11

Cyber Crime, Bitcoin, And Money Laundering

Crime Group v. **Zealous Citizens**

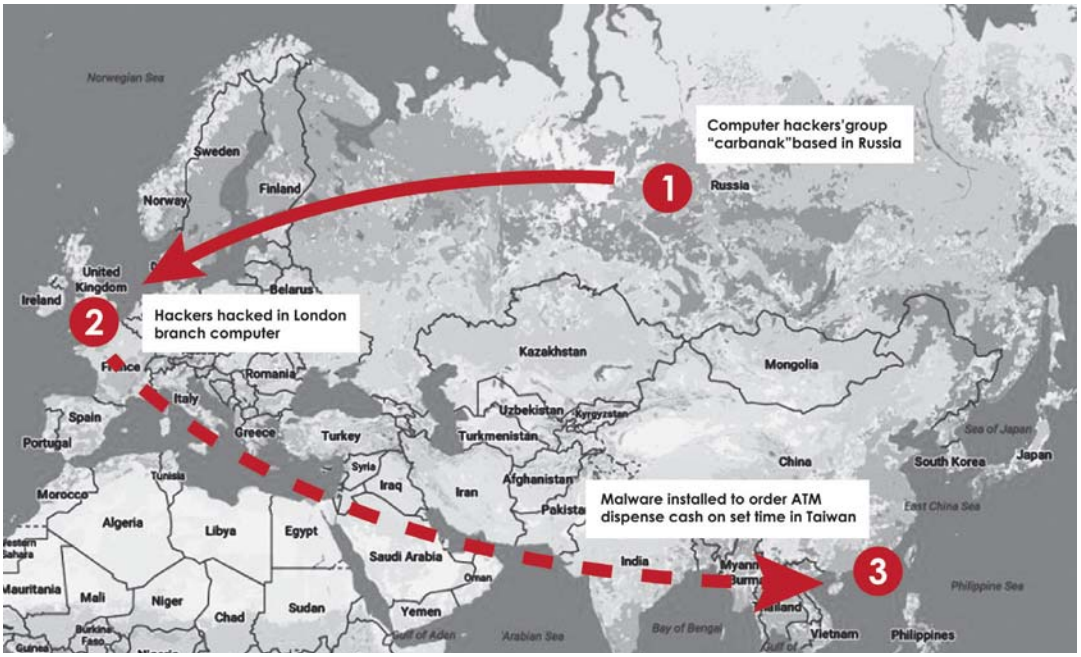


Photo from ediotrs

At 8 o'clock on the evening of July 10, 2016, two Russians, Manukian Gaik and Adiian Kamo, came to GuTing Branch of The First Commercial Bank to withdraw cash from an ATM. They came alone by taxi. Only one man got off wearing a mask and a fisherman's hat. However, when the man ran into a couple at the ATM, he rushed out with the cash still in the machine. The couple reported the suspicious situation to the police.

Police then informed the bank clerk to the scheme and counted the cash for 60 thousand dollars. No clue yet for what had happened to the ATM.

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 (277 萬 5920 美元)，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。本件偵查檢察官李彥霖，公訴檢察官黃筵銘。

ATM
Photo from July 13, 2016 CNA

At 2 o'clock on the early morning of July 11, 2016, two Russians, Berezovskiy Sergey and Berkman Vladiair, showed up at Nanmen Branch of the First Commercial Bank to withdraw cash from an ATM. They were sneaky and caught the attention of Mr. Tsai, a passer-by. Mr. Tsai reached out and tried to grab Berezovskiy's arm. In the pulling and dragging, Berezovskiy dropped his credit card on the ground. He was unaware of the loss and left soon.

Mr. Tsai, though failing to catch them, memorized their car number and called the police immediately. When the Police rushed to the scheme, the two Russians had gone but left the key evidence, the credit card. Through the credit card, Police found out Berezovskiy used his real name to apply for that card. Staring from here, the compliances of the crime group were gradually floated to the surface.

The **Investigation**

With the precious credit card information, car number, and videotapes from ATMs, the police started to trace the crime group. Police first used Berezovskiy's ID to look into his immigration information. Then to sort out other accomplices who either traveled with him or stayed with him. Police later realized that there were 22 defendants altogether that entered Taiwan, out of which 19 had left.

