Xiaoqiying/Genesis Day Threat Actor Group Targets South Korea, Taiwan

Research (Insikt)

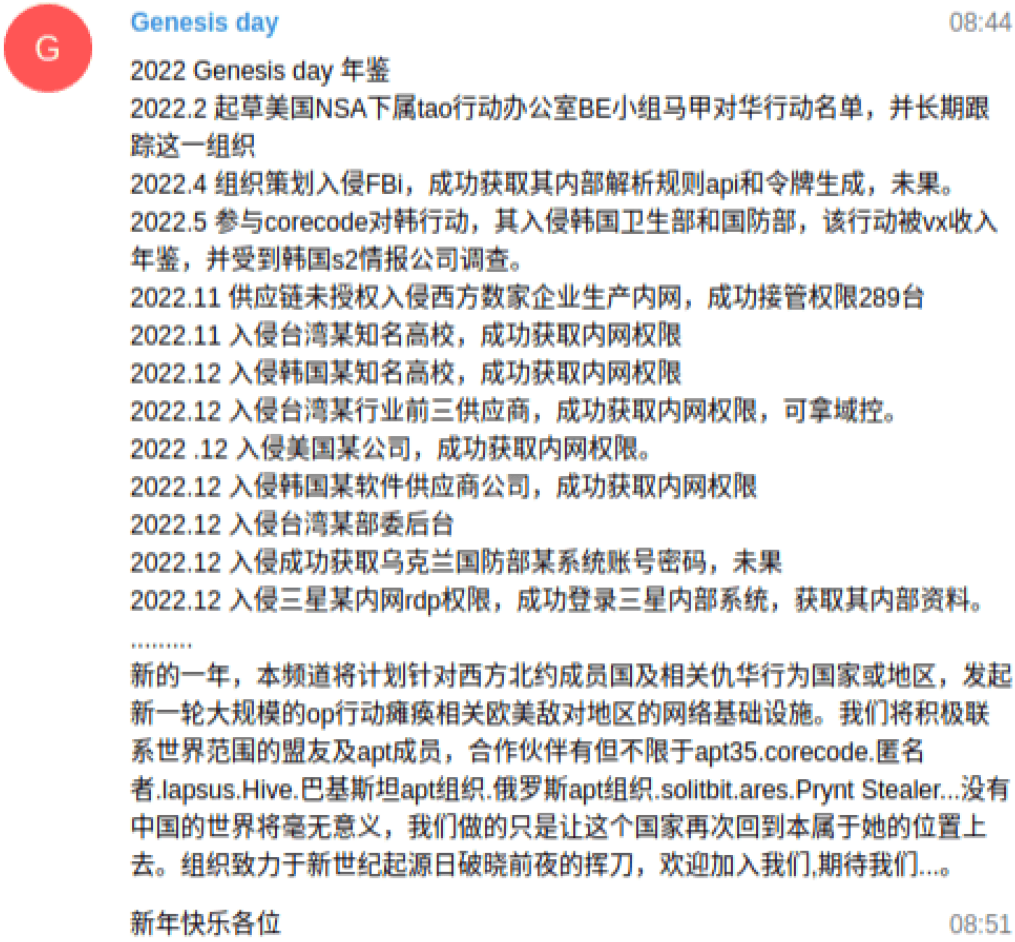
Posted: 20th April 2023

By: Insikt Group®

Xiaoqiying (aka Genesis Day, Teng Snake) is a primarily Chinese-speaking threat group that is most well known for conducting website defacement and data exfiltration attacks on more than a dozen South Korean research and academic institutions in late-January 2023. New research from Recorded Future's Insikt Group has found that more recently, the group's affiliated threat actors have signaled a new round of cyberattacks against organizations in Japan and Taiwan. Although it shows no clear ties to the Chinese government, Xiaoqiying is staunchly pro-China and vows to target NATO countries as well as any country or region that is deemed hostile to China.

Since January 25, 2023, open-source reporting from South Korea has revealed a mass cyberattack against websites belonging to 12 South Korean research and academic institutions during the Lunar New Year holiday conducted by Xiaoqiying. According to Korea Internet & Security Agency (KISA) reports, all 12 of the websites suffered website defacements in which the adversaries replaced each hosted website with their own in a compromised server. KISA also identified IP addresses linked with the attack to origins within various countries such as China, the US, Singapore, and Taiwan. Based on a report from The Korea Times (koreatimes.co.kr), the Chinese threat group disclosed on its public Telegram channel that it included KISA as one of its potential targets and it is the first government agency targeted by the threat group. Other reports claimed that the threat group threatened to target approximately 2,000 government agencies, including South Korea's Ministry of Culture, Sports, and Tourism.

Our analysis of Xiaoqiying's activity on Telegram is based on 2 Telegram invitation links obtained in early January 2023. The Genesis Day threat group was active on Telegram up until February 2023 when the news of its alleged breaches reached the media. Then, both Telegram channels went offline. These 2 Telegram channels included an announcement channel and a member channel and consisted primarily of Chinese-speaking users. From analyzing the downloaded data, we identified the threat group's administrators, tools and data shared among members, tactics, techniques, and procedures (TTPs) used by the threat group, and connections with other special-access cybercriminal forums and threat actors. We also assessed the credibility of the offers and predicted the future course of action of the group.



The new year message posted by "Genesis Day" on December 31, 2022, served as a summary for the group's activities in 2022 and a call to action for 2023. The English translation is provided below. (Source: Telegram)

"In the upcoming year, this channel will plan to launch another round of operations against NATO members and related countries/regions that are hostile to China, to paralyze the network and infrastructure of these countries.

We are actively cooperating with our global allies and APT members, our partners include but are not limited to APT 35, Corecode [sic], Anonymous, Lapsus, Hive, Pakistani APTs, Russian APTs, Solitbit.ares [sic], Prynt Stealer, …. A world without China would be a meaningless world, we are only trying to restore this country to her rightful place. We strive to wield our swords at the dawn of this new era. You are welcomed to join us, expect us …

Happy New Year everyone"

The group claimed to be responsible for some unverified cyberattacks before the confirmed intrusions against numerous South Korean organizations in January and February 2023. As a result, we rate its credibility as moderate. It shared available penetration testing tools, malware, proofs of concept and exploits, and leaked data, and it claimed to have working relationships with some well-known cybercriminal and APT groups around the world. The group appears to be ambitious and is actively recruiting individuals with hacking skills.

The most recent postings by its affiliated threat actors on special-access forums shows it has possibly compromised new targets in Japan and Taiwan and signaled a new round of cyberattacks against these countries. We recommend that organizations that are possibly targeted by this group, especially education, research, and government organizations in the Asian Pacific region, maintain a frequent patching cadence for their internet-facing devices and disable any unnecessary remote access tools.

To read the entire analysis with endnotes, click here to download the report as a PDF.