THE UNITED STATES ATTORNEY'S OFFICE
EASTERN DISTRICT of NEW YORK

NEWS

May 09, 2013

Eight Members of New York Cell of Cybercrime Organization Indicted in $45 Million Cybercrime Campaign

New York Cell Withdrew $2.8 Million In Cash From Hacked Accounts In Less Than 24 Hours

A four-count federal indictment was unsealed in Brooklyn charging eight defendants with participating in two worldwide cyberattacks that inflicted $45 million in losses on the global financial system in a matter of hours.[1] These defendants allegedly formed the New York-based cell of an international cybercrime organization that used sophisticated intrusion techniques to hack into the systems of global financial institutions, steal prepaid debit card data, and eliminate withdrawal limits. The stolen card data was then disseminated worldwide and used in making fraudulent ATM withdrawals on a massive scale across the globe. The eight indicted defendants and their co-conspirators targeted New York City and withdrew approximately $2.8 million in a matter of hours. The defendants are charged variously with conspiracy to commit access device fraud, money laundering conspiracy, and money laundering.

Seven of the eight defendants have been arrested on the charges in the indictment: the arrested defendants are Jael Mejia Collado, Joan Luis Minier Lara, Evan Jose Peña, Jose Familia Reyes, Elvis Rafael Rodriguez, Emir Yasser Yeje, and Chung Yu-Holguin, all residents of Yonkers, New York. Rodriguez was arrested on a criminal complaint on March 27, 2013, when he attempted to flee the United States for the Dominican Republic. Peña was arrested on a criminal complaint in Yonkers, New York, on April 3, 2013. Lara, Reyes, and Yeje surrendered to law enforcement authorities on April 15, 2013, and Collado and Yu-Holguin were arrested yesterday afternoon. The indictment also charges an eighth defendant, Alberto Yusi Lajud-Peña, also known as "Prime" and "Albertico," who is reported to have been murdered on April 27, 2013, in the Dominican Republic. The case has been assigned to United States District Judge Kiyo A. Matsumoto.

The charges were announced by Loretta E. Lynch, United States Attorney for the Eastern District of New York, Steven Hughes, Special Agent in Charge, United States Secret Service, New York Field Office, and James T. Hayes, Jr., Special Agent in Charge, U.S. Immigration and Customs Enforcement (ICE), Homeland Security Investigations (HSI), New York.

"As charged in the indictment, the defendants and their co-conspirators participated in a massive 21st century bank heist that reached across the Internet and stretched around the globe. In the place of guns and masks, this cybercrime organization used laptops and the Internet. Moving as swiftly as data over the Internet, the organization worked its way from the computer systems of international corporations to the streets of New York City, with the defendants fanning out across Manhattan to steal millions of dollars from hundreds of ATMs in a matter of hours," stated United States Attorney Lynch. "Law enforcement is committed to moving just as swiftly to solve these cybercrimes and bring their perpetrators to justice."

"New technologies and the rapid growth of the Internet have eliminated the traditional borders of financial crimes and provided new opportunities for the criminal element to threaten the world's financial systems. However, as demonstrated by the charges and arrests announced today, the Secret Service and its law enforcement partners have adapted to these technological advancements and utilized cutting edge investigative techniques to thwart this cybercriminal activity," said Secret Service Special Agent in Charge Hughes. "I want to take this opportunity to commend the dedicated men and women of the Secret Service and HSI for their extraordinary efforts in this investigation. This case is an excellent example of the impact that can be made when the law enforcement community works together."

"The arrests today reflect the government's joint efforts to bring a global cybercrime enterprise to justice," said HSI Special Agent in Charge Hayes. "HSI is proud to be part of a proactive federal law enforcement initiative that uses its collective resources to pull the plug on those who attempt to use the Internet to commit bank robbery."

The "Unlimited Operation"

As alleged in the indictment and other court filings, the cyberattacks employed by the defendants and their co-conspirators in this case are known in the cyber underworld as "Unlimited Operations" – through its hacking "operation," the cybercrime organization can access virtually "unlimited" criminal proceeds.

The "Unlimited Operation" begins when the cybercrime organization hacks into the computer systems of a credit card processor, compromises prepaid debit card accounts, and essentially eliminates the withdrawal limits and account balances of those accounts. The elimination of withdrawal limits enables the participants to withdraw literally unlimited amounts of cash until the operation is shut down. "Unlimited Operations" are marked by three key characteristics: (1) the surgical precision of the hackers carrying out the cyberattack, (2) the global nature of the cybercrime organization, and (3) the speed and coordination with which the organization executes its operations on the ground. These attacks rely upon both highly sophisticated hackers and organized criminal cells whose role is to withdraw the cash as quickly as possible.