All 22 of them flew into Taiwan from different countries starting from July 6 to July 11, 2016, and broke up to form 9 groups. One or two of them stayed in hotels and migrated by car or by foot to withdraw cash from ATM of the First Commercial Bank located in Taichung City and Taipei City. After finishing targeted ATM withdrawal, they left Taiwan immediately. They stayed only for two to six days. After they withdrew cash, they left the cash to accomplices that relayed to withdraw cash or to launder money outside of Taiwan.

On July 11, the First Commercial Bank reported illegal withdrawal to the police. Up until then, the cash withdrawn was 6.8 million NT dollars. The total withdrawn cash in the end was 83 million 277 thousand and 6 hundred NT dollars (i.e. 2.78 million USD) .

Peregudovs
Andrejs

Ursu
Vitalie

Niklae
Penkov

Arsenii
Alexandru

Colibaba
Mihail

22

DEFENDANTS

Police invested thousands of manpower to review over 1500 street monitors, 212 immigration data, 500 hotels, 28 websites and Facebook of suspects, 23 taxi and 15 buses used by suspects, and sorted out 22 defendants. Police also got 53 finger prints and 45 DNA samples from targeted ATM, hotels and rental cars used by defendants. Among which, Mr. Berkman Vladiair and Mr. Peregudovs Andrejs were singled out and identified.

Judging from the videotapes of ATM, Police found out that the person who intended to withdraw cash from ATM didn't even need to touch it. With a cell phone, ATM would deliver cash automatically.

Police therefore presumed that the computer system of the First Commercial Bank may have been installed with malware.

Police then went to the Bank's headquarter, victim branches, and maintenance company for further investigation. They figured out that the hacked ATM was a Type ProCash 1500 produced by Wincor Nixdorf Company. There were two malware found, "cngdisp_new.exe" and "cngdisp.exe". Upon reactivating the malware, the ATM would automatically deliver cash.

Malic Oleg

Berezovskiy Sergey

Berkman Vladimir

Tann Xander

Kharechko Victor

Sarkisova Oxana

Velicoglo Igor

Adiian Kamo

Secrieru Ion

Manukian Gaik

Lvovskiy Alexander

Babii Evgenii

To authenticate the existence of malware, the forensic office traced every single change to the computer system of the ATM and the First Commercial Bank. Forensic Officers concluded that on May 31, 2016, this crime group found that there was a phone recording host in London Branch of the First Commercial Bank connected to the intranet and internet. They then hacked into the host at 10:36 pm that night.

Later they produced computer programs to read information in ATM, to order ATM to deliver cash, and to delete everything in ATM computer and remote-controlled computer. The crime group then hacked into bank's computer to prepare for ATM withdrawal. In addition, an unidentified man had tested the proceeding on June 30 in Nanmen Branch of the First Commercial Bank. After he confirmed the proceeding would be successful, this man reported to the group by cellphone and disappeared.

Once everything was set and prepared, the crime group sent out pick-ups to Taiwan in separate groups to avoid suspicion.

They unilaterally took actions on the early morning of July 10, 2016 in Taichung City and Taipei City. Those pick-ups then dropped the cash in the hotels and left the cash for the relayed accomplices to take over. Pick-ups then left Taiwan for different countries. Those who left with cash now needed to launder money out of Taiwan.

In Defendant Colibaba Mihail's mobile, the police found google search results relating to "how much money can be wired out of Taiwan", "how to buy bitcoin in Taiwan", and "the currency in Taiwan", and WeChat message with Roma, "The person we arranged had fucked up. Now I got another one who had 2 million US dollars in cash in Taipei. Do you have any way that I can get the money in Russia?" All these above points confirmed that the crime group intended to launder money by bitcoin. Only before they ever found a way to launder the money, all defendants were caught.

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 pick-ups, the police found out that one pick-up, Mr. Babii Evgenii, had travelled with two luggages to Taipei Main Station on July 12, 2016. He left two luggages in the Large Lockers. He came back again with another luggage and left it in the large locker on July 13, 2016. Barbii left Taiwan thereafter.

The police then waited for co-defendants to pick up these luggages. At 16:50 in the afternoon of July 16, 2016, Mr. Colibaba Mihail and Mr. Pencov Nicolae came to Taipei Main Station to pick up those luggages in the large lockers. They then checked into Victoria Hotel.

