The world first indictment of bank hacker “Carbanak”

Prosecutor AnChen Chang
Taipei District Prosecutors’ Office

10th IAP Asia & Pacific Regional Conference, Busan, Korea
Movie or Life?

- Sep. 15, 1995, American Movie “Hackers” released

- 2010, Las Vegas, Black Hat computer security conference, Barnaby Jack demonstrated how to make 2 ATMs dispense cash on stage, like “jackpotting”
Bank Hacker Group “Anunak”

- 2014, Dutch security company Fox-IT and Russian security company Group-IB, discovered in 2012-2014, a hacker group “Anunak” based in Russia and the Ukraine stolen more than $15 million from Eastern European banks

- Anunak members send phishing emails to banking employees that appear to be from the Central Bank of the Russian Federation, but which actually contain malware designed to infect the employees' computers by exploiting recently-patched flaws in Microsoft Office

- They install more malware on the banks' ATMs

- This malware causes the ATMs to muddle up money denominations, meaning a criminal can go to an ATM, request 10100-rouble notes, and receive 105,000-rouble notes instead
Bank Hacker Group “Carbanak”

- 2014, Kaspersky Lab, under authorization of an Ukraine bank, investigated an incident that an ATM dispensed cashes without anyone around, like “jackpotting”
- 2015, Kaspersky Lab released an official report on the investigation and called the type of attack as “Carbanak”
- Carbanak is a type of hackers’ crime which attacks banks and financial institutes.
- Started in Eastern European
- Crime groups members spam from Chinese, Russians, Ukrainians, Latvians, Romanians, Estonians, Moldovans, to Australians.
- Victim banks over 100, worldwide
Carbanak worldwide attacks

- Sep. 2015, Center for Strategic and International Studies (CSIS) discovered mutant carbanak malware targeted banks in Western Europe and America.

- March 2016, Proofpoint computer security company reported evidences showing that carbanak turned to attack banks in the Middle East and the U.S.
Carbanak worldwide attacks

- April 8, June 15, Barcelona, Spain
- April 19, Madrid, Spain
- April 21, Alicante, Spain
- Aug. 22, Barcelona, Spain
- Dec. 5-7, Warszawa, Poland
- July 5-7, Dushanbe, Tajikistan
- Aug. 7-8, Minsk, Belarus
- Sep. 2-3, Romania
- July 9-11, Taiwan
- July 15-17, Baku, Azerbaijan
- July 15-17, Nice, France
- Oct. 1, Kyrgyz
- July-Aug., Bangkok, Thailand
Carbanak aimed at Taiwan

- 8 pm, July 10, 2016, 2 Russians, Manukian Gaik and Adiian Kamo, Guting Branch of the First Commercial Bank, Taipei City, get 0.11 million USD, ran into a couple, left 2000 USD cash at ATM.

- 2 am, July 11, 2016, 2 Russians, Berezovskiy Sergey, Berkman Vladiair, Nanmen Branch, Taipei City, get 62000 USD, ran into a passer-by Mr. Tsai, Berezovskiy dropped his credit card on spot, Mr. Tsai memorized taxi plate.

- 22 group members formed 9 groups and flew to Taiwan from Hong Kong, Turkey, Dubai, Philippine, Sydney, and Macau; stayed 1-5 days to withdrew cash from ATMs; 19 of them left for Hong Kong,
Investigation Team

Ministry of Justice, Investigation Bureau
Prosecutor Assistants
Criminal Investigation Bureau, National Police Agency
City Police Departments, National Police Agency

- confiscate bank ATM and main computer, computer
- Interpol assistance, bank internal information checks, immigration information
- City surveillance system screening, transportation screening
Investigation works

- Over **1000** polices dedicated in reviewing **1500** street monitors, **212** immigration data, **28** websites/facebook of suspects, **23** taxi+**15** buses used by suspects—sort out **22** defendants/**19** fled overseas, **3** under surveillance in Taiwan
- **53** fingerprints, **45** DNA samples collected from targeted ATM, hotels, and rental cars used by defendants.
- Search Bank headquarter, victim branches, ATM maintenance company
- **2** malwares found, “cngdisp_new.exe”, “cngdisp.exe”
  Hacked ATMs are Type ProCash 1500, produced by Wincor Nixdorf Company (Siemens, Germany)
The hacking trace
How 3 Defendants transported stolen cash

• Babii, pick-up, transported 3 luggage to lock in the large lockers of Taipei Main Station on July 12-13, 2016.

• Mihail and Nicolae picked up 3 luggage on July 16, 2016 and checked in Victoria Hotel.

