11

Cyber Crime, Bitcoin,and Money Laundering[1]

Crime Group v. **Alert Citizens**

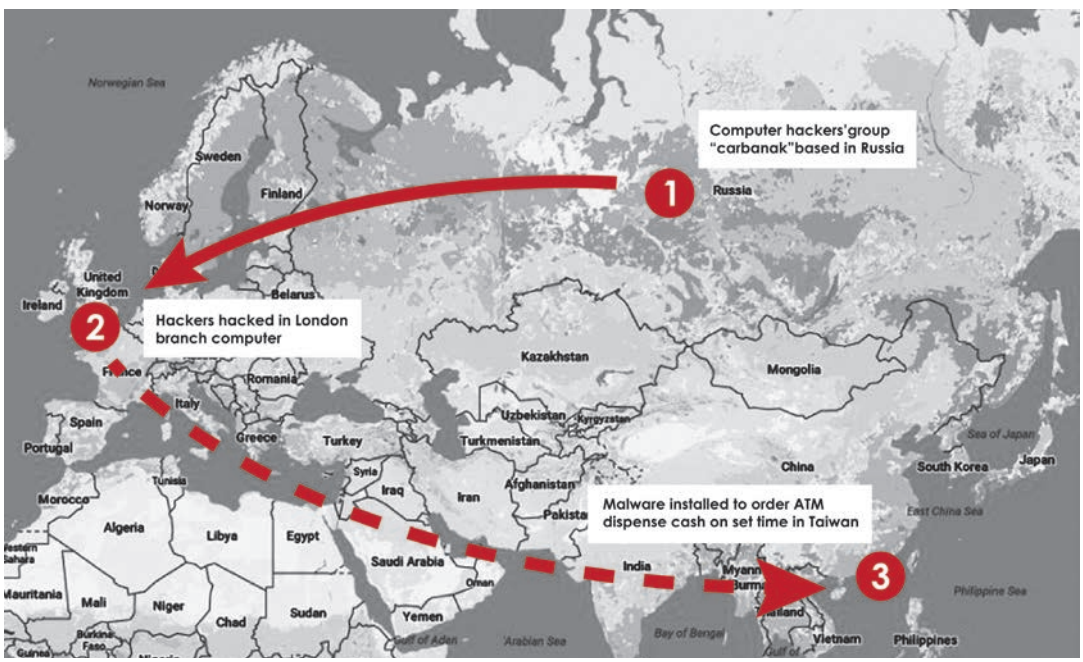


Photo from ediotrs

At 8:00 in the evening of July 10th, 2016, two Russians, Manukian Gaik and Adiian Kamo, came to the GuTing Branch of The First Commercial Bank to withdraw cash from an ATM. They arrived alone by taxi, and only one man got out of the car, wearing a mask and a fisherman's hat. However, when the man ran into a couple at the ATM, he rushed out of the bank with the cash still in the machine. The couple reported the suspicious incident to the police, who then informed the bank clerk about the scheme. No one had a clue yet what had happened at the ATM.

[1] 民國 105 年 9 月 9 日，臺北地檢署以 105 年度偵字第 15086 號等案件，認被告 Peregudovs Andrejs 等 3 人 (另 14 名共犯通緝中) 利用電腦系統漏洞入侵銀行電腦內部網路而盜領 ATM 內現金共新臺幣 8327 萬 7600 元，犯刑法入侵電腦、破壞電磁紀錄、干擾電腦、違法從自動付款設備取得財物等罪。臺北地方法院以 105 年度訴字第 426 號案件判決被告三人各有期徒刑五年，目前上訴台灣高等法院中。本件起訴檢察官李彥霖，公訴檢察官黃筵銘。

ATM
Photo from July 13, 2016 CNA

At 2:00 in the morning of July 11th, 2016, two Russians, Berezovskiy Sergey and Berkman Vladiair, showed up at the Nanmen Branch of the First Commercial Bank to withdraw cash from an ATM. They were acting sneaky, which caught the attention of Mr. Tsai, a passerby. Mr. Tsai reached out and tried to grab Berezovskiy's arm and, in the tussle that followed, Berezovskiy dropped his credit card. He was unaware of the loss when he left the scene in a hurry. Mr. Tsai, though, failing to catch them, memorized their car number and called the police about the incident.

