

06 August 2008

US authorities bust card hacking gang in biggest ever ID fraud case

US authorities have indicted an international criminal gang thought to be responsible for the theft and sale of over 40 million credit and debit card numbers that were hacked from the computer systems of nine major US retailers, including TJX.

In what is believed to be the largest hacking and ID theft case ever prosecuted by the Department of Justice (DoJ), three US citizens, one man from Estonia, three from Ukraine, two from China and one from Belarus, as well as another individual who is only known by an online alias, have been charged with numerous counts of fraud and ID theft.

In an indictment returned yesterday by a federal grand jury in Boston, Albert "Segvec" Gonzalez, of Miami, was charged with computer fraud, wire fraud, access device fraud, aggravated ID theft and conspiracy for his role in the scheme.

Gonzalez, alongside Christopher Scott and Damon Patrick Toey, all from Miami, are accused of hacking into the wireless computer networks of retailers, including TJX, BJ's Wholesale Club, OfficeMax, Boston Market, Barnes & Noble, Sports Authority, Forever 21 and DSW.

The defendants then allegedly installed "sniffer" programs that would capture card numbers, as well as password and account information, as they moved through the retailers' credit and debit processing networks.

Once the data was collected it was concealed in encrypted computer servers that the defendants controlled in Eastern Europe and the US, says the DoJ. Some of the card numbers were sold to other criminals in the US and Eastern Europe over the Internet.

The stolen numbers were "cashed out" by encoding card numbers on the magnetic strips of blank cards. The DoJ says the defendants then used these cards to withdraw tens of thousands of dollars at a time from ATMs.

Prosecutors say Gonzalez and others were allegedly able to conceal and launder their fraud proceeds by using anonymous Internet-based currencies both within the US and abroad and by channelling funds through bank accounts in Eastern Europe.

Meanwhile, in related charges bought in San Diego, eight people are accused of operating an international stolen credit and debit card distribution ring.

In May Gonzalez, and two of the men charged in San Diego were also charged in a related indictment in New York alleging that the trio hacked into computer networks run by the Dave & Buster's restaurant chain and stole card numbers from at least 11 locations.

Gonzalez had been arrested by the secret service for access device fraud in 2003 and was actually working for the agency as an informant. But during the course of the investigation it was discovered he was involved in the activities, says the DoJ. He now faces a maximum penalty of life in prison if he is convicted of all the charges alleged in the Boston indictment.

In a statement released by the DoJ, US Attorney General, Michael Mukasey, says: "So far as we know, this is the single largest and most complex identity theft case ever charged in this country."

US Attorney Michael Sullivan, adds: "While technology has made our lives much easier it has also created new vulnerabilities. This case clearly shows how strokes on a keyboard with a criminal purpose can have costly results."

Convictions have already been made in connection to the stolen data. Last September the ringleader of a gang that used financial information stolen during the computer hacking at TJX was sentenced to five years in prison and ordered to pay nearly \$600,000 in restitution.

Irving Escobar, 19, from Miami, pleaded guilty to charges that he participated in a criminal operation that used counterfeit cards featuring credit card data stolen data from the TJX data breach in December 2006.

Five other gang members who were accused of playing lesser roles in the operation also pleaded guilty to similar charges in Florida courts.

However, this gang is not believed to have been involved in the actual hacking at TJX.

UK card cloner jailed

On a smaller scale, a UK petrol station worker who used a fake card reader to clone the bank cards of hundreds customers in the Leicestershire village of Houghton-on-the-Hill has been jailed.

Abdul Samad Mohamed Raik, 33, used the card details of more than 500 cards to steal around £175,000 between October and December last year.

Raik gave himself up to police in March and admitted obtaining property by deception. He was sentenced to two years and nine months.