• Andrejs picked up 1 luggage with cask left by other pick-ups in Hyatt Hotel in Taipei and transported it to day-rent apartment.

• Andrejs divided cash into 2 bags and hide them in the bushes near a hiking trail in NeiHu area of Taipei City.

• Andrejs sent out GPS info of these 2 bags to other crime members and headed to YiLan County to hide.
The Arrest

- A police accidentally ran into Andrejs in a restaurant of YiLan County and reported to local police station for help.
- Andrejs was arrested on July 17, 2016
- Police monitored Mihail and Nicolae also made arrest on the same day in Room 715 of Victoria Hotel and discovered NTD 60,240,000 (i.e. 2 million USD). 
Andrejs led police to retrieve NTD 12,639,000 in July
1 bag lost

- Mr. Ko DeLin found the hidden bag and took it home before police came
- After Police released news about the missing bag, Mr. Ko returned the bag after 16 hours
- NTD 4,542,200 was found in the bag
- Mr. Ko was indicted for embezzlement
- A total of NTD 77,485,100 (2.6 million USD) was retrieved (93.4% of stolen money)
3 Arrested Defendants
Cross Analysis for Defendant Andrejs’s 2 Mobiles
GPS Records from Mihail’s and Nicolae’s Mobiles (1050601-1050724)
Taiwan GPS Records from Mihail’s and Nicolae’s Mobiles
Defendant Nicolae’s Mobile had cash photos taken in July 7, 2016
Defendant Nicolae’s Mobile had photos taken in July 7, 2016, at Tajikistan
Defendant Nicolae’s Mobile has payment records for pick-ups

Prosecutor AnChen Chang

4/7/2017
Defendant Mihail’s Mobile inquired ATMs information all over the world

<table>
<thead>
<tr>
<th>Time</th>
<th>Source</th>
<th>Value</th>
<th>Search Results</th>
</tr>
</thead>
<tbody>
<tr>
<td>2016/4/11 上午 03:10:02(UTC+0)</td>
<td>Google</td>
<td>catalunya caixa atm</td>
<td>加泰羅尼亞儲蓄銀行 ATM</td>
</tr>
<tr>
<td>2016/4/11 上午 03:12:00(UTC+0)</td>
<td>Google</td>
<td>spania atm</td>
<td>spania ATM</td>
</tr>
<tr>
<td>2016/4/11 上午 03:14:12(UTC+0)</td>
<td>Google</td>
<td>portugal atm</td>
<td>葡萄牙 ATM</td>
</tr>
<tr>
<td>2016/4/11 上午 03:21:07(UTC+0)</td>
<td>Google</td>
<td>atm maroco</td>
<td>ATM 品佳昌實業</td>
</tr>
<tr>
<td>2016/4/11 上午 03:23:06(UTC+0)</td>
<td>Google</td>
<td>atm france</td>
<td>ATM 法國</td>
</tr>
<tr>
<td>2016/4/11 上午 03:25:50(UTC+0)</td>
<td>Google</td>
<td>italy atm</td>
<td>ATM 意大利</td>
</tr>
<tr>
<td>2016/4/11 上午 03:28:07(UTC+0)</td>
<td>Google</td>
<td>atm horvatia</td>
<td>ATM horvatia</td>
</tr>
<tr>
<td>2016/4/11 上午 03:29:38(UTC+0)</td>
<td>Google</td>
<td>atm norvegia</td>
<td>ATM 挪威</td>
</tr>
<tr>
<td>2016/4/11 上午 03:30:32(UTC+0)</td>
<td>Google</td>
<td>atm norway</td>
<td>ATM 挪威</td>
</tr>
<tr>
<td>2016/4/11 上午 03:32:43(UTC+0)</td>
<td>Google</td>
<td>atm danemark</td>
<td>ATM danemark</td>
</tr>
<tr>
<td>2016/4/11 上午 03:34:42(UTC+0)</td>
<td>Google</td>
<td>atm swizerland</td>
<td>ATM 瑞士</td>
</tr>
</tbody>
</table>
Defendant Mihail’s WeChat mentioned Bitcoin, Yacht in Taiwan, Cash in Moscow

