Peter Kisang Kim

- Age 51 at time of sentencing
- Resided in Ben Lomond, CA
- Born in South Korea
- Moved to the United States with his family when he was 11 years old

CASE STUDY

Economic Espionage

WHAT HAPPENED

An indictment revealed that a federal grand jury in San Jose charged a former Broadcom engineer with stealing trade secrets. Kim was employed by Broadcom for over 20 years. His last role at the company was Principal Design Engineer with the design verification team in the Core Switch Group. Kim had worked on various Broadcom products during his time at the company, including the Trident family of networking integrated circuit (IC) chips (such as the Trident 3 and the Trident 4) that are frequently used in high-volume data centers.

In July 2020, Kim abruptly resigned from Broadcom. Before he left, Kim copied more than 500 sensitive Broadcom files from its document repository system and stole Broadcom trade secrets related to the Trident family of chips, including:

- Test plans for the Trident family of chips, including top-level chip features, flexible port speed, ingress data buffer, top-level performance, and layer 2 features
- Design verification environment files for the Trident family of chips, including scripts facilitating verification testing, compilation scripts, universal verification methodology, and memory interfacing
- Design specifications for the Trident family of chips, including top-level design and an interface sub-block (collectively, “Broadcom trade secrets”).

Less than two weeks following his departure from Broadcom, Kim began working as IC Design Verification Director for a startup company based in the People’s Republic of China (PRC). He wanted to become a leading chip designer focused on the PRC’s domestic market for networking chips.

At trial, Kim acknowledged that he knowingly stole and stored Broadcom trade secrets. Kim also admitted to signing confidentiality agreements with Broadcom and that he received annual training on confidentiality.

Kim pleaded guilty to three counts of Trade Secret Theft and was sentenced to eight months in prison, a fine of $5000, and restitution of $48,395.

INDICATORS

- **Technical Activity** – Kim copied more than 500 Broadcom files from its document repository system, which he was not authorized to access, and used it to advance his new career.
- **Allegiance to the United States** – Kim committed espionage against the United States, supporting and helping an Integrated Circuit startup company in the People’s Republic of China.
- **Access Attributes** – Kim had unauthorized access to Broadcom files and passed the information to the People’s Republic of China.

CDSE

Center for Development of Security Excellence

IMPACT

- The Broadcom trade secrets derived from independent economic value are not generally known or readily ascertainable through proper means. Broadcom lost more than $250,000 in research and development costs after their trade secrets were stolen by Kim.
- Kim admitted in his plea agreement that having the Broadcom information could injure Broadcom and benefit his new employer, which was seeking to become a competitor to Broadcom by developing competing products abroad in China.

ADDITIONAL INFO

- Kim had no opportunity to move into management at Broadcom and realized his skills were not as sharp as they once were, just like an aging athlete. Kim saw working for the Chinese networking chip design startup called Mersenne Technologies as his opportunity to become a manager.
- On April 29, 2021, FBI agents executed a federal search warrant at Kim's residence, seizing multiple electronic devices. Law enforcement's forensic review of the seized devices revealed that during Kim's employment at the Chinese company, he repeatedly accessed and referenced the Broadcom trade secrets on his personal electronic devices as well as his company-issued Lenovo laptop. Further, Kim looked at several of the Broadcom trade secrets while working on various materials, including verifications, test plans, and architecture documents for his Chinese employer.
- Kim admitted that he possessed the Broadcom trade secrets knowing that he took them illegally. In addition to using them for reference purposes, Kim knew that having them could advance the quality of his work as an employee for Mersenne and therefore economically benefit the company. Kim also knew that his actions could injure Broadcom by turning Mersenne into a competitor.

Questions to consider:

- What efforts could be implemented in your organization to enhance awareness of the real dangers associated with Insider Threats?
- Why didn't Kim just retire after working for Broadcom for 22 years instead of committing economic espionage?

Resources for further exploration:

Protecting Microelectronics Short: (https://usg01.safelinks.protection.office365.us/?url=https%3A%2F%2Fsecurityawareness.usalearning.gov%2Fcdse%2Fmultimedia%2Fshorts%2Fmicroelectronics%2Fstory.html&data=05%7C01%7Csamuel.s.dillard.ctr%40mail.mil%7C656e0c556b7146f7d20108dbf1acdfb0%7C102d0191eeae4761b1cb1a83e86ef445%7C0%7C0%7C638369497001807022%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C3000%7C%7C%7C&sdata=LXpcxQP8b63qt1hQyt9zMV8UHCdQE2tzgMCN1%2BEpN6k%3D&reserved=0)

- Insider Threats 101: What you need to know (https://www.cisa.gov/sites/default/files/2022-11/Insider%20Threats%20101%20What%20You%20Need%20to%20Know_508.pdf)
- Economic Espionage by the FBI (https://www.fbi.gov/file-repository/economic-espionage-1.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