A Study on the First Commercial Bank ATM Heist Investigation in Taiwan

Chou, Tai-Wei

Introduction

Several cybercrimes occurred in Taiwan throughout 2016, such as the computer hacking of governmental intranet that led to the theft of confidential information, website attacks by distributed denial-of-service attack (DDoS), the crack of the public bicycle-sharing system, and the rampant ransomware. This phenomenon is not endemic in Taiwan but exists in other countries as well, which indicates that cybercrime has becoming a major type of crimes worldwide. Of all cybercrimes, the First Commercial Bank (hereafter referred to as FCB) ATM Heist was thrust into the international spotlight because the suspects were arrested and almost all the stolen cash was recovered. Besides, the malware planted into the ATMs was found in the next day after the crime was committed. Moreover, the modus operandi adopted by the hackers were successfully cracked in an unprecedently short period of time.

1. Case Profile

On 11 July 2016, the FCB reported the incident of abnormal withdrawal to Taiwan’s Financial Supervisory Commission (FSC) as follows: more than NT$83.27 million (approximately US$2.63
million) was withdrawn in cash by unknown subjects from 41 ATMs at 22 FCB branches in Taiwan.¹

The evidence collected suggests that this crime was committed by a foreign criminal group consisting of 22 suspects from 8 countries.² The criminal syndicate infiltrated FCB’s intranet from one of the bank’s foreign branch and withdrew the money in cash by remotely taking control over its server. On 17 July 2016, 3 bagmen of this criminal syndicate, namely Peregudovs Andrejs (Latvia), Pencov Nicolae (Moldova) and Colibaba Mihail (Romania), were apprehended by the police in Taiwan, and the prosecution authorities also issued a warrant for the arrest of the other 19 suspects. By virtue of multiple sources of information such as the informants’ reports, the suspects’ call detail records, the confessions by the arrested suspects, and the monitor video clips, a total of NT$77.48 million (approximately US$2.44 million) was recovered. On 13 September 2016, the Taipei District Prosecutor’s Office charged the three arrested suspects with offences of fraudulence and money-laundering as well as offences against the computer security under Taiwan’s Criminal Code, requesting the court to sentence each of them to a 12-year term of imprisonment.³ The court of first instance finally sentenced each of them to a 5-year term of imprisonment and a fine of NT$600,000.

2. Crime Reconstruction and the Modus Operandi

¹ See Annex II: “A Brief of ‘First Commercial Bank ATM Heist’ Investigated by the MJIB,” provided by the Information & Communication Security Division of the MJIB.
² See Annex I: the copy of the excerpt of indictment by Taipei District Prosecutors Office. The 22 suspects come from 9 counties, including Australia, Belarus, Estonia, France, Latvia, Moldova, Romania, and Russia.
³ See Annex V, the English newspaper clippings.
(a) Crime Reconstruction

Since May 2016, the criminal syndicate had gradually taken control over FCB’s ATM network by infiltrating and planting malware into the bank’s intranet and ATMs (Type PC1500XE), which allowed the criminal syndicate to change FCB’s financial records and withdraw money from specific ATMs in Taiwan.

On 10 and 11 July 2016, Berezovskiy Sergey and the other 11 bagmen approached those selected ATMs. They contacted the hackers overseas who managed to force the ATMs to dispense cash to them. Then they handed the stolen money to Pencov Nicolae, Colibaba Mihail, Peregudovs Andrejs and the other 4 bagmen who were responsible for hiding and transferring the filthy lucre.

(b) The Modus Operandi of the Criminal Syndicate

The digital forensic laboratory of the Investigation Bureau, Ministry of Justice (MJIB) managed to recover the digital evidence from the wiped ATM hard drives seized by the police, based on which the instruments of crime and the log-in information were identified and the traces of pertinent program execution were found. The FCB London branch’s firewall log also helped reveal the traces of the hackers’ infiltration route into FCB’s intranet. The criminal syndicate’s modus operandi was thus

---

4 See Annex III, the *corpus delicti* in the referral paper provided by the Information & Communication Security Division of the MJIB, p.1.
5 This type of ATM is manufactured by Wincor Nixdorf International.
6 See Annex III, the *corpus delicti* in the referral paper provided by the Information & Communication Security Division of the MJIB, pp. 2-5.
verified. By virtue of all the pieces of evidence gathered and analyzed, the MJIB confirmed that the
foreign criminal syndicate infiltrated FCB’s intranet, stole the money from selected FCB ATMs by
planting homemade malware, and tried to hide and transfer the illicit money. Their modus operandi
proceeded as follows:

Step 1: Hacking into the call recording server of the FCB London branch

Checking the outbound connection attempts recorded in the FCB London branch’s firewall log, the MJIB
found that the call recording server at that branch had abnormal connections with an
unknown IP address in Switzerland (IP: 95.183.53.210) at 22:36:15 on 31 May 2016.

