Chinese Naikon Group Back with New Espionage Attack

cyware.com/news/chinese-naikon-group-back-with-new-espionage-attack-66a8413d

Chinese state-sponsored cyberespionage gang Naikon, aka Override Panda and Lotus Panda, has reappeared with a new phishing attack that aims to exfiltrate confidential information. The APT group was first tracked in 2010 and its infrastructure was first detected in 2015.

Diving into details

Cluster25 analyzed Lotus Panda and found that it used a spear-phishing email to deliver a Red team framework beacon, dubbed Viper. While the targets remain unknown, researchers surmise that it could be a government entity from a South Asian nation.

Kill chain

- The spear-phishing email consists of a weaponized document pretending to be a call for tender.
- Two payloads are hidden in the document as document properties.
- Viper is described as a “graphical intranet penetration tool that modulates and enhances the tactics and techniques commonly used during intranet penetration.”
- It features more than 80 modules to expedite initial access, privilege escalation, credential access, persistence, arbitrary command execution, and lateral movement.
- The C2 server contains both Viper framework and ARL dashboards.

Noteworthy attacks by Chinese hackers

- Cyberespionage group Moshen Dragon is targeting telcos in Central Asia. It is attempting to sideload malicious DLLs into antivirus solutions to move laterally, steal credentials, and exfiltrate sensitive information.
- APT10 or Cicada was found responsible for a long-term espionage campaign against Japanese entities. The activities continued from mid-2021 to February 2022.
- In March, the Mustang Panda APT was found using a new strain of PlugX RAT. Dubbed Hodur, the trojan is capable of multiple actions, such as collecting system details, executing commands, and reading and writing arbitrary files.

The bottom line

Override Panda’s TTPs indicate that it is conducting long-term espionage and intelligence operations. The group is infamous for targeting foreign officials and governments. The sectors targeted by Naikon are indicative of its intentions to infect ASEAN countries. The group has, furthermore, changed and evolved its TTPs over the years to minimize detection and maximize profits.

Naikon APT | Chinese APT Group | spearphishing email

Publisher

Cyware