Cyberspies target military organizations with new Nebulae backdoor

bleepingcomputer.com/news/security/cyberspies-target-military-organizations-with-new-nebulae-backdoor/

Sergiu Gatlan

By
Sergiu Gatlan

- April 28, 2021
- 09:00 AM
- 0

A Chinese-speaking threat actor has deployed a new backdoor in multiple cyber-espionage operations spanning roughly two years and targeting military organizations from Southeast Asia.

For at least a decade, the hacking group known as Naikon has actively spied on organizations in countries around the South China Sea, including the Philippines, Malaysia, Indonesia, Singapore, and Thailand, for at least a decade, since 2010.

Naikon is likely a state-sponsored threat actor tied to China, mostly known for focusing its efforts on high-profile orgs, including government entities and military orgs.

Backdoor used for persistence backup after detection

During their attacks, Naikon abused legitimate software to side-load the second-stage malware dubbed **Nebulae** likely used to achieve persistence, according to research published today by security researchers at Bitdefender's Cyber Threat Intelligence Lab.

Nebulae provides additional capabilities allowing attackers to collect system information, manipulate files and folders, download files from the command-and-control server, and execute, list, or terminate processes on compromised devices.

The malware is also designed to gain persistence by adding a new registry key to relaunch automatically on system restarts after login.

"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 backup access point to victim in the case of a negative scenario for actors," Bitdefender researcher Victor Vrabie said.

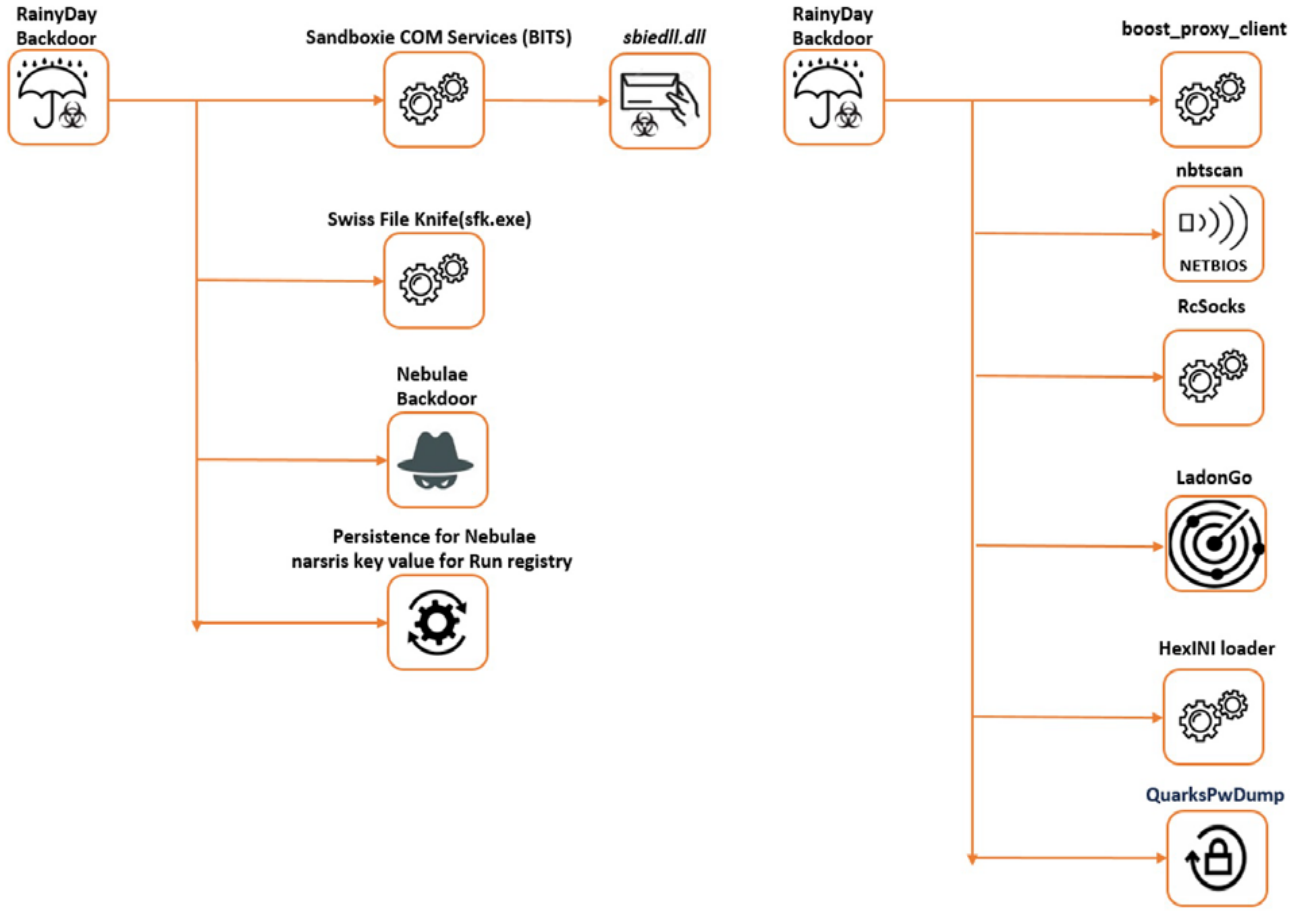
Nebulae side-loading (*Bitdefender*)

First-stage backdoor used as a swiss-army knife

In the same series of attacks, the Naikon threat actors also delivered first-stage malware known as RainyDay or FoundCore used to deploy second-stage payloads and tools used for various purposes, including the Nebulae backdoor.

"Using the RainyDay backdoor, the actors performed reconnaissance, uploaded its reverse proxy tools and scanners, executed the password dump tools, performed lateral movement, achieved persistence, all to compromise the victims' network and to get to the information of interest," Vrabie added [PDF].

Besides deploying additional payloads on compromised systems, attackers can also send RainyDay commands over TCP or HTTP to manipulate services, access a command shell, uninstall the malware, taking and collecting screen captures, and manipulate, download, or upload files.



RainyDay backdoor (*Bitdefender*)
During attacks observed between June 2019 and March 2021, Naikon dropped malicious payloads using side-loading and DLL hijacking vulnerabilities impacting:

- Sandboxie COM Services (BITS) (SANDBOXIE L.T.D)
- Outlook Item Finder (Microsoft Corporation)
- VirusScan On-Demand Scan Task Properties (McAfee, Inc.)
- Mobile Popup Application (Quick Heal Technologies (P) Ltd.)
- ARO 2012 Tutorial

Bitdefender confidently attributed this operation to the Naikon threat actor based on command-and-control servers and malicious payloads belonging to the Aria-Body loader malware family used in the group's past operations.

Related Articles:

Cyberspies use IP cameras to deploy backdoors, steal Exchange emails

New ChromeLoader malware surge threatens browsers worldwide

New ERMAC 2.0 Android malware steals accounts, wallets from 467 apps

BPFDoor malware uses Solaris vulnerability to get root privileges

BPFDoor: Stealthy Linux malware bypasses firewalls for remote access