Bloomberg Businessweek

News From Bloomberg

http://www.businessweek.com/news/2014-04-17/grape-condom-carrying-hacker-lured-from-romania-by-u-dot-s-dot-agents

Hacker Lured From Romania by U.S. Agents, Complete With Grape Condoms

By Del Quentin Wilber April 17, 2014

U.S. Secret Service Agent Matt O'Neill was growing nervous. For three months, he'd been surreptitiously monitoring hackers' communications and watching as they siphoned thousands of credit card numbers from scores of U.S. retailers.

Most every day O'Neill was alerting a credit card company or retailer to an online heist. The result was predictable: the companies canceled hijacked credit and debit cards and the aggravated hackers' customers began complaining that the stolen card numbers weren't working as promised.

It was only a matter of time before the cyber thieves realized they were being watched.

"We were hoping they wouldn't figure it out until we could catch them," O'Neill said.

The Secret Service and FBI are investigating an increasing number of attacks on U.S. retailers' data, including the massive breach of Target Corp (TGT:US). last year that affected more than 40 million debit and credit card accounts. Investigators won't talk about the Target probe. Instead, the Secret Service pointed to O'Neill's investigation that began in 2010 as an example of how they go about solving such crimes.

The chase for the hackers took three years. It uncovered what federal prosecutors described in court records as a "massive, international computer hacking and credit card data theft scheme."

800 Stores

The conspirators hit more than 800 U.S. stores from 2009 to 2011, stealing data from in excess of 150,000 credit card accounts and inflicting losses to financial institutions conservatively tallied at $12.5 million, according to interviews with the agent, his supervisors and U.S. Justice Department prosecutors, as well as a review of court filings.

O'Neill's green eyes and sly grin mask an intensity for the hunt that relied on a mix of high-tech sleuthing and traditional police work, with some creativity sprinkled in: the agent even went undercover online as an "attractive, independently wealthy waitress."

"These hackers are sophisticated," said U.S. Secret Service Agent Ed Lowery, who is in charge of the agency's criminal division. "The type of individual we are talking about -- the highest-level cyber criminal --

they don't leave bread crumbs."

The son of a former Secret Service agent who investigated counterfeiting rings in Philadelphia, O'Neill joined the service in 1998 after a post-college stint at ESPN. He specialized in cyber crimes, except for four years on Vice President Dick Cheney's security detail.

'Subway Case'

In the agency's four-agent Manchester, New Hampshire, office, he juggled five or six cases at a time. None were as big as what became known as the "Subway case."

It began on a February afternoon in 2010 with calls from banks. American Express (AXP:US) and Citibank (C:US) reported fraudulent activity on accounts that had one thing in common -- purchases made at a Subway sandwich shop in Plaistow, New Hampshire, a town of 7,609 people about 25 miles southeast of Manchester. American Express reported that 36 compromised credit cards had been used at the Plaistow Subway; Citibank said it had suffered $80,000 in losses tied to cards swiped at the store.

Within days, O'Neill and a New Hampshire state trooper were inspecting the store's computer. It was clear it had been hacked through the Internet, and the attacker had planted a "key logger" program onto its hard drive. Acting like a vacuum cleaner, the program sucked up the data from credit and debit cards swiped through the store's magnetic reader.

The investigators determined the stolen data was only stored briefly on the computer before being uploaded to a website, ftp.tushtime.info.

Romanian Beetle

A password embedded in the software code -- Carabus05 -- provided a clue to its source. When O'Neill Googled the word, he discovered it was Romanian for beetle. Russia, Romania and other Eastern European countries are hotbeds for hackers.

"The important thing in these cases isn't so much: How did they get in?" O'Neill said. "It's: Where did the data go? It's the destination that matters."

Representatives of Subway Restaurants reported multiple hacks of other stores and the stolen data was flowing to several "dump sites" such as ftp.tushtime.info.

Armed with search warrants, O'Neill saw the stolen data was flowing from the dump sites to computer servers scattered across the U.S. Agents tracked down those servers -- one belonged to a law office, another a dentist -- but none were still being used by the hackers. Then, in July of 2010, O'Neill got lucky.

One of those computer servers belonged to New Harrisburg Truck and Body in Mechanicsburg, Pennsylvania. With permission from the shop's innocent owner, agents in August 2010 placed a "sniffer" on his computer.

Truck Shop

The sniffer revealed that the hackers were using the truck shop's computer to store and use their "tools" -- malicious software that scanned the Internet for vulnerable computers, allowed them to break into those computers, steal the data, upload it to a dump site, download it to the truck shop's computer and then zap it around the globe.

The hackers were careful. They masked their identities by using anonymous e-mail and chat accounts. They hid their location by routing through other servers in Europe.

