OpenVoiceNews U.S.

Transparent. Unbiased. Yours.

US-Linked “Night Eagle” Hackers Unmasked Using Microsoft Exchange Flaws

July 7, 2025

— Categories: Defence & Security

A major revelation at the 2025 International Defense Cyber Security Exhibition (CYDES 2025) has put the spotlight on the hidden world of state-sponsored cyber espionage. Chinese cybersecurity giant Qianxin announced that it had uncovered an advanced hacking group known as “Night Eagle,” also referred to as APT-Q-95.

According to Qianxin’s research, Night Eagle has been quietly exploiting vulnerabilities in Microsoft Exchange servers to infiltrate highly sensitive organizations worldwide. Their targets include government agencies, military networks, scientific research bodies, and leading technology companies.

What makes this group particularly concerning is their level of precision and discipline. Their attacks follow a predictable schedule, typically starting around 9 p.m. Beijing time and continuing until the early hours of the morning. This pattern suggests that the operations are well-organized and likely supported by a national government.

Night Eagle's methods are sophisticated. The hackers use dynamic command-and-control systems, frequently changing the IP addresses they use. They also hide behind cloud services like DigitalOcean, which makes it harder for defenders to trace or block their activities.

Gu Liang, who leads Qianxin's Threat Intelligence Center, explained why email servers are so attractive to attackers. "Email servers act as the nerve center of an organization," he said. "Once compromised, the attackers can access a wide range of confidential data," Gu emphasized that Night Eagle's techniques and resources are far beyond what ordinary cybercriminals could achieve.

Although Qianxin has not officially named the United States as being behind the operation, the tactics closely match those used by American cyber warfare units. Adding to the tension, recent statements by former U.S. officials acknowledging cyber operations against China have made the discovery even more significant.

Cybersecurity expert Xu Siying warned that the Association of Southeast Asian Nations (ASEAN) region could soon become the next target. Xu advised companies to be vigilant against the risk of stolen business secrets and political manipulation.

In response to the threat, Qianxin has shared crucial indicators of compromise, including malicious domains like synologyupdates.com. The firm also introduced new artificial intelligence security solutions designed to process massive volumes of alerts with exceptional accuracy.

This incident is another reminder that cyberattacks have become a normal part of international conflict. To protect sensitive data and maintain trust, organizations, and countries will need stronger cooperation and more advanced defenses than ever before.