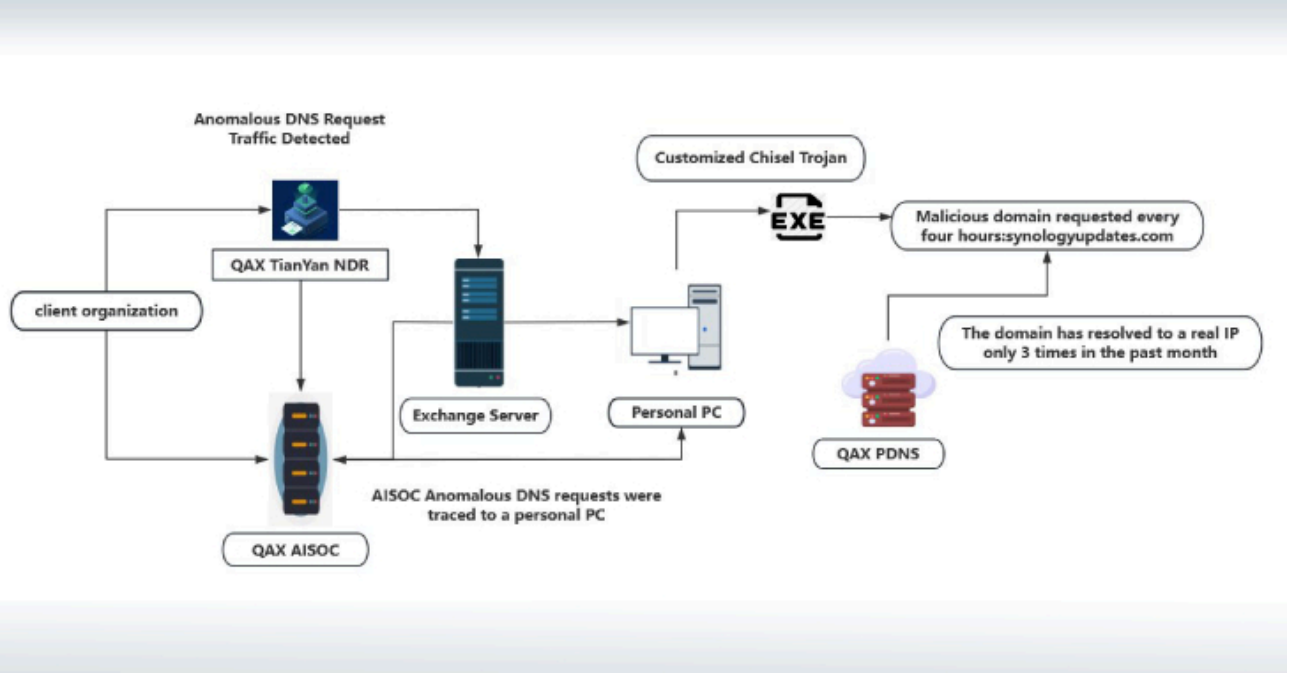
NightEagle APT Exploits Microsoft Exchange Flaw to Target China's Military and Tech Sectors