Even so, O'Neill suspected they were in Romania. They chatted in e-mails in the language, and the agent managed to track some of their computer activity back to the country.

It was now late 2010 and O'Neill was getting concerned that the hackers would figure out he was monitoring them. The Secret Service was caught in a Catch-22: agents wanted to keep watching in secret to find out the hackers' identities yet had an obligation to alert customers, retailers and financial institutions that the accounts had been hacked.

"Their clients were emailing them and saying, 'Why are you cheating me? These are bum cards,'" O'Neill said, of the messages he secretly read.

Solid Lead

Finally, in late October, agents picked up a solid lead: in an online chat, a hacker mentioned that his computer had been seized and his house raided by Romanian police investigating his cyber activities.

O'Neill called his Romanian counterparts and provided them with the information. In less than a day, they gave O'Neill the hacker's identity: Adrian Tiberiu Oprea, a 26-year-old who had studied computer science and lived in the Black Sea port city of Constanta. Romanian authorities told O'Neill they were investigating Oprea for hacking retailers in Eastern Europe.

From the hackers' e-mails and social media postings, O'Neill found the identity of one Oprea's customers: a Romanian living in France named Cezar Butu, 27.

A third member of the conspiracy was harder to identify. In January 2011, O'Neill was examining more than 15,000 e-mails from an anonymous account when he found two that stood apart. They were from a personal e-mail and had attachments that were core to the scam: a program that masked the hackers' activities in their victims' computers, and a trove of stolen credit card numbers.

E-Mail Mistake

The hacker had mistakenly used his personal account to forward himself the information. The misstep was enough for O'Neill to finger Iulian Dolan, 25, a third Romanian.

O'Neill and the federal prosecutors still weren't optimistic that they could put the Romanians on trial. Though the U.S. has an extradition treaty with Romania, getting the country to hand over suspects was far from guaranteed.

"I thought our best case scenario would be that we would approach Romanian law enforcement and hope we

could convince them to prosecute these people, assuming we could ever able to identify them," said Mona Sedky, a prosecutor in the U.S. Justice Department's computer crimes division. "I never in a million years thought they would see the inside of a U.S. courtroom."

O'Neill and his Romanian counterparts discussed his options, which amounted to taking the risk of trying to extradite the men, or finding a less official way to arrest them. "They basically said, 'Do whatever you can do legally to get them to the United States,'" O'Neill recalled.

Ladies Man

Research showed the thieves had obvious weaknesses: Dolan was an online gambler, and Butu was a ladies' man. To capture Dolan, O'Neill became "Sarah," a marketing specialist for a Connecticut casino who invited the Romanian to a poker tournament.

For eight months, O'Neill e-mailed Dolan, sometimes late at night from his home where he was on paternity leave with a baby boy. His wife was understanding: she's an agent with the U.S. Federal Bureau of Investigation.

"Dolan seemed kind of like a lonely guy," O'Neill said. "And, yes, there was some gentle flirting." When Dolan finally walked off the plane in Boston on Aug. 13, 2011, he was carrying a gold necklace for "Sarah" and six boxes of grape-flavored condoms.

"He was being optimistic," O'Neill said.

Meanwhile, O'Neill was also masquerading as "Chrissy," a wealthy waitress for a restaurant chain known for its scantily-clad servers, who had met Butu during a recent sojourn through Europe.

Wealthy Waitress

O'Neill's gambit this time was that "Chrissy" had enjoyed meeting Butu and hoped to re-establish contact. Eventually, "Chrissy" invited Butu to visit her in the U.S. Butu took the bait, arriving in Boston the day after Dolan.

"You tell them what they want to hear, within reason," O'Neill said.

He took the traditional route with Oprea. The U.S. government sought the Romanian's extradition. It worked: Oprea was arrested in December 2011 and sent to New Hampshire in May of last year.

All three pleaded guilty to hacking-related charges, admitting they hit more than 800 U.S. stores, about 250 of which were Subways. In interviewing Dolan and Oprea, O'Neill determined that they didn't target Subway. It was just luck that so many got hacked. There are about 25,000 Subways in the U.S. and many had poor online security, O'Neill said.

As for the hackers, they didn't make much profit -- Oprea, the ring leader, made only $40,000. He paid a steep price for the estimated $12.5 million in losses inflicted on financial institutions and the $5 million Subway spent upgrading its cyber security systems. Oprea was sentenced in September to 15 years in federal prison. Butu got 21 months behind bars, and Dolan received a 7-year sentence.

“They weren’t stealing from Romanians,” O’Neill said, “so they never expected to get caught.”

To contact the reporter on this story: Del Quentin Wilber in Washington at dwilber@bloomberg.net

To contact the editors responsible for this story: Steven Komarow at skomarow1@bloomberg.net Jeanne Cummings

---