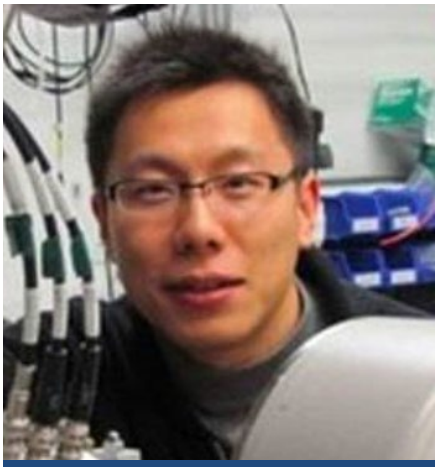

Hongjin Tan

- Staff Scientist at Phillips 66 Petroleum Company
- Chinese National
- Lived in the United States since 2012
- Legal permanent resident
- Earned a PhD at an American university
- Worked for a number of firms in California before making his way to the energy company in Oklahoma

CDSE

Center for Development of Security Excellence

CASE STUDY

Theft of Trade Secrets

WHAT HAPPENED

Hongjin Tan was a research scientist in the battery development group at Phillips 66 Petroleum Company. After nine months with Phillips 66 and giving them a two weeks' notice, he resigned. Tan told his superiors that he planned to return to China to care for his aging parents. He told Phillips that he had not arranged his next job, so the company agreed to let him continue working there until his departure date in December 2018.

However, Tan told a colleague over dinner that he did have a job waiting for him in China with Xiamen Tungsten. Xiamen Tungsten is a Chinese firm that smelts, processes, and distributes metal products and supplies battery materials. Tan's colleague reported the conversation to Phillips 66. One of Philips 66's most innovative products was a battery technology they had spent decades researching and developing. The technology has a secondary, and perhaps even more valuable, use in melting metal.

Tan's resignation prompted Phillips 66 to conduct a Systems Access review of Tan's computer activity. That review confirmed he had accessed hundreds of files, including research reports about the proprietary battery technology. The review revealed Tan downloaded restricted files to a personal thumb drive that he did not have authorization to use. Tan's supervisor confirmed that nothing in the downloaded files was within Tan's area of responsibility and that he did not have a work related need to access or download the restricted files.

Upon learning this, the company immediately fired Tan and began to look back at the documents and systems he had accessed while employed there. The company insisted Tan return the thumb drive.

When Tan brought back the thumb drive, the firm looked at the slack space on the drive and found several files had been erased. The deleted files were the files the company was most concerned about.

Tan pleaded guilty to theft of a trade secret, unauthorized transmission of a trade secret, and unauthorized possession of a trade secret and was sentenced to 24 months in federal prison and ordered to pay $150.000 in restitution.

INDICATORS

- Access Attributes – Tan used his privileged access to copy proprietary files without authorization and without a need to know
- Security and Compliance Incidents – Despite training on security procedures, Tan chose to illegally copy files for his new employer
- Foreign Considerations – Frequent unreported foreign travel, contact with foreign nationals, and undisclosed foreign employment
- Technical Activity – Tan used an unauthorized thumb drive to copy the files, and he attempted to hide the fact when he returned the thumb drive

IMPACT

Investigators say the information involved the manufacturing of a “research and development downstream energy market product.” The market value of the next-generation battery technology Tan was accused of stealing was more than $1 billion. Battery storage advances are a key goal under Beijing’s “Made in China 2025” blueprint aimed at fast-tracking its economy with applications for electric vehicles, alternate energy generation, and other green technologies.

Despite the fact that Tan was arrested and the thumb drive recovered, we cannot know for certain that Tan didn't transmit the unclassified documents on the thumb drive to China from his home, from a borrowed computer or some other location.

Hongjin Tan was a participant in the well-known Thousand Talents Plan that was launched by China in 2008. Through this plan, China aims to recruit foreign expertise in targeted scientific areas. The Chinese government offers lucrative financial and research benefits to recruit individuals working and studying outside of China who possess access to, or expertise in, high-priority research fields.

While mere participation in a “talent plan” is not illegal, investigations by the FBI and other agencies have revealed that participants are often incentivized to transfer to China the research they conduct in the United States, as well as other proprietary information to which they can gain access, and remain a significant threat to the United States. In Tan’s case, his participation resulted in violations of U.S. laws, including economic espionage and theft of trade secrets.

In addition, many talent plan participants sign contracts outlining work that mirrors the research they perform at American institutions. Investigators found such an employment contract on Tan’s laptop.

ADDITIONAL INFO

Hongjin Tan was captured thanks to the report from a colleague. Without that report, Phillips 66 could have lost a billion dollar technology. Implementation of user activity monitoring may have resulted in proactive identification of this behavior.

Consider the following questions:

- How can an insider threat program identify anomalous behavior?
- Why is user activity monitoring a part of an effective insider threat program?
- How do we balance the protection of First and Second Amendment rights with Safety and National Security?

Resources for further exploration:

- Insider Threat Indicators in User Activity Monitoring
  https://www.cdse.edu/Portals/124/Documents/jobaids/insider/Insider-Threat-Indicators-in-UAM.pdf
- Insider Threat Privacy and Civil Liberties INT 260.16 eLearning Course
  https://www.cdse.edu/Training/eLearning/INT260/

IF YOU SEE SOMETHING, SAY SOMETHING!

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

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