When the police arrived at the scene soon after, the two Russians had gone … but the authorities now had one of the suspect's credit cards, which was fortuitously issued in Berezovskiy's own name rather than an alias. Staring from this initial clue, the members of a heretofore unknown crime group gradually floated to the surface.

The **Investigation**

With the credit card information, car license number, and videotapes from the ATMs, the police began to trace this crime group. Police first used Berezovskiy' s ID to examine his customs and immigration file and linked him with 22 potential coconspirators, 19 of whom were no longer in country.

All 22 of these individuals had flown to Taiwan from different countries between July 6th to July 11th, 2016 and then broken into 9 groups. A few of these stayed in hotels and went regularly by car or foot to withdraw cash from ATMs of First Commercial Bank branches in Taichung City and Taipei City. They departed Taiwan immediately after finishing their ATM withdrawals and were in Taiwan for just two to six days. The withdrawn cash was left with accomplices still in Taiwan, who withdrew more cash or laundered the money outside of Taiwan.

On July 11th, the First Commercial Bank reported illegal withdrawal activity to the police. Up to this point, NT$6.8 million had been withdrawn. However, by the end of this long-running heist, withdrawals would reach a total of NT$83,277,600 (US$2.78 million).

Peregudovs
Andrejs

Ursu
Vitalie

Niklae
Penkov

Arsenii
Alexandru

Colibaba
Mihail

22

DEFENDANTS

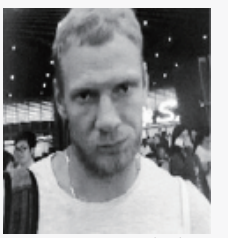
Police assigned thousands of staff to review over 1,500 street monitors, 212 immigration data records, the guest records of 500 hotels, the 28 websites and Facebook accounts of the suspects, and 23 taxis and 15 buses used by suspects. Police also took 53 finger prints and 45 DNA samples from ATMs, hotels, and rental cars suspected of being used in the scams. Berkman Vladiair and Peregudovs Andrejs were singled out and identified as the prime suspects.

Viewing the ATM videotapes, police discovered that cell phones were used to remotely control the ATMs, allowing the thieves to make withdrawals without ever touching the machines. Police thus presumed that the First Commercial Bank's computer system had been compromised with malware.

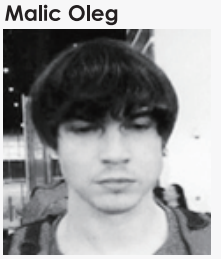
Police then went to the bank's headquarters and its targeted branches as well as the ATM maintenance company for further investigation. The targeted ATMs, all Type ProCash 1500 models manufactured by Wincor Nixdorf, were found to be infected by two malware programs, "cngdisp_new.exe" and "cngdisp.exe", which would direct the ATM to automatically deliver cash when activated.

Malic Oleg

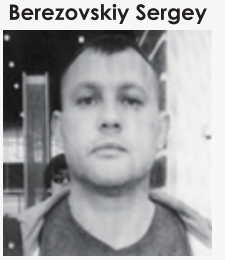
Berezovskiy Sergey



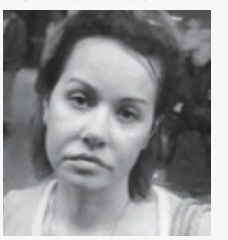
Berkman Vladimir



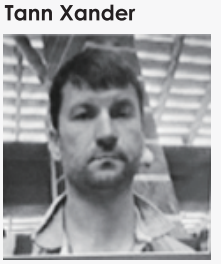
Tann Xander



Kharechko Victor



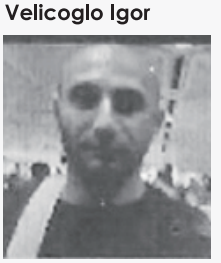
Sarkisova Oxana



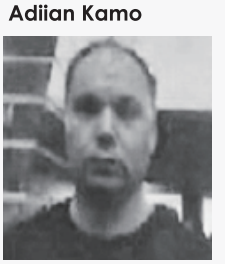
Velicoglo Igor

Adiian Kamo

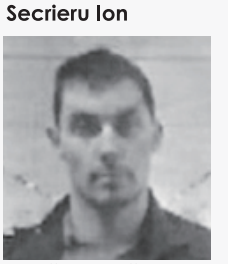
Secrieru Ion



Manukian Gaik



Lvovskiy Alexander



Babii Evgenii

The forensic office traced every change to the computer system of the affected ATMs and of the First Commercial Bank and found that someone had on May 31st, 2016 made changes via the bank's intranet and the Internet through the First Commercial Bank's London Branch. The individual or individuals then hacked into the host at 10:36pm that night and then later on produced computer programs that hijacked the ATMs to give out data, deliver cash, and delete information on the illicit transactions in both the ATM computer and remote-controlled computer. The crime group then hacked into the bank's computer to prepare for ATM withdrawals. In addition, an unidentified man had tested the proceedings on June 30th at the Nanmen Branch of the First Commercial Bank. After confirming that the procedures worked as planned, this man reported to the group by cellphone and disappeared from the story.

