China-aligned Evasive Panda leverages religious festival to target and spy on Tibetans, ESET Research discovers

DUBAI, UNITED ARAB EMIRATES, March 13, 2024 /EINPresswire.com/ -- ESET researchers have discovered a cyberespionage campaign that, since at least September 2023, has been victimizing Tibetans via a targeted watering hole (also known as a strategic web compromise), and a supply-chain compromise to deliver trojanized installers of Tibetan language translation software. The attackers aimed to deploy malicious downloaders for both Windows and macOS to compromise website visitors with MgBot as well as a backdoor that has not been publicly documented yet; ESET has named it Nightdoor. The campaign by the China-aligned Evasive Panda APT group leveraged the Monlam Festival — a religious gathering — to target Tibetans in several countries and territories. Targeted networks were located in India, Taiwan, Hong Kong, Australia, and the United States.

ESET discovered the cyberespionage operation in January 2024. The compromised website abused as a watering hole (the attacker infests a website that the victim likely or regularly uses) belongs to Kagyu International Monlam Trust, an organization based in India that promotes Tibetan Buddhism internationally. The attack might have been intended to capitalize on international interest in the Kagyu Monlam Festival that is held annually in January in the city of Bodhgaya, India. The network of the Georgia Institute of Technology (also known as Georgia Tech) in the United States is among the identified entities in the targeted IP address ranges. In the past, the university was mentioned in connection with the Chinese Communist Party's influence on education institutes in the U.S.

Around September 2023, the attackers compromised the website of a software development company based in India that produces Tibetan language translation software. The attackers placed several trojanized applications there that deploy a malicious downloader for Windows or macOS.

In addition to this, the attackers also abused the same website and a Tibetan news website called Tibetpost to host the payloads obtained by the malicious downloads, including two full-featured backdoors for Windows and an unknown number of payloads for macOS.

“The attackers fielded several downloaders, droppers, and backdoors, including MgBot — which is used exclusively by Evasive Panda — and Nightdoor, the latest major addition to the group’s toolkit and that has been used to target several networks in East Asia,” says ESET researcher Anh Ho, who discovered the attack. “The Nightdoor backdoor, used in the supply-chain attack, is a recent addition to Evasive Panda’s toolset. The earliest version of Nightdoor that we've been able to find is from 2020, when Evasive Panda deployed it onto the machine of a high-profile target in Vietnam. We have requested that the Google account associated with its authorization token be taken down,” adds Ho.

With high confidence, ESET attributes this campaign to the Evasive Panda APT group, based on the malware that was used: MgBot and Nightdoor. Over the past two years, we have seen both backdoors deployed together in an unrelated attack against a religious organization in Taiwan, in which they also shared the same Command & Control server.

Evasive Panda (also known as BRONZE HIGHLAND or Daggerfly) is a Chinese-speaking and China-aligned APT group, active since at least 2012. ESET Research has observed the group conducting cyberespionage against individuals in mainland China, Hong Kong, Macao, and Nigeria. Government entities were targeted in Southeast and East Asia, specifically China, Macao, Myanmar, The Philippines, Taiwan, and Vietnam. Other organizations in China and Hong Kong were also targeted. According to public reports, the group has also targeted unknown entities in Hong Kong, India, and Malaysia.

The group uses its own custom malware framework with a modular architecture that allows its backdoor, known as MgBot, to receive modules to spy on its victims and enhance its capabilities. Since 2020 ESET has also observed that Evasive Panda has capabilities to deliver its backdoors via adversary-in-the-middle attacks hijacking updates of legitimate software.

For more technical information about the latest malicious campaign of the Evasive Panda group, check out the blogpost “Evasive Panda leverages Monlam Festival to target Tibetans” on WeLiveSecurity.com. Make sure to follow ESET Research on Twitter (today known as X) for the latest news from ESET Research.

About ESET
For more than 30 years, ESET® has been developing industry-leading IT security software and services to protect businesses, critical infrastructure and consumers worldwide from increasingly sophisticated digital threats. From endpoint and mobile security to endpoint detection and response, as well as encryption and multifactor authentication, ESET’s high-performing, easy-to-use solutions unobtrusively protect and monitor 24/7, updating defenses in real time to keep

users safe and businesses running without interruption. Evolving threats require an evolving IT security company that enables the safe use of technology. This is backed by ESET's R&D centers worldwide, working in support of our shared future. For more information, visit www.eset.com or follow us on LinkedIn, Facebook, and X (Twitter).

Sanjeev Kant
Vistar Communications
+971 55 972 4623
email us here
