

Chinese Cyberspies Delivered Malware via Legitimate Software Updates

A Chinese APT actor tracked as Evasive Panda has been observed targeting in-country members of an international non-governmental organization (NGO) with the MgBot backdoor, and the malware was likely delivered through the legitimate update channels of popular Chinese software, cybersecurity firm ESET reports.

Active since at least 2012 and also referred to as Bronze Highland and Daggerfly, Evasive Panda is a cyberespionage group historically targeting individuals and government entities in mainland China, India, Hong Kong, Macao, Malaysia, Myanmar, the Philippines, Nigeria, Taiwan, and Vietnam.

For roughly a decade, the APT has been relying on a custom, modular malware framework that includes the MgBot backdoor to spy on victims.

While investigating a MgBot backdoor attack observed in January 2022, ESET discovered a broader malicious campaign that started in 2020 and continued throughout 2021, and which targeted individuals in China's Gansu, Guangdong, and Jiangsu provinces.

Most of the victims, ESET discovered, are members of an international NGO that operates in two of the targeted provinces. One victim in Nigeria was also identified.

As part of the attacks, the MgBot backdoor was likely delivered to victims through legitimate update channels,

either a supply chain attack (via the compromised update servers of Tencent's legitimate application QQ), or via adversary-in-the-middle (AitM) attacks, where threat actors compromise internet infrastructure.

"With access to ISP backbone infrastructure – through legal or illegal means – Evasive Panda would be able to intercept and reply to the update requests performed via HTTP, or even modify packets on the fly," ESET explained.

According to ESET, there's not enough evidence to support or discard either of the hypotheses in favor of the other, given that both methods have been used in previous Chinese APT attacks.

Developed in C++ and relying on plugins to expand its functionality, the MgBot backdoor used in these attacks allows attackers to harvest large amounts of information from the victims' Windows machines.

The malware can log keystrokes, steal files from hard disks, USB drives, and CDs, can steal clipboard content, capture audio, steal credentials from multiple applications (Outlook, Foxmail, Chrome, Firefox, FileZilla, Opera, QQBrowser, WinSCP, and more), and steal browser cookies.

Most of the backdoor's plugins are designed to target popular Chinese applications developed by Tencent, including QQ, QQBrowser, Foxmail, and WeChat.

Related: Chinese Cyberspies Use 'Melofee' Linux Malware for Stealthy Attacks

Related: Report: Suspected Chinese Hack Targets Indian Media, Gov't

Related: Chinese Threat Actor Uses New MgBot Variant in Attacks on India, Hong Kong

Chinese Cyberspies Delivered Malware via Legitimate Software

Updates