Once everything was set, the crime group sent out pickup runs to Taiwan in separate groups to avoid arousing suspicion. Each group acted independently in the early morning of July 10th, 2016 in Taichung City and Taipei City and dropped the withdrawn cash in the hotels for their relay accomplices to handle the next phase. These first-phase criminals then left Taiwan for various countries.

The remaining criminals in the group, who now had piles of cash in hand, needed to launder the money out of Taiwan.

Police found on Colibaba Mihail's mobile phone Google search queries on "how much money can be wired out of Taiwan", "how to buy bitcoin in Taiwan", and "the currency in Taiwan" as well as a WeChat message in Roma that read "The person we arranged has fucked up. Now I got another one who has 2 million US dollars in cash in Taipei. Do you have any way that I can get the money into Russia?" All of these supported the case that the group intended to launder money using bitcoin. However, the case was broken before they had acted on their poorly conceived laundering schemes.

London Branch of the First Commercial Bank

Mr. Babii Evgenii
travelled with 2 luggages to Taipei Main Station

The person who intended to withdraw cash from ATM

Photos from

Apple Daily - lower right
Liberty Times - upper right
First Commercial Bank - left

2016

While tracing the trail of the pickups, the police found out that one of the pickup men, Babii Evgenii, had arrived with two suitcases at Taipei Main Station on July 12th, 2016 and had left them in long-term lockers at the station. He returned with another suitcase and left it in a locker as well on July 13th. He left Taiwan immediately afterward. The police then waited for his coconspirators to make the collection from these three lockers. At 4:50 in the afternoon of July 16th, Colibaba Mihail and Pencov Nicolae arrived at Taipei Main Station, took the suitcases from the lockers, and then checked into Victoria Hotel.

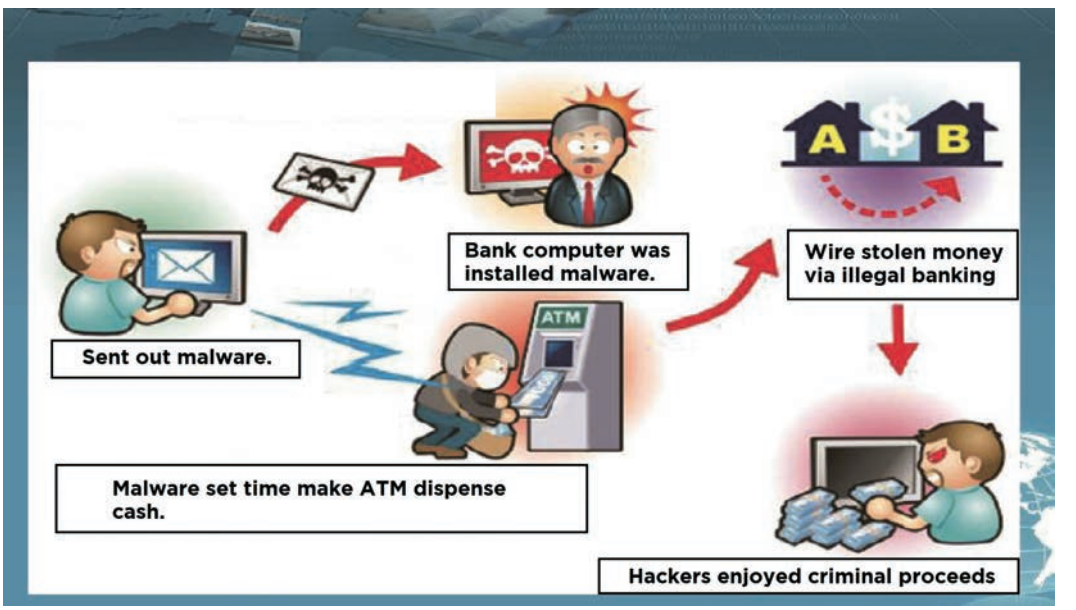
Peregudovs Andrejs came to Taiwan on July 12th and collected a suitcase filled with cash left by another pickup man at the Hyatt Hotel in Taipei and transported it to a short-term rental apartment in the city. Andrejs then rearranged the cash into two different bags and hid them in the bushes in NeiHu District near a mountain-hiking trail on July 13th. Andrejs sent out the GPS coordinates of the two bags to other crime group members and took off to Yilan County to lay low. The crime group arranged for Freijs Renars to purchase a new mobile and hide it in a tetrapod at WuShi Harbor for Andrejs to use. By this time, however, the bank and police were aware of the crime and those conspirators who were still in Taiwan were working out how to effect an escape from Taiwan.