Peregudovs Andrejs came in Taiwan on July 12 and picked up luggage with cash left by other pick-ups in Hyatt Hotel and transported it to day-rent apartments on Taipei's MingShen East road. Andrejs then rearranged these cash into two different bags and hid them in the bushes in NeiHu District near a mountain-hiking trail on July 13.

Andrejs sent out GPS information of these two bags to other members of the crime group and took off to Yilan County to hide. The Crime Group arranged for Freijs Renars to purchase a new mobile and hide it in tetrapod of WuShi Harbor for Andrejs's use. At this time, the crime had out broke and defendants present in Taiwan were waiting to get away.

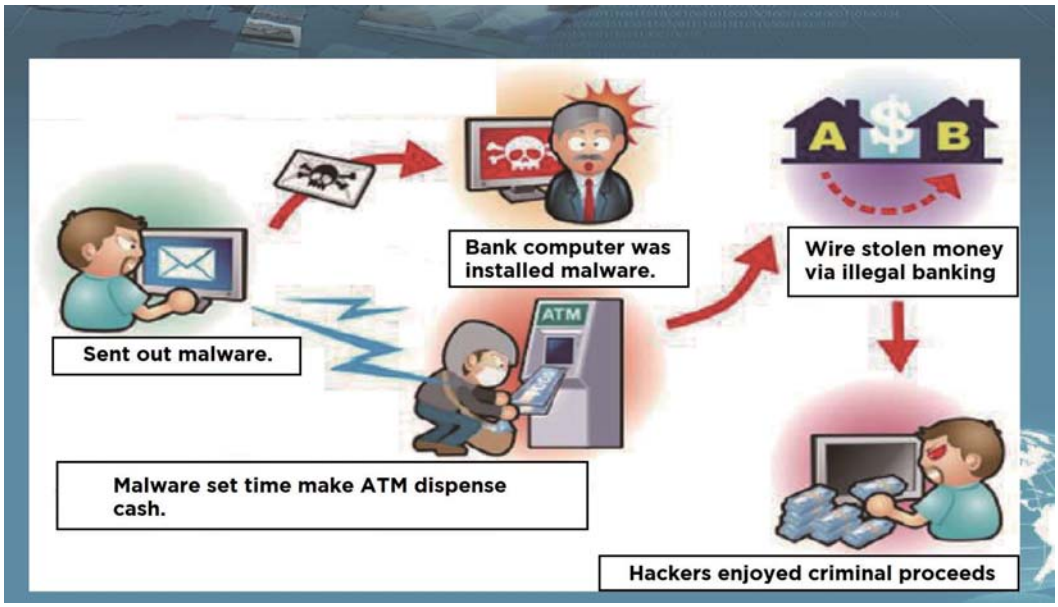
THE ARREST

At 5:10 pm on July 17, 2016, while Andrejs was dinning in a restaurant in SuAo Town of Yilan County, he was spotted by a policeman who happened to be on his vacation. The policeman recognized the face that was wanted by police for the First Commercial Bank's case.

He immediately called local police to arrest Andrejs. Meanwhile, the police in Taipei City were monitoring Colibaba Mihail and Pencov Nicolae in Victoria Hotel. When the police learned that Andrejs was caught in Yilan County, they figured that it was the ripe time to arrest the co-defendants in Victoria Hotel. In room 715 of Victoria Hotel, the police discovered three luggages with cash adding up to 60 million and 240 thousand NT dollars (i.e. 200 thousand USD) .

The police took Andrejs to NeiHu to pick up the cash he left on July 20 but only found one with 12 million and 639 thousand NT dollars. The police then made a public call on the news to whoever found the bag. In the evening of the same day, a civilian took the bag he found behind the bushes to the police. Total cash in this bag was 4 million 542 thousand and 2 hundred NT dollars. (i.e. 151 thousand USD)

As a result, the police recovered 77 million 481 thousand and 1 hundred NT dollars (i.e. 2.58 million USD) crime proceeds. Compared to what had been withdrawn, the First Commercial Bank only lost 5 million 796 thousand and 5 hundred NT dollars (i.e. 193 million USD) .



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 **OF INVESTMENT TEAM**

When the case broke out, Prosecutors Office called upon a special Task Force meeting on July 15, 2016. In this meeting, investigation manpower gathered to work together, including 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. Under Prosecutor's instructions, all sectors exercised their best functions to collect and sort out evidences.

