CASE STUDY

Fraud



Jason Hines

- U.S. citizen
- Resident of Caldwell, New Jersey
- Age 44 at time of sentencing

WHAT HAPPENED

Hines operated a New Jersey-based communications company called Direct Business Services International (DBSI). DBSI serviced an array of international and domestic resellers and end-users with business communications equipment and software licenses. Prior to Hines' arrest and subsequent plea agreement, DBSI was an authorized partner with the company Avaya and would purchase a surplus of Avaya Direct International (ADI) license keys to resell on the open market.

Hines conspired with Brad Pearce to sell pirated ADI software licenses for proprietary telephone equipment manufactured by Avaya. These software licenses were required for end users to unlock telephone features such as voicemail and other functionalities. To protect the copyrighted software and ensure product integrity, Avaya utilized authorized resellers and distributors to generate these software license keys. Hines' co-conspirator, Brad Pearce, was a long-time employee of Avaya. Pearce secretly used his system administrator privileges to generate tens of thousands of unauthorized license keys which he then sold to Hines. After purchasing the fraudulently produced license keys from Pearce, Hines would sell them to his global network of resellers and end users. Over the duration of their fraud scheme, Pearce and Hines sold tens of thousands of pirated business telephone system software licenses, valued at over $88 million.

In July 2023, Hines pleaded guilty to conspiracy to commit wire fraud. In September 2023, Pearce also pleaded guilty to conspiracy to commit wire fraud.

In July 2024, Hines was sentenced to 18 months in prison, an additional 18 months of home confinement, and was ordered to forfeit $2 million. Additionally, Hines agreed to pay restitution in the amount of $5 million.

INDICATORS

- **Access Attributes –** Hines conspired with privileged users to obtain the information he needed to enact the wire fraud scheme. In addition to utilizing his own credentials, Brad Pearce used his system administrator privileges to hijack former ADI employees' accounts to generate software license keys.
- **Criminal Conduct –** Hines and his co-conspirators knowingly participated in an international scheme to sell pirated business telephone system software licenses.
- **Personal Conduct –** Throughout the course of his illicit activity, Hines and his co-conspirators knowingly utilized aliases to conceal their true identities.

CDSE
Center for Development of Security Excellence

IMPACT

- The ADI software licensing system that was exploited for Hines' and Pearce's wire fraud scheme has since been decommissioned.
- Although Pearce sold the pirated licenses to other users, Hines accounted for 55% of all purchases. Hines was one of the biggest users of the ADI license system in the world at the time of his arrest. Altogether, the scheme resulted in the sale of tens of thousands of pirated business telephone system software licenses, valued at over $88 million.

ADDITIONAL INFO

- Throughout the duration of Hines' elaborate wire fraud scheme, he utilized the aliases Joe Brown, Chad Johnson, and Justin Albaum. Hines' co-conspirators jointly utilized the alias Terri Jenkins.
- The retail value of each ADI license ranged from under $100 to thousands of dollars.
- The conspirators utilized a PayPal account created under a fictitious name to route their ill-gotten gains. They funneled the money to multiple bank accounts and then transferred it to investment and other bank accounts. They also purchased large quantities of gold valuables to hide the source of their income.

Questions to consider:

- How can your organization proactively address insider threats? What measures are currently in place to detect this type of activity?
- What tools could ADI have used to ensure the integrity of their business practices?

Resources for further exploration:

- Insider Threat Program (ITP) for Industry Job Aid
  (https://www.cdse.edu/Portals/124/Documents/jobaids/insider/insider-threat-job-aid-for-industry.pdf)
- Insider Threat Fraud Job Aid
  (https://www.cdse.edu/Portals/124/Documents/jobaids/insider/INT_Fraud_JobAid.pdf)
- Insider Threat Programs for the Critical Manufacturing Sector Implementation Guide
  (https://www.cdse.edu/Portals/124/Documents/jobaids/insider/insider-threat-implem-guide-critical-man-job-aid.pdf)
- Insider Risk in Software Supply Chains Poster
  (https://www.cdse.edu/Portals/124/Documents/posters/small/INTSupplyChain.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