January 31, 2014

A Byte Out of History

$10 Million Hack, 1994-Style

It was hardly the opening salvo in a new era of virtual crime, but it was certainly a shot across the bow.

Two decades ago, a group of enterprising criminals on multiple continents—led by a young computer programmer in St. Petersburg, Russia—hacked into the electronic systems of a major U.S. bank and secretly started stealing money. No mask, no note, no gun—this was bank robbery for the technological age.

Our case began in July 1994, when several corporate bank customers discovered that a total of $400,000 was missing from their accounts. Once bank officials realized the problem, they immediately contacted the FBI. Hackers had apparently targeted the institution’s cash management computer system—which allowed corporate clients to move funds from their own accounts into other banks around the world. The criminals gained access by exploiting the telecommunications network and compromising valid user IDs and passwords.

Working with the bank, we began monitoring the accounts for more illegal transfers. We eventually identified approximately 40 illegal transactions from late June through October, mostly going to overseas bank accounts and ultimately adding up to more than $10 million. Meanwhile, the bank was able to get the overseas accounts frozen so no additional money could be withdrawn.

The only location where money was actually transferred within the U.S. was San Francisco. Investigators pinpointed the bank accounts there and identified the owners as a Russian couple who had previously lived in the country. When the wife flew into San Francisco and attempted to withdraw funds from one of the accounts, the FBI arrested her and, soon after, her husband. Both cooperated in the investigation, telling us that the hacking operation was based inside a St. Petersburg computer firm and that they were working for a Russian named Vladimir Levin. (See the sidebar for more on the San Francisco angle of the case from one of the agents who worked it.)

We teamed up with Russian authorities—who provided outstanding cooperation just days after a new FBI legal attaché office had been opened in Moscow—to gather evidence against Levin, including proof that he was accessing the bank’s computer from his own laptop. We also worked with other law enforcement partners to arrest two co-conspirators attempting to withdraw cash from overseas accounts; both were Russian nationals who had been recruited as couriers and paid to take the stolen funds that had been transferred to their personal accounts.

In March 1995, Levin was lured to London, where he was arrested and later extradited back to the United States. He pled guilty in January 1998.

Believed to be the first online bank robbery, the virtual theft and ensuing investigation were a needed wakeup call for the financial industry…and for law enforcement. The victim bank put corrective measures in place to shore up its network security. Though the hack didn’t involve the Internet, the case did generate media coverage that got the attention of web security experts. The FBI, for its part, began expanding its cyber crime capabilities and global footprint, steadily building an arsenal of tools and techniques that help us lead the national effort to investigative high-tech crimes today.

Reflections of a Case Investigator

Special Agent Andrew Black, who back in 1994 was part of a white-collar crime squad in the FBI's San Francisco Office, recalled that he became involved in the New York-based investigation when it was discovered that some of the money moved out of the bank by the hacker ended up in several San Francisco bank accounts.

"At the time," Black said, "we didn't have a cyber crime team in the office, so the white-collar crime route seemed the most logical way to go." He remembered that in August 1994, after identifying the owners of the bank accounts as Russian nationals Evygeny and Ekaterina Korlokova—who had an apartment in San Francisco—Ekaterina attempted to withdraw funds from one of the accounts. "Because the account had been frozen, she wasn't able to get the money," he said. Ekaterina went back to her apartment and started packing her bags. Black said when he and an FBI interpreter went to her residence to arrest her, her suitcases were in the hallway and she had a one-way ticket to Russia.

And where was her husband? Black said Evygeny had flown back to Russia, "leaving his young wife alone in the U.S. to withdraw the illegal funds from their bank accounts." But Ekaterina, who agreed to cooperate in the investigation, managed to convince him to return—according to Black, she "read him the riot act over the phone…in Russian, of course." He returned, was arrested, and agreed to cooperate as well.

Black remembered that the case garnered a great deal of attention at the time, "which was good, because it resulted in a lot more focus on network security." And after it ended, he gave presentations on it to raise general awareness of an emerging criminal threat. "There was a particularly high demand for the presentation from the banking industry," he added. And in 1995, Black was asked to become a part of the San Francisco FBI's newly formed computer intrusion squad…one of the Bureau's first.

Read about today's FBI cyber crime efforts (https://www.fbi.gov/investigate/cyber)