Adding a little bit of luck, the case was solved in a very short period of time and recovered proceeds before they were laundered. This is the first time this bank hacker group was ever cracked and arrested in the world. According to estimation, the cybercrime groups utilized the same way to withdraw cash from ATMs all over the world. No one was ever caught in any country.

In Russia, the cybercrime group installed malware to hack bank computers and stole billions of Russian Ruble. In Romania, the cybercrime group used the same way to stole cash from ATMs up to 2000 thousand Euros. Back in Asia, in 2016 July, the Government Savings Bank in Thailand was hacked and lost 13million Thai Baht. Thailand Government even sent agents to Taiwan to study the case.

Photos from editors

THE BITCOIN CASE

As a matter of fact, this was not the first case involving bitcoin money laundering in Taiwan.

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 ransom by bitcoin. Before the ransom was paid, Police had rescued the victim. Therefore, the family member of the victim didn't have the chance to pay ransom by bitcoin.

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

Photos from Wiki

BITCOIN”

Bitcoin is not a currency recognized by any jurisdiction or bank that can be deposited or withdrawn, and its calculation unit was invented by a computer.It is a cryptocurrency and a payment system invented by unanimous programmer(s) under the name of Satoshi Nakamoto. It was introduced on October 30, 2008 to a cryptography mailing list, and released as an 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 public distributed ledger called the blockchain, which uses bitcoin as its unit. Only several years since it was created, Bitcoin is now available in many countries, including Taiwan. People can purchase bitcoin through an automatic vending machine in the convenience store, such as Family Mart. Anyone can convert national currency to bitcoin with an email address and a cell phone number.

Though unrecognized by any jurisdiction or bank, bitcoin has become a strong underground currency.Now through cooperating with Visa International, bitcoin debit cards are available. A card holder only has to pay 1 euro per month for management fee to withdraw cash in Europe.

Outside of Europe, a card holder would have to pay 2.75 euro plus 3% fee for every withdrawal. This debit card is valid in any ATMs in the world as long as there is money in the account. In addition, bitcoin uses an off-line purse to store money, which means the system stores money in a place without connection to internet. A bitcoin user may create new transactions in an on-line computer, store the information into an USB, and then use that USB to log into the off-line purse to sign and verify the transaction.

In this way, the safety of the transaction and the money are highly elevated. Adding up all the features above, bitcoin has become a tool adored by crime groups all over the world to transfer illegal proceeds.

THE INDICTMENT

On September 9, 2016, Prosecutor Lee YenLin (李彥霖) indicted three defendants to court and issued want warrants for the other 19 defendants. Considering the malice and magnitude of their wrongdoings, Prosecutor asked the court to sentence defendants to 12 year's incarceration.

This is the first case established against the bank hacker group "Carbanak" in the world.

Photo from CTV

THE TRIAL

In the court room, three defendants admitted participating in disposition of stolen cash but denied being involved in computer crimes. Peregudovs Andrejs even stated that the reason he came to Taiwan to care for the stolen cash was because he owed money to a gang and under the gang's threat.

During his stay in Taiwan, the gang actually kidnapped his wife and kids as threat to force him obey the orders. However, judging from the transcripts of 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 discussing suitable money laundering methods. In addition, based on the skype records of Peregudovs Andrejs, he and his wife still communicated without difficulty and the only thing his wife complaint about was that the gang tried to brainwash her. Therefore, there was no evidence to prove Andrejs's argument.In the end, the three-judge tribunal sentenced the three defendants were in violation of computer evasion and to five years' incarceration.

Judge also expressed their regret in the judgment that they were willing to sentence a higher incarceration to the defendants but the maximum sentence of this crime was only five years. Although the sentencing of this case couldn't perfectly reflect the damage and magnitude of the crimes, this was the best the judges could do under the restriction of law.

Photo from January 25, 2017 FTV

The judges further stated that hopefully this case will inspire legislators to amend the related law to elevate the sentencing.

Prosecutor, on receiving the sentence, appealed right away to Taiwan High Court for the reason that the district court judges falsely considered all wrongdoings as one account but Prosecutor indicted for 12 accounts. Both defendants and prosecutor appealed to Taiwan High Court.

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

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