CASE STUDY

Theft of Trade Secrets

XIAOQING ZHENG

- Age 59 at time of sentencing
- U.S. citizen of Chinese descent
- Principal Engineer at GE Power in Schenectady, New York
- Holds degrees from Northwestern Polytechnic University and Massachusetts Institute of Technology in "aero engine" fields
- Specialized in turbine sealing technology

CDSE

Center for Development of Security Excellence

WHAT HAPPENED

In 2014, GE corporate security learned that Zheng had copied 19,020 electronic files from one of his GE-issued computers onto a USB external storage device. GE was unable to determine the contents of the 19,020 files; however, they suspected that the files related to Zheng's work for GE. GE investigators interviewed Zheng in 2014 regarding this incident, and Zheng told them that he had since deleted the files.

In November - December 2017, GE discovered that Zheng had saved approximately 400 encrypted files on his work (desktop) computer. Zheng encrypted the files using a program called Axcrypt - a program not used by GE. Due to the encryption, GE was unable to view the contents of the files.

GE installed monitoring software on Zheng's computer(s) to determine what he was encrypting, and what he was doing with the information. The monitoring showed that on July 5, 2018, Zheng moved approximately 40 encrypted files to a "temp folder" on his GE-issued work computer. GE determined that the files were MatLab and Excel files containing calculations related to sealing and optimizing turbine technology - information that GE considers proprietary and secret.

GE's monitoring also showed that Zheng used "steganography" to conceal the data. Zheng placed the files into the binary code of an innocuous looking separate electronic file on the computer - a digital photograph of a sunset. Zheng then e-mailed the image to his personal e-mail address.

On August 1, 2018, FBI agents executed a federal search warrant at Zheng's residence in Niskayuna, New York. During the execution of the search warrant, agents interviewed Zheng. He stated that it was common knowledge that "MatLab" electronic files are GE's property and that it would be unlawful to take them without permission. Zheng also said he used the steganography process on July 5, 2018, to take multiple GE electronic files that contained data about turbine technology; he had previously used steganography between 5 and 10 times to take materials that belonged to GE.

Zheng was sentenced to 24 months in prison for conspiring to steal trade secrets with the intent to benefit the People's Republic of China (PRC), and he was fined $7,500.

INDICATORS

- **Foreign Considerations** – Zheng holds dual citizenship in the U.S. and the Peoples Republic of China. Zheng was also an acknowledged member of the Chinese "Thousand Talents" program.
- **Security and Compliance Issues** – Zheng had previously admitted to copying files to an unauthorized USB device. Zheng did not surrender the USB device , nor provide any corroboration that the files had been deleted.
- **Outside Activities** - Zheng owned two Chinese companies that were in competition with GE.

IMPACT

- "American ingenuity is an integral part of the United States economic security – it is what has guided the U.S. to become the global leader, even as China seeks to topple our status," said Assistant Director Alan E. Kohler Jr. of the FBI Counterintelligence Division. "Xiaoqing Zheng was a Thousand Talents Program member and willingly stole proprietary technology and sent it back to the PRC. Let today's sentencing serve as a reminder that the FBI remains dedicated in our pursuit of those who collaborate with the People's Republic of China (PRC) and steal American trade secrets."
- "This is a case of textbook economic espionage. Zheng exploited his position of trust, betrayed his employer and conspired with the government of China to steal innovative American technology," said Assistant Attorney General Matthew G. Olsen of the Justice Department's National Security Division. "The Justice Department will hold accountable those who threaten our national security by conniving to steal valuable trade secrets on behalf of a foreign power."

ADDITIONAL INFO

- Zheng owns a business called Nanjing Tainyi Aeronautical Technology, Ltd, located in Nanjing, China. Zheng disclosed this information to GE. He also disclosed to GE that he and "his brothers" own the company. Zheng has described the business as a "parts supplier for civil aviation engines."
- GE conducted a conflict-of-interest analysis and determined that Zheng's Chinese company presented at least three potential conflicts: However, GE did not instruct Zheng that his interest in the Chinese company was unacceptable and allowed Zheng to retain his GE employment.
- According to the publicly available internet postings, Zheng was a 2012 selectee of the "Thousand Talents Program" (a Chinese government program designed to recruit highly educated researchers to bring their skills to China).
- Steganography" is a means of hiding a data file within the code of another data file.
- Through talent recruitment programs like the Thousand Talents Program, the Chinese Communist Party pays scientists at American universities and businesses to steal knowledge and research to share with China.

Questions to consider:

- What policies does your organization use to deter, detect and mitigate a malicious insider from stealing proprietary information?
- After Zheng's security incident in 2014, what additional steps could GE take that may have prevent Zheng from successfully stealing their trade secrets?

Resources for further exploration:

- Counterintelligence Awareness for Defense Critical Infrastructure (https://www.cdse.edu/Portals/124/Documents/jobaids/ci/CDSE_CIP__Job_Aid.pdf)
- Foreign Collection Methods: Indicators and Countermeasures https://www.cdse.edu/Portals/124/Documents/jobaids/ci/foreign-collection-methods.pdf ()
- Establishing Prevention, Assistance, and Response (PAR) Capabilities (https://www.cdse.edu/Portals/124/Documents/jobaids/insider/INTJ0156-par.pdf)

Supporting Through Reporting!

Contact the appropriate POC to report any observed potential risk indicators:

Name: _____ Agency/Department: _____
Title: Supervisor/Security Officer/ITP Senior Official/ITP Manager