Discovery |
| **T1574** Hijack Execution Flow | **T1574.001** DLL | **T1027** Obfuscated Files or Information | **T1033** System Owner/User Discovery |
| **T1547** Boot or Logon Autostart Execution | **T1547.001** Registry Run Keys / Startup Folder | | |

## Indicators of Compromise (IOCs)

| TYPE | VALUE |
|---|---|
| SHA256 | f3570bb6e0f9c695d48f89f043380b43831dd0f6fe79b16eda2a3ffd9fd7ad16, 9f33095a24471bed55ce11803e4ebbed5118bfb5d3861baf1c8214efcd9e7de6, 7b2599ed54b72daec0acfd32744c7a9a77b19e6cf4e1651837175e4606dbc958, 82611e60a2c5de23a1b976bb3b9a32c4427cb60a002e4c27cadfa84031d87999, 35e0b22139fb27d2c9721aedf5770d893423bf029e1f56be92485ff8fce210f3 |
| File Path | C:\xamp\htdocs\123.php, C:\Windows\Cursors\x.exe, C:\Windows\system32\SQLlite.exe, C:\Windows\system32\32138546.dll, C:\Windows\Cursors\live.exe |
| URL | hxxps[:]//rism[.]pages[.]dev/microsoft[.]exe |
| IPv4 | 54[.]46[.]50[.]255, 45[.]207[.]220[.]12, 172[.]245[.]52[.]169 |
| Domains | c[.]mid[.]al, gd[.]bj2[.]xyz |
| Mutex | gd[.]bj2[.]xyz[:]53762[:]SQLlite |

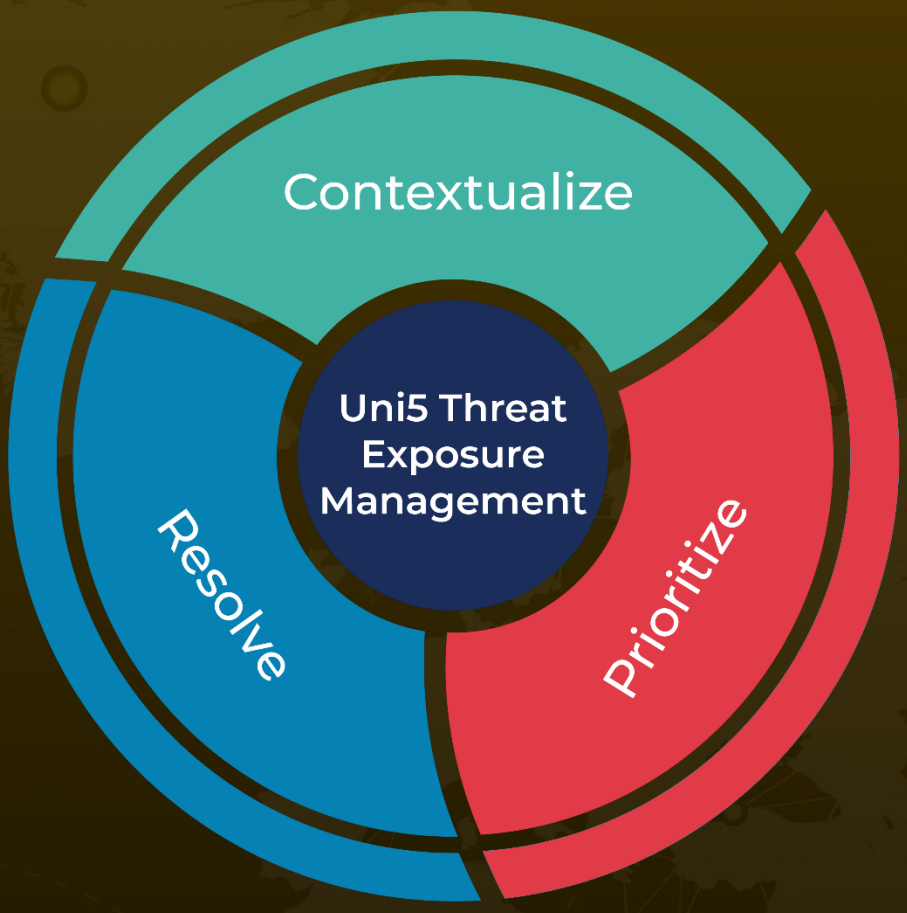
# References

https://www.huntress.com/blog/nezha-china-nexus-threat-actor-tool

# What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.




REPORT GENERATED ON

**October 10, 2025 • 9:00 AM**



More at www.hivepro.com