Hackers charged for global racket

NEW YORK CITY, USA: The US authorities indicted five men on Thursday, 25 July, on charges of running a global hacking operation that enabled them to steal the bank card numbers of more than 160m people.

Prosecutors in Newark, New Jersey described the scheme as the largest hacking and data breach case ever prosecuted in the United States.

According to the indictment, the men - four Russians and a Ukrainian - targeted major payment processors, retailers and financial institutions around the world over the course of seven years, resulting in hundreds of millions of dollars in losses.

The defendants were charged with attacks on, among others, NASDAQ, Visa Jordan, the Belgian bank Dexia, and Diners Singapore. Just three of the corporate victims have reported combined losses in excess of US$300m.

"This type of crime is the cutting edge," New Jersey US Attorney Paul Fishman said.

"Those who have the expertise and the inclination to break into our computer networks threaten our economic well-being, our privacy and our national security," he said.

Hackers named, arrested

The defendants were named as Russians Vladimir Drinkman, Alexandr Kalinin, Roman Kotov and Dmitriy Smilianets, and Ukrainian Mikhail Rytikov.

Only Smilianets is currently in US custody. He was arrested in the Netherlands last year along with Drinkman and extradited. Drinkman is awaiting an extradition hearing in the Netherlands. The other three suspects are still at large.

US investigators have been on the trail of the hackers for at least four years with Kalinin and Drinkman having been identified as Hacker 1 and Hacker 2 in a 2009 indictment of Albert Gonzalez, who was subsequently convicted and

sentenced to 20 years in prison for accessing the confidential data of Heartland Payment Systems and other corporations in what was, until then, the biggest case of its kind.

The pair were described as specialists in penetrating network security and gaining access to the systems of major corporations. Moscow-based Kotov was said to be the expert in mining the networks his accomplices had opened up.

This involved installing malicious code, or malware, on compromised systems, enabling the harvesting of user names and passwords, means of identification and bank card numbers.

Conservative estimates

The US investigators regard the estimate of 160m numbers obtained by the group as a conservative one. The group was prepared to wait for months at a time for their efforts to break a particular company's security.

Instant message chats between the defendants indicate they had malware implanted on some companies' servers for over a year, according to investigators.

Rytikov, based in Odessa in the Ukraine, allegedly ran the web-hosting services the hackers used to disguise their activities and Similianets, also a Muscovite, was said to be the person who sold on the information and shared the proceeds with the group.

A stolen American credit card number and the details needed to use it were said to be worth US$10, a Canadian one US$15 and a European one US$50 to the identity theft wholesalers who bought the data.

They would then sell them on to individuals who could encode the data onto blank plastic cards and use them to buy goods or make cash withdrawals.

Meanwhile, Kalinin was also named on Thursday, 25 July, in a separate indictment in New York which accuses him of hacking into computer servers used by the New York technology market NASDAQ.

He is charged by the New York authorities with a scheme to steal bank account information from US financial institutions in partnership with another Russian hacker, Nikolay Nasenkov.

Source: AFP via I-Net Bridge