Cyber enabled espionage in the aviation sector

Reference: Memo [190425-1] Date: 25/04/2019 - Version: 1.0
Keywords: espionage, steganography, China, aviation, transportation
Sources: publicly available information

Key Points

- A General Electric's employee reportedly stole aerospace turbine technology secrets for the benefit of China.
- The spy used several methods such as encryption, exfiltration via USB storage devices, steganography and sending stolen files to his personal email address.
- China has been suspected to conduct cyber-espionage operations in the aviation sector for several years.
- According to researchers, since 2004, a total of 20 active Chinese threat actor groups have been detected targeting aviation as a whole.

Summary

Open sources recently reported that a US citizen of Chinese descent, named Xiaoqing Zheng, has been accused of espionage against General Electric (GE). Xiaoqing Zheng allegedly stole GE's turbine technology secrets and delivered them to the People's Republic of China.

Zheng was hired by GE in 2008 and has been working there until 2018. The secrets he stole involve mathematical computations relating to sealing and optimization of turbines, in the form of MatLab (a high-level computer language used for mathematical computing) and Excel (spreadsheet) files.

In 2014, GE learned that Zheng had copied 19 020 files from its work desktop computer onto a USB external storage device, believed to be a thumb drive. In 2016 or 2017, GE instituted a policy restricting employees' use of external USB drives such as thumb drives.

Zheng reportedly switched to alternatives methods, encrypting files in folders on his work desktop computer (using a program called Axcrypt, which was not in use by its employer). Then, GE installed monitoring software on Zheng's computers in an attempt to determine what information he was encrypting and what he was doing with it. Zheng moved encrypted files to a "temp folder", and used steganography to hide data files in the binary code of digital photo files. He plugged an iPhone into his work desktop computer to copy an image file he would use to hide stolen data into it. Zheng exfiltrated stolen secrets by e-mailing data files to his personal e-mail address (...@hotmail.com).

Comments

According to investigators, methods used by Zheng (moving files, renaming them, encrypting them, hiding them within the binary code of seemingly harmless files) are uncommon even among trained computer experts.

China has been suspected to conduct cyber-espionage operations in the aviation sector for several years.

In May 2011, a targeted intrusion into Lockheed Martin's IT networks was reported and attributed to Chinese hackers.

In 2012, a watering hole campaign affected the website of US-based turbine manufacturer, Capstone Turbine, and was attributed to a Chinese threat group.

A watering hole attack is a form of cyberattack targeting a particular organisation or sector, in which malware is installed on a website or websites regularly visited by the organisation's or sector's members in order to infect computers of visitors.

In 2014, according to CrowdStrike cyber security firm, another watering hole attack, attributed to a Chinese cyber-threat actor dubbed Aurora Panda, targeted the French aerospace industries association (GIFAS). Safran, a France-based aerospace and defence company with a focus on the design and production of aircraft engines and equipment, was likely one of the intended targets.

In October and December 2018, the US Department of Justice indicted several Chinese nationals (including members of a cyber-threat actor group, dubbed APT10), for theft of aviation trade secrets (see Memo [231218]).

In February 2019, open sources reported that, the Montreal-based International Civil Aviation Organization (ICAO) had been hit by a serious cyberattack that affected the whole aviation sector in November 2016. The author of the attack is allegedly an advanced cyber-espionage group dubbed Emissary Panda (also known as APT27) with ties to the Chinese government (see Memo [190327-1]).

According to researchers from FireEye, since 2004, a total of 27 active threat actor groups have been detected targeting aviation as a whole, and 20 of which are based in China. FireEye says this is "the highest number of China-based threat groups we have observed targeting any single industry."

In May 2017, the C919, China's indigenous long-haul airliner successfully, completed its maiden flight. The aviation industry was listed as one the key 10 areas of focus in the "Made in China 2025" (MIC2025) industrial plan, unveiled in 2015 with the aim of lifting the country's industries up the value chain, replacing imports with local products and building global champions capable of taking on Western giants in global markets.