NEWS

United States Department of Justice
U.S. Attorney, District of New Jersey
970 Broad Street, Seventh Floor
Newark, New Jersey 07102

Ralph J. Marra, Jr., Acting U.S. Attorney

More Information? Call the Assistant U.S. Attorney or other contact listed below to see if more information is available.

News on the Internet: News Releases, related documents and advisories are posted short-term at our website, along with links to our archived releases at the Department of Justice in Washington, D.C. ***Go to:*** **http://www.usdoj.gov/usao/nj/press/**

Assistant U.S. Attorneys
SETH KOSTO
EREZ LIEBERMANN

gonz0817.rel
FOR IMMEDIATE RELEASE
Aug. 17, 2009

Three Men Indicted for Hacking into Five Corporate Entities, including Heartland, 7-Eleven, and Hannaford, With Over 130 Million Credit and Debit Card Numbers Stolen

(More)

Public Affairs Office **973-645-2888**
http://www.njusao.org
Michael Drewniak, PAO

NEWARK, N.J. – An Indictment was returned today against three individuals who are charged with being responsible for five corporate data breaches, including the single largest reported data breach in U.S. history, announced Acting U.S. Attorney Ralph J. Marra, Jr., along with Assistant Attorney General of the Criminal Division Lanny A. Breuer and United States Secret Service Director Mark Sullivan.

The scheme is believed to constitute the largest hacking and identity theft case ever prosecuted by the U.S. Department of Justice.

The Indictment describes a scheme in which more than 130 million credit and debit card numbers together with account information were stolen from Heartland Payment Systems, Inc., based in Princeton, N.J., 7-Eleven, Inc., and Hannaford Brothers Co. In addition, the Indictment describes two unidentified corporate victims as being hacked by the coconspirators.

As alleged in the Indictment, between October 2006 and May 2008, Albert Gonzalez, 28, of Miami, Fla., acted with two unnamed coconspirators to identify large corporations, often by scanning the list of Fortune 500 companies and exploring corporate websites. Upon identifying a potential victim, Gonzalez and his coconspirators sought to identify vulnerabilities, both by physical observation and by online exploration. For example, according to the Indictment, Gonzalez and an individual identified in the Indictment as "P.T." would go to the retail locations of their potential victims in an attempt to identify the type of point-of-sale ("checkout") machines utilized by the victim companies. After reconnaissance of the computer systems was completed, information would be uploaded to servers which served as hacking platforms. These servers, located in New Jersey and around the world, were used by the coconspirators to store information critical to the hacking schemes and to subsequently launch the hacking attacks.

According to the Indictment, the hacking attacks launched against the corporate victims consisted of what is known as a SQL-injection attack, which is an attack that exploits security vulnerabilities in elements of a computer that receives user input. Gonzalez provided some of the malicious software (malware) to his coconspirators, and they added their own as they sought to identify the location of credit and debit card numbers and other valuable data on the corporate victims' computer systems.

The coconspirators often worked together on a real-time basis, contacting each other by instant messaging as they were improperly accessing the corporate victims' computer systems, according to the Indictment. Once the target information was discovered, it would be stolen from the corporate victims' servers and placed onto servers controlled by Gonzalez and the coconspirators. In addition to searching for credit and debit card data on the victims' computer systems, the Indictment alleges that Gonzalez and the coconspirators installed "sniffers" which conducted real-time interception of credit and debit card data being processed by the corporate victims and subsequently stolen from the corporate victims' computer servers.

The Indictment alleges that Gonzalez and the coconspirators employed numerous techniques to hide their hacking efforts and data breaches. For example, they allegedly accessed the corporate websites only through intermediary, or "proxy," computers, thereby disguising their own whereabouts. They also tested their malware by using approximately twenty of the leading anti-virus products to determine if any of those products would detect their malware as potentially unwanted. Furthermore, they programmed their malware to actively delete traces of the malware's presence from the corporate victims' networks.

Upon stealing the credit and debit card data, Gonzalez and the coconspirators would seek to sell the data to others who would use it to make fraudulent purchases, make unauthorized withdrawals from banks and further identity theft schemes.

"This investigation marks the continued success of law enforcement in tracking down cutting edge hacking schemes committed by hackers working together across the globe," said Marra. Marra added that the investigation was greatly facilitated by those companies that took a proactive approach in working with law enforcement to identify and stop hackers. "When companies make the decision to work with law enforcement and disclose a data breach at the earliest possible opportunity, it provides the best chance at apprehending a hacker and demonstrates that those corporate victims will actively defend their systems."

A federal grand jury sitting in Newark, N.J., charged Gonzalez and two individuals identified only as "Hacker 1," and "Hacker 2," both in or near Russia, in the two-count Indictment. The first count charges conspiracy to (1) gain unauthorized access to computers, (2) commit fraud in connection with computers, and (3) damage computers. The second count charges conspiracy to commit wire fraud. Each defendant faces a maximum penalty of 5 years in prison on Count One and an additional 30 years on Count Two, for a total of 35 years. In addition, each of the individuals is subject to a maximum fine of $250,000 per Count One, and $1 million per Count Two, or twice the gain resulting from the offense, whichever is greater.

Gonzalez was previously indicted in the Eastern District of New York on May 12, 2008, and the District of Massachusetts on August 5, 2008, for his involvement in different conspiracies relating to data breaches of multiple companies. He was also previously arrested in New Jersey in 2003 for his role in ATM and debit card fraud. Gonzalez is currently detained in the Metropolitan Detention Center in Brooklyn, New York.

Marra credited the Special Agents of the United States Secret Service, under the direction of Special Agent in Charge Cynthia Wofford, for their work in the investigation.

An Indictment is merely an accusation, and all defendants are presumed innocent unless and until proven guilty beyond a reasonable doubt.

The case is being prosecuted by Assistant U.S. Attorneys Seth Kosto and Erez Liebermann of the U.S. Attorney's Office Computer Hacking and Intellectual Property Section, part of the Commercial Crimes Unit in Newark, New Jersey, and Senior Counsel Kimberly Kiefer

Peretti of the Criminal Division’s Computer Crime & Intellectual Property Section.

-end-