Step 2: Infiltrating FCB’s intranet and remotely controlling its server

After the criminal syndicate managed to infiltrate the call recording server of the FCB London
branch on 31 May 2016, it firstly cracked the administrator’s account and password, and then accessed
FCB’s intranet and the PCs used by the bank’s employees.

On 11 June 2016, the criminal syndicate took the call recording server of the FCB London branch
as a relay server, and then infiltrated the bank’s NCR server (produced by the NCR Systems Taiwan
Ltd. and used for updating FCB’s NCR ATM programs). On 17 June 2016, the syndicate logged in the
FCB intranet with the administrator’s account and collected the information it needed.
Step 3: Distributing package files, collecting information of the ATMs, and deploying malware

After taking control over the AP server, the criminal syndicate successively distributed the utility programs disguised as the package files (with the filename extension “.DMS”) for FCB’s ATM updating programs. Then the syndicate used the AP server with the administrator’s account and password to distribute the abnormal package files to some of the bank’s ATMs. On 4 July 2016, the syndicate began to intensively distribute the package files to FCB’s ATMs in order to crack the Telnet server. It not only developed, distributed and executed programs such as the abovementioned abnormal package files to gather the information about FCB’s ATMs, but also deployed cash-dispensing programs (cnginfo.exe, cngdisp.ex, and cngdisp_new.exea) and programs for destroying the evidence (cleanup.bat and sdelete.exe) in the NCR server that operates FTP service, allowing its bagmen to download the programs and withdraw the money from the selected ATMs.

Step 4: Perpetrating the crime

From 9 to 11 July 2016, Berezovskiy Sergey and the other 11 bagmen of the criminal syndicate approached the selected FCB ATMs in Taiwan, contacting the members who remotely controlled the call recording server of the FCB London branch to connect and control the cracked ATMs via the Telnet server. Then the bagmen downloaded and executed the programs such as cnginfo.exe, and cngdisp.exe pre-installed in the NCR server through the FTP service, making those ATMs dispense
cash to them. After the ATMs finished dispensing cash, the bagmen executed the program cleanup.bat (containing Sdelete.exe, a Microsoft software used for erasing data from hard drives) 32 times with the instruction “Sdelete – p 32,” which made it extremely difficult for the MJIB to recover the erased records with available forensic tools. The 12 bagmen then took and hid the illicit money.

Step 5: Destroying the evidence

After the criminal syndicate got the illicit money from all the selected FCB ATMs on 12 July 2016, it cracked FCB’s ATM distribution system (AP server) again and distributed 5 abnormal package files to those ATMs, thereby further destroying all the scraps of evidence pertinent to the crime.

3. The Need for International Cooperation

Examining the FCB London branch’s firewall log, the MJIB found that the call recording server at the branch had abnormal connections with an unknown IP address in Switzerland (IP: 95.183.53.210) at 22:36:15 on 31 May 2016. However, Taiwan is not a member of the Interpol, and has no official relationship and mutual legal assistance agreement with Switzerland, which prevented the MJIB from accessing the IP address and related information. It was with the cooperation from foreign law enforcement agencies such as the National Crime Agency in the United Kingdom and the Federal Bureau of Investigation in the United States that the MJIB was able to gather and trace the registration
and log-in information of the IP address as well as other forensic evidence. Such a practice stood as testimony to the important fact that international cooperation is of urgent necessity for combating transnational organized crime.
A Study on the FCB ATM Heist Investigation in Taiwan

Chou, Tai-Wei
Section Chief
Cyber Crime Section
Information and Communication Security Division,

Investigation Bureau, Ministry of Justice
outline

- Introduction
- Case Profile
- Crime Reconstruction and the Modus Operandi
- The Need for International Cooperation
Introduction

RANSOMWARE

APT ATTACK

DDOS

COMPUTER HACKING

INTRINSIC THREATS

IOT AND INFRASTRUCTURE
Case Profile

◆ On 11 July 2016, more than NT$83.27 million (approximately US$2.63 million) was withdrawn in cash by unknown subjects from 41 ATMs at 22 FCB branches in Taiwan.
Case Profile

◆ The evidence collected suggests that this crime was committed by a foreign criminal group consisting of 22 suspects from 8 countries.

