Chinese Cyberspies Target Military Organizations in Asia With New Malware

securityweek.com/chinese-cyberspies-target-military-organizations-asia-new-malware

By Ionut Arghire on April 29, 2021

A cyber-espionage group believed to be sponsored by the Chinese government has been observed targeting military organizations in Southeast Asia in attacks involving previously undocumented malware, Bitdefender reported on Wednesday.

Linked to the Chinese People's Liberation Army (PLA) over half a decade ago, the Naikon advanced persistent threat (APT) was revealed last year to have conducted a five-year stealth campaign against targets in Australia, Indonesia, the Philippines, Vietnam, Thailand, Myanmar, and Brunei. The group has been known to focus on government and military organizations.

Although reports on Naikon's activity were so far published only in 2015 and 2020, the persistent APT has been quietly operational for at least a decade, making changes to its infrastructure and toolset to ensure it can stay under the radar.

Last year, after its activity was exposed, Naikon made a similar move: it switched to a new backdoor, although it continued to use previously known malware for the first stages of attack. The group has also been abusing legitimate software for nefarious purposes.

The latest campaign ran between June 2019 and March 2021, and one of the new backdoors, dubbed RainyDay, was first used in attacks in September 2020, Bitdefender says. To remain undetected, the APT would mimic legitimate software running on the infected machines. The purpose of the attacks remains espionage and data exfiltration, and the group continues to focus on Southeast Asian targets.

The RainyDay backdoor allows the attackers to perform reconnaissance on the infected machines, deploy reverse proxies, install scanners, execute tools for password dumping, move laterally on the victim's network, and achieve persistence.

Naikon has always used DLL side-loading for the RainyDay execution, "and there was always a vulnerable executable along with a DLL file and the rdmin.src file containing the encrypted backdoor payload," Bitdefender explains.

The same execution technique along with the use of rdmin.src are employed by China-linked Cycldek (Goblin Panda, Conimes) for the deployment of the FoundCore RAT. Furthermore, the shellcode used for payload extraction and other payload characteristics suggest a close connection between the two malware families and a possible overlap in activity between the two groups.

The similarities are not surprising, considering that Chinese threat actors are known to be sharing infrastructure and tools, and because Naikon was previously observed using exploits attributed to other threat groups, in an attempt to evade detection.

As part of the latest attacks, the adversary also deployed a second new backdoor called Nebulae, likely as a precautionary measure.

Attempting to impersonate a legitimate application, the Nebulae backdoor can harvest drive information, list and modify files and directories, execute and terminate processes, and download and run files from the command and control (C&C) server.

“The data we obtained so far tell almost nothing about the role of the Nebulae in this operation, but the presence of a persistence mechanism could mean that it is used as a backup access point to victims in the case of a negative scenario for actors,” Bitdefender notes.

Furthermore, admin domain credentials were used for lateral movement, likely after being stolen at an early stage of the attack. Persistence was typically achieved manually, while data of interest was exfiltrated to Dropbox.

“Our research confidently points to an operation conducted by the Naikon group based on the extraction of the C&C addresses from Nebulae samples. The particular domain dns.seekvibega.com obtained from such a sample points out to the Naikon infrastructure,” Bitdefender concludes.

Related: FireEye CEO: Reckless Microsoft Hack Unusual for China

Related: Cyber Attack Tied to China Boosts Development Bank's Chief

Tweet

Ionut Arghire is an international correspondent for SecurityWeek.
Previous Columns by Ionut Arghire:
IBM Dives Into TrickBot Gang's Malware Crypting Operation
Nikkei Says Customer Data Likely Impacted in Ransomware Attack

New Brute Force Attacks Against SQL Servers Use PowerShell Wrapper
DoJ Will No Longer Use CFAA to Charge Ethical Hackers
US Recovers $15 Million From Ad Fraud Group
Virtual Event Series - Security Summit Online Events by SecurityWeek

2022 ICS Cyber Security Conference | USA [Hybrid: Oct. 24-27]

2022 Singapore/APAC ICS Cyber Security Conference]

2022 CISO Forum: September 13-14 - A Virtual Event

sponsored links

Tags:

- NEWS & INDUSTRY
- Virus & Threats