Center for Development of Security Excellence
CDSE
Learn. Perform. Protect.

INSIDER THREAT JOB AID

Insider Threat: Jiaqiang Xu – Economic Espionage

Who could become an insider threat? Anyone with authorized access to U.S. government resources who uses that access (either wittingly or unwittingly) to harm national security. Insider threats can have far reaching consequences and impacts on national security.

Jiaqiang Xu

- 32-year-old system software developer at a cleared company from November 2010 to May 2014
- A Naturalized U.S. citizen from China
- 2009 Master of Science, University of Delaware; 2007 Bachelor in Computer Science from Huazhong University of Science and Technology in China
- January 18, 2018: Sentenced to five years in federal prison for attempting to commit economic espionage and theft of a trade secret with the intent to benefit the National Health and Family Planning Commission, a government agency within the People's Republic of China

Insider Indicators

- User Activity Monitoring identified anomalies and reported to FBI
- Stolen proprietary information made available shortly following employment self-termination
- Anonymous report to FBI of someone in China claiming to have access to source code information and using it for business ventures
- Leak had to come from a very limited number of employees with access to source code information
- The victim company had an effective insider threat program in place

What Happened

- While employed by a cleared company, Xu stole proprietary software and source code information for his own profit
- May 2014: Xu resigned from the company and initiated attempts to market stolen software
- December 7, 2015: Xu demonstrated to FBI undercover agents he had developed a copy of the proprietary software using his former company's source code information and could write computer scripts modifying the propriety source code to conceal its origins

Impacts

- Those who steal America's trade secrets for the benefit of foreign nations pose a threat to our economic and national security interests
- Based on their trend analysis of cleared industry reporting, the DSS Counterintelligence Directorate indicates that foreign targeting of Command, Control, Communications, and Computers (C4) technologies has been a high priority for several years and will most likely continue to be highly sought after with the constant changes made within C4.

This case study examined a real-life insider threat. Your awareness is key to protecting our national security from insider threats like this one. Visit the Center for Development of Security Excellence's website (https://www.cdse.edu/catalog/insider-threat.html) for additional case studies, information, materials, and training or go directly to the Insider Threat Toolkit at (https://www.cdse.edu/toolkits/insider/index.php)

If you SEE something, SAY something.