By The Hacker News

Published: 2025-07-04 · Archived: 2026-04-05 17:51:21 UTC



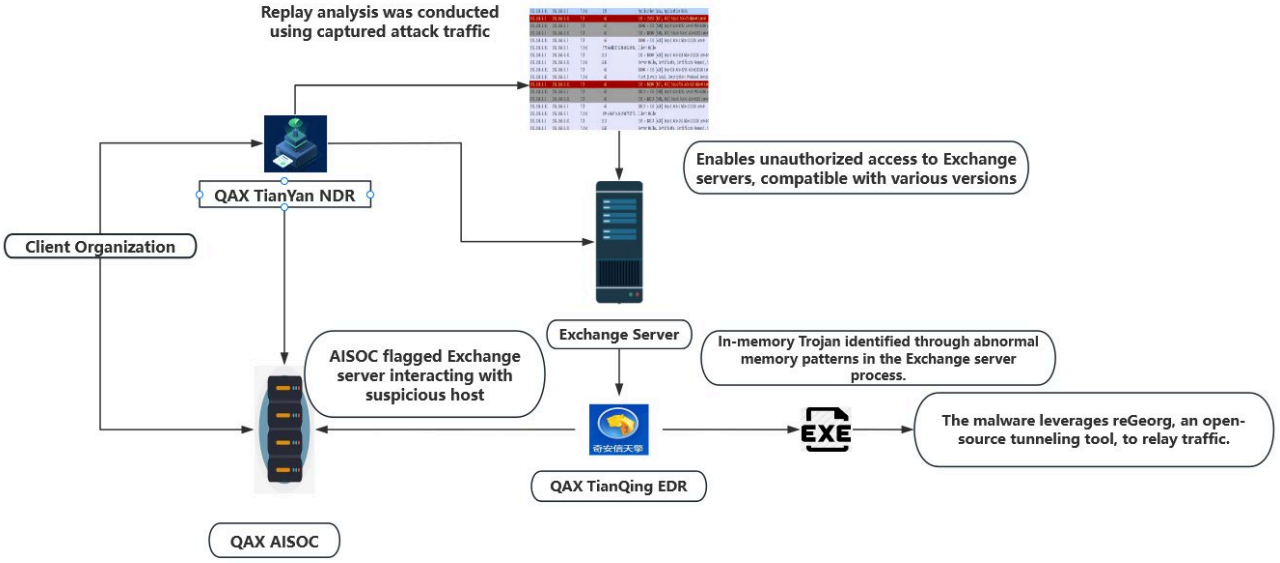
Cybersecurity researchers have shed light on a previously undocumented threat actor called **NightEagle** (aka APT-Q-95) that has been observed targeting Microsoft Exchange servers as a part of a zero-day exploit chain designed to target government, defense, and technology sectors in China.

According to QiAnXin's RedDrip Team, the threat actor has been active since 2023 and has switched network infrastructure at an extremely fast rate. The findings were presented at CYDES 2025, the third edition of Malaysia's National Cyber Defence & Security Exhibition and Conference held between July 1 and 3, 2025.

"It seems to have the speed of an eagle and has been operating at night in China," the cybersecurity vendor said, explaining the rationale behind naming the adversary NightEagle.

Attacks mounted by the threat actor have singled out entities operating in the high-tech, chip semiconductors, quantum technology, artificial intelligence, and military verticals with the main goal of gathering intelligence, QiAnXin added.

The company also noted that it began an investigation after it discovered on one of its customer's endpoints a bespoke version of the Go-based Chisel utility, which was configured to automatically start every four hours as part of a scheduled task.



"The attacker modified the source code of the open-source Chisel intranet penetration tool, hard-coded the execution parameters, used the specified username and password, established a socks connection with the 443 end of the specified C&C address, and mapped it to the specified port of the C&C host to achieve the intranet penetration function," it said in a report.

It's said that the trojan is delivered by means of a .NET loader, which, in turn, is implanted into the Internet Information Server (IIS) service of the Microsoft Exchange Server. Further analysis has determined the presence of a zero-day that enabled the attackers to obtain the machineKey and gain unauthorized access to the Exchange Server.

"The attacker used the key to deserialize the Exchange server, thereby implanting a trojan into any server that complies with the Exchange version, and remotely reading the mailbox data of any person," the report said.

QiAnXin claimed that the activity was likely the work of a threat actor from North America given that the attacks took place between 9 p.m. and 6 a.m. Beijing time. It also said the threat actor exhibits all the traits of an advanced persistent threat (APT) group, describing it as "fast, accurate, and ruthless."

When reached for comment, Microsoft told The Hacker News it's continuing its investigation but noted that it has not found any vulnerabilities at this stage.

"We have reviewed this report and have not identified any new actionable vulnerabilities to date," a Microsoft spokesperson said. "Our investigation is ongoing, and we will take action as appropriate based on our findings. We remain committed to addressing reported issues promptly, while maintaining the highest standards of safety and trust, to help keep our customers protected."

(The story was updated after publication on July 10, 2025, to include a response from Microsoft.)

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