THE ARREST

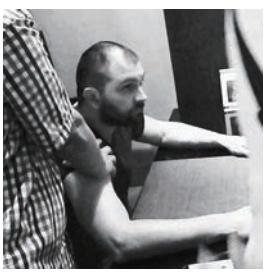
An off-duty policeman made a chance spotting of Andrejs dining at a restaurant on July 17th in SuAo Town of Yilan County. He recognized the man as being wanted by the police in the First Commercial Bank case and called in the arrest. Meanwhile, the police in Taipei City were monitoring Colibaba Mihail and Pencov Nicolae at Victoria Hotel. When the police learned that Andrejs had been caught in Yilan County, they figured that the time was ripe to arrest his coconspirators at Victoria Hotel. All told, the police uncovered NT$60.240 million (US$2 million) in three suitcases in room 715 of Victoria Hotel.

The police took Andrejs to NeiHu to pick up the cash that he had left on July 20th, but found only one of the bags and NT$12.639 million in cash. The police then made a public call on the news for assistance in locating the second bag. That same evening, the man who had found the bag reported that he had turned it into the police. The bag contained NT$4.542 million (US$151,000) in cash.

The police had thus recovered NT$77,481,100 (US$2.58 million), which was just NT$5.796 million (US$193,000) short of the total amount stolen from First Commercial Bank.



The hacking footsteps



Mr. Colibaba Mihail and Mr. Pencov Nicolae
was arrest in Victoria Hotel

Mr. Peregudovs Andrejs was arrest in Yilan County

Photos from

United Daily News - left
Apple Daily - right

Minister Chu Tai-San of the Ministry of Justice praised the whistle blower Mr. Tsai of this case.

THE **COLLABORATION**

When the case first broke, Prosecutors Office called a meeting on July 15th, 2016 that created a special task force comprising the 9th Investigation Corp. and Forensic Examination Division of Criminal Investigation Bureau, Criminal Investigation Division of Taipei City Police Department, New Taipei Police Department, Taichung City Police Department, Daan Police Station, ZhongShan Police Station, Shinyi Police Station, the Computer Science Division, and New Taipei City Department of the Investigation Bureau. The prosecutor instructed all representatives to exert their best efforts to collect and sort out the evidence. This effort combined with not a little luck helped solve the case in a very short period of time and recover most of the stolen money.

This case was the first time that this type of bank hacker group had been thwarted and arrested. Cybercrime groups had utilized similar methods to withdraw cash from ATMs all over the world and had never been caught and prosecuted – until now.

A cybercrime group had previously installed malware to hack bank computers and steal billions of Russian rubles in Russia. In Romania, a cybercrime group had used the same approach to steal €2 billion from ATMs. Also, around the same time as the hit in Taiwan, the Government Savings Bank in Thailand was hacked and lost 13 million Thai baht. The Thailand Government even sent agents to Taiwan to study Taiwan's experience with this case.

Photos from editors

THE BITCOIN CASE

This was not the first money laundering case in Taiwan to involve bitcoin.

In October 2015, A Hong Kong businessman was kidnapped in Taiwan by a group of Taiwanese and asked for ransom from his family in Hong Kong. These outlaws ordered the family member in Hong Kong to pay the ransom in bitcoin. Fortunately, before the ransom had been paid, police rescued the victim and the transaction never went through.

Why do crime groups favor bitcoin as a way of collecting criminal proceeds? To answer that question, we should learn more about Bitcoin.