As alleged in court filings, "Unlimited Operations" are executed in the following manner: First, over the course of months, the hackers plan and execute sophisticated cyber intrusions to gain unauthorized access to the computer networks of credit card processors that are responsible for processing prepaid debit card transactions. They target databases of prepaid debit cards, which are typically loaded with finite funds; such cards are used by many employers in lieu of paychecks and by charitable organizations to distribute disaster assistance. The cybercriminals breach the debit card accounts' security protocols, then

dramatically increase the balances and effectively eliminate the withdrawal limits on the accounts. The elimination of withdrawal limits enables the participants to withdraw unlimited amounts of cash until the operation is shut down. Next, the cybercrime organization cashes in, by distributing the hacked prepaid debit card numbers to trusted associates around the world – the two cyberattacks charged in this case allegedly involved 26 countries. These associates operate cells or teams of "cashers," who encode magnetic stripe cards, such as gift cards, with the compromised card data. When the cybercrime organization distributes the personal identification numbers (PINs) for the hacked accounts, the casher cells spring into action, immediately withdrawing cash from ATMs across the globe. Meanwhile, the cybercrime organization maintains access to the computer networks of the credit card processors they have hacked in order to monitor the withdrawals. At the end of an operation, when the cards are finally shut down, the casher cells launder the proceeds, often investing the operation's proceeds in luxury goods, and kick money back up to the cybercrime organization's leaders.

The Charged "Unlimited Operation" Cyberattacks

According to the government's filings, between approximately October 2012 and April 2013, the defendants and their co-conspirators conducted two Unlimited Operations. The first operation, on December 22, 2012, targeted a credit card processor that processed transactions for prepaid MasterCard debit cards issued by the National Bank of Ras Al-Khaimah PSC, also known as RAKBANK, in the United Arab Emirates. After the hackers penetrated the credit card processor's computer network, compromised the RAKBANK prepaid card accounts, and manipulated the balances and withdrawal limits, casher cells across the globe operated a coordinated ATM withdrawal campaign. In total, more than 4,500 ATM transactions were conducted in approximately 20 countries around the world using the compromised RAKBANK account data, resulting in approximately $5 million in losses to the credit card processor and RAKBANK. In the New York City area alone, over the course of just two hours and 25 minutes, the defendants and their co-conspirators conducted approximately 750 fraudulent transactions, totaling nearly $400,000, at over 140 different ATM locations in New York City.

As alleged in the indictment and other court filings, the second of these Unlimited Operations occurred on the afternoon of February 19 and lasted into the early morning of February 20, 2013. This operation again breached the network of a credit card processor that serviced MasterCard prepaid debit cards, this time issued by the Bank of Muscat, located in Oman. Again, after the cybercrime organization's hackers compromised Bank of Muscat prepaid debit card accounts and distributed the data, the organization's casher cells engaged in a worldwide ATM withdrawal campaign. This attack was particularly devastating: Over the course of approximately 10 hours, casher cells in 24 countries executed approximately 36,000 transactions worldwide and withdrew about $40 million from ATMs. From 3 p.m. on February 19 through 1:26 a.m. on February 20, the defendants and their co-conspirators withdrew approximately $2.4 million in nearly 3,000 ATM withdrawals in the New York City area.

As charged in the indictment and other filings, defendant Alberto Yusi Lajud-Peña was the leader of the New York cell of this organization, and in the wake of the charged Unlimited Operations, he and defendants Elvis Rafael Rodriguez and Emir Yasser Yeje laundered hundreds of thousands of dollars in illicit cash proceeds. In one transaction alone, nearly $150,000 in the form of 7,491 $20 bills, was deposited at a bank branch in Miami, Florida, into an account controlled by defendant Alberto Yusi Lajud-Peña. Cell members

also invested the criminal proceeds in portable luxury goods, such as expensive watches and cars. To date, the United States has seized hundreds of thousands of dollars in cash and bank accounts, two Rolex watches and a Mercedes SUV, and is in the process of forfeiting a Porsche Panamera. The Mercedes and Porsche were purchased with $250,000 in proceeds of this scheme.

In announcing the charges, United States Attorney Lynch praised the extraordinary efforts of the Secret Service in responding so rapidly to these attacks and investigating both the complex network intrusions that occurred overseas and the criminal activity occurring locally. Ms. Lynch also thanked the Department of Homeland Security for its invaluable role in recent arrest and seizure operations, as well as MasterCard, RAKBANK, and the Bank of Muscat for their cooperation with this investigation. Ms. Lynch expressed gratitude for the timely and extensive assistance of law enforcement authorities in Japan, Canada, Germany, and Romania, and also thanked authorities in the United Arab Emirates, Dominican Republic, Mexico, Italy, Spain, Belgium, France, United Kingdom, Latvia, Estonia, Thailand, and Malaysia for their cooperation in this investigation.

If convicted, the defendants face a maximum sentence of 10 years' imprisonment on each of the money laundering charges and 7.5 years on the conspiracy to commit access device fraud charge, restitution, and up to $250,000 in fines. In addition, all property involved in the money laundering offenses and all proceeds of the conspiracy to commit access device fraud are subject to forfeiture.

The government's case is being prosecuted by Assistant United States Attorneys Cristina M. Posa, Hilary Jager, Brian Morris, and Kevin Trowel.

The Defendants:

ALBERTO YUSI LAJUD-PEÑA (deceased)
Age: 23

JAEL MEJIA COLLADO
Age: 23

JOAN LUIS MINIER LARA
Age: 22

EVAN JOSE PEÑA
Age: 35

JOSE FAMILIA REYES
Age: 24

ELVIS RAFAEL RODRIGUEZ
Age: 24

EMIR YASSER YEJE
Age: 24

CHUNG YU-HOLGUIN
Age: 22

[1] The charges contained in the indictment are merely allegations, and the defendants are presumed innocent unless and until proven guilty.