◆ The criminal syndicate infiltrated FCB’s intranet from one of the bank’s foreign branch and withdrew the money in cash by remotely taking control over its server.
Case Profile

On 17 July 2016, 3 bagmen of this criminal syndicate were apprehended by the police in Taiwan, and the prosecution authorities also issued a warrant for the arrest of the other 19 suspects.
By virtue of multiple sources of information such as the informants’ reports, the suspects’ call detail records, the confessions by the arrested suspects, and the monitor video clips, a total of NT$77.48 million (approximately US$2.44 million) was recovered.
Case Profile

On 13 September 2016, the Taipei District Prosecutor’s Office charged the three arrested suspects with offences of fraudulence and money-laundering as well as offences against the computer security under Taiwan’s Criminal Code, requesting the court to sentence each of them to a 12-year term of imprisonment.
The court of first instance finally sentenced each of them to a 5-year term of imprisonment and a fine of NT$600,000.
Crime Reconstruction and the Modus Operandi

◆ Crime Reconstruction

◆ The Modus Operandi of the Criminal Syndicate
Crime Reconstruction

Since May 2016, the criminal syndicate had gradually taken control over FCB’s ATM network by infiltrating and planting malware into the bank’s intranet and ATMs (Type PC1500XE), which allowed the criminal syndicate to change FCB’s financial records and withdraw money from specific ATMs in Taiwan.
Crime Reconstruction

◆ On 10 and 11 July 2016, The bagmen approached those selected ATMs.

◆ They contacted the hackers overseas who managed to force the ATMs to dispense cash to them. Then they handed the stolen money to the other bagmen who were responsible for hiding and transferring the filthy lucre.
The Modus Operandi

◆The digital forensic laboratory of the MJIB managed to recover the digital evidence from the wiped ATM hard drives seized by the MJIB, based on which the instruments of crime and the log-in information were identified and the traces of pertinent program execution were found.
The Modus Operandi

◆ The FCB London branch’s firewall log also helped reveal the traces of the hackers’ infiltration route into FCB’s intranet.

◆ The criminal syndicate’s modus operandi was thus verified.
The Modus Operandi

By virtue of all the pieces of evidence gathered and analyzed, the MJIB confirmed that the foreign criminal syndicate infiltrated FCB’s intranet, stole the money from selected FCB ATMs by planting homemade malware, and tried to hide and transfer the illicit money.
An international crime ring

Internet

Firewall

Bank’s Network in London

Call Recording Server

Infect

http://www.mjib.gov.tw/
An international crime ring

Bank's Network in London

Schematic diagram

Bank's Intranet

Conquer
An international crime ring

Schematic diagram

Bank’s Network in London

Infect & Conquer

Bank’s Network in Taiwan
An international crime ring

Bank's Network in London

Firewall

CCTV in operation

ATM DMS admin's PC

Commands

Information Collection

Bank's Network in Taiwan

Offsite Targeted ATM

Information Collection

Onsite Targeted ATM

Bank's Network in London

Proxy

SSO

Server Farm

ATM DMS system

ATM NCR Server (FTP)

Commands

Commands
Schematic diagram

An international crime ring

Bank's Network in London

Server Farm

Firewall

IPS

IDS

Proxy

SSO

ATM DMS system

ATM NCR Server(FTP)

the Call Recording Server

ATM DMS admin's PC

Bank's Network in Taiwan

Execution

Offsite Targeted ATM

Spew out money

Onsite Targeted ATM

Spew out money

Spew out money

Spew out money
Schematic diagram

An international crime ring

Bank's Network in London

Evidence Destruction

Offsite Targeted ATM

Onsite Targeted ATM

Bank's Network in Taiwan

Server Farm

Firewall

CCTV in operation

ATM DMS

admin's PC

the Call Recording Server

Commands

IPS

IDS

Proxy

SSO

ATM DMS system

ATM NCR Server(FTP)

sDelete Files

sDelete Files

sDelete Files

IPS

IDS

Proxy

SSO

ATM DMS system

ATM NCR Server(FTP)

sDelete Files

sDelete Files

sDelete Files
The Need for International Cooperation

• Examining the FCB London branch’s firewall log, the MJIB found that the call recording server at the branch had abnormal connections with an unknown IP address in Switzerland (IP: 95.183.xx.xxx) at 22:36:15 on 31 May 2016.
The Need for International Cooperation

- However, Taiwan is not a member of the Interpol, and has no official relationship and mutual legal assistance agreement with Switzerland, which prevented the MJIB from accessing the IP address and related information.
The Need for International Cooperation

◆ It was with the cooperation from foreign law enforcement agencies that the MJIB was able to gather and trace the registration and log-in information of the IP address as well as other forensic evidence. Such a practice stood as testimony to the important fact that international cooperation is of urgent necessity for combating transnational organized crime.
Thank You
For Your Attention
pdoc1403@mjib.gov.tw