Photos from Wiki

BITCOIN”

Bitcoin is not a currency recognized by any jurisdiction or bank for deposit or withdrawal. It is a cryptocurrency and a payment system invented by an anonymous programmer (or programmers) under the name Satoshi Nakamoto. It was introduced on October 30th, 2008 via a cryptography mailing list, and released as open-source software in 2009. The system is peer-to-peer, and transactions take place between users directly, without any intermediary. The transactions are verified by network nodes and recorded in a publicly distributed ledger called the blockchain, which uses bitcoin as its unit.

Bitcoin is now available in many countries, including Taiwan, where anyone may purchase bitcoins through automatic vending machines in convenience stores such as Family Mart. Anyone can convert national currency to bitcoin using just an email address and a cell phone number. Although unrecognized by any jurisdiction or bank, bitcoin has emerged as a strong underground currency.

Cooperation with Visa International has led to the inauguration of bitcoin debit cards, with cardholders required to pay a management fee of just €1/month to withdraw cash in Europe. Outside of Europe, cardholders pay €2.75/month plus a 3% fee for each withdrawal. This debit card is valid at ATMs worldwide as long as there is money in the account.

In addition, bitcoin uses an offline purse to store money, which means the system stores money in a place that is not connected to the Internet. A bitcoin user may create new transactions in an online computer, store the information to an USB, and then use that USB to log into the offline purse to sign and verify the transaction – a multistep method that significantly improves the safety of the transaction and the money.

In light of these features, bitcoin has become a tool preferred by crime groups worldwide to transfer illegal proceeds.

THE **INDICTMENT**

On September 9th, 2016, Prosecutor Lee YenLin（李 彥 霖）indicted the three defendants to court and issued want warrants for the other 19 defendants. Considering the malice and magnitude of their wrongdoings, Prosecutor Lee asked the court to sentence the defendants to 12 years' incarceration each. This was the first case established anywhere in the world against the bank hacker group "Carbanak".

Photo from CTV

THE **TRIAL**

In the courtroom, the three defendants admitted to participating in the disposition of stolen cash but denied being involved in the computer crimes. Peregudovs Andrejs even stated that the only reason he came to Taiwan to look after the stolen cash was because he owed money to a gang and was under threat from them. During his stay in Taiwan, Andrejs said that the gang had kidnapped his wife and children to force him to obey their orders. However, judging from the transcripts of the conversations between these three defendants and the other fraud group members, the defendants were not only following orders from the other group members, but also actively discussing ways to launder their hot money. Furthermore, based on Andrejs' Skype records, he and his wife had communicated frequently, and his wife's only complaint was that the gang was trying to brainwash her. The evidence thus worked against Andrejs' argument.

In the end, the three-judge tribunal also found the three defendants in violation of computer evasion laws and sentenced them all to five years' incarceration. While expressing their regret at the short sentences and their willingness to impose longer incarceration times, the judges noted that the current maximum sentence for the crimes at hand was only five years. The judges further expressed their hope that this case might inspire national legislators to amend the relevant laws in order to allow for harsher sentencing.

Photo from January 25, 2017 FTV

The prosecutor, on receiving the sentence, appealed immediately to the Taiwan High Court, accusing the district court judges of erroneously considering all of wrongdoings as one count instead of the 12 counts asked for by the prosecutor. The defendants appealed the tribunal's decision to the Taiwan High Court as well.

On May 18th, 2017, the Taiwan High Court overruled the district court's sentence and sentenced Peregudovs Andrejs to 4 years and 10 months, Colibaba Mihail to 4 years and 8 months, and Pencov Nicolae to 4 years and 6 months.

QUOTE FROM PROSECUTOR

Lee Yen-Lin

I must say that this case could be closed within a week were credited to the hardworking of the team members from the Investigation Bureau of the Ministry of Justice, the Criminal Investigation Bureau, and Taipei City Police Department. When I was assigned with this case, my first instinct was to retrieve criminals and lost money.

However, since all defendants were foreigners and we didn't have basic information regarding them, we actually receive assistance from Interpol and Egmont.

In addition, we were lucky to be able to trace down the pickups who were remaining in Taiwan to launder the money. As a result, we arrested three defendants and retrieved 93.4% of stolen money.

This was the first case established in the world to fight against a fraud group like this. With the achievement in this case, we were invited by other international criminal justice organizations to report on the case; and hopefully it would also increase the opportunity for us for further mutual legal assistance with other countries

National Performing Arts Center - National Theater & Concert Hall , Taipei
Photo from Tourism Bureau