<table>
<thead>
<tr>
<th>Date and Time</th>
<th>Google Search Keywords</th>
<th>Translation</th>
</tr>
</thead>
<tbody>
<tr>
<td>2016/7/12 下午 07:14:32(UTC+0)</td>
<td>amex in taiwan 高盛信用卡台湾</td>
<td>AMEX 台灣 高盛信用卡台湾</td>
</tr>
<tr>
<td>2016/7/12 下午 07:16:10(UTC+0)</td>
<td>amex in taiwan 高盛信用卡台湾</td>
<td>AMEX 台灣 高盛信用卡台湾</td>
</tr>
<tr>
<td>2016/7/12 下午 12:21:34(UTC+0)</td>
<td>news on taiwan today 今天台湾新闻</td>
<td>今天台灣新聞</td>
</tr>
<tr>
<td>2016/7/12 下午 12:41:49(UTC+0)</td>
<td>rent car in taipei 租汽车在台北</td>
<td>租汽車在台北</td>
</tr>
<tr>
<td>2016/7/12 下午 12:52:10(UTC+0)</td>
<td>buy car in taiwan 買汽車在台灣</td>
<td>買汽車在台湾</td>
</tr>
<tr>
<td>2016/7/13 上午 08:08:09(UTC+0)</td>
<td>tayyib sambyul 台北伊斯坦布爾</td>
<td>台北伊斯坦布爾</td>
</tr>
<tr>
<td>2016/7/13 上午 08:08:16(UTC+0)</td>
<td>tayyib sambyul evra 台北伊斯坦布爾預訂</td>
<td>台北伊斯坦布爾預訂</td>
</tr>
<tr>
<td>2016/7/14 下午 05:51:18(UTC+0)</td>
<td>moskva tayyib aviabity 高速航空台北的航班</td>
<td>莫斯科飛往台北的航班</td>
</tr>
<tr>
<td>2016/7/16 上午 06:22:27(UTC+0)</td>
<td>tayyib putyeta tayyib 台北站到貨</td>
<td>台北站到貨</td>
</tr>
</tbody>
</table>

Prosecutor AnChen Chang

4/7/2017
## Defendant Mihail’s WeChat Log mentioned Money Laundering

<table>
<thead>
<tr>
<th>Date</th>
<th>Time</th>
<th>WeChat: wxid_e1w4eeujcq3r12 Freedom Finance.</th>
<th>Text</th>
</tr>
</thead>
<tbody>
<tr>
<td>2016/4/27</td>
<td>07:30:53(UTC+0)</td>
<td>WeChat: wxid_e1w4eeujcq3r12.</td>
<td>Defendant Mihail’s WeChat Log mentioned Money Laundering</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Date</th>
<th>Time</th>
<th>WeChat: wxid_c0caovkccqvp12.</th>
<th>Text</th>
</tr>
</thead>
<tbody>
<tr>
<td>2016/4/27</td>
<td>下午</td>
<td></td>
<td>Zavtra utrom?</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Date</th>
<th>Time</th>
<th>WeChat: wxid_e1w4eeujcq3r12.</th>
<th>Text</th>
</tr>
</thead>
<tbody>
<tr>
<td>2016/7/10</td>
<td>上午</td>
<td>09:29:12(UTC+0)</td>
<td>Рамин привет. у тебя случайно связь нет в Тайване? рамин,你在台湾有沒有频道?</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Date</th>
<th>Time</th>
<th>WeChat: wxid_e1w4eeujcq3r12. Freedom Finance</th>
<th>Text</th>
</tr>
</thead>
<tbody>
<tr>
<td>2016/7/10</td>
<td>上午</td>
<td>09:45:06(UTC+0)</td>
<td>Пиши сюда. 你继续写。</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Date</th>
<th>Time</th>
<th>WeChat: wxid_e1w4eeujcq3r12. Freedom Finance</th>
<th>Text</th>
</tr>
</thead>
<tbody>
<tr>
<td>2016/7/10</td>
<td>上午</td>
<td>09:54:43(UTC+0)</td>
<td>Смотри у меня ребят сейчас в тайбэй в тайване у них там напал в их валюты почти на 2 лимона. $ в эквиваленте. ты можешь как то помочь привезти его там и что я его в мск получил?</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Date</th>
<th>Time</th>
<th>WeChat: wxid_e1w4eeujcq3r12.</th>
<th>Text</th>
</tr>
</thead>
<tbody>
<tr>
<td>2016/7/10</td>
<td>上午</td>
<td>09:55:23(UTC+0)</td>
<td>Это срочный вопрос. Потому что меня подвели люди очень сильно с кем я договаривался. 這件事很塌, 因为我原本谈好的那些人给了我搞砸了。</td>
</tr>
</tbody>
</table>
# Instant Messages (15)

<table>
<thead>
<tr>
<th>#</th>
<th>From</th>
<th>To</th>
<th>Subject</th>
<th>Body</th>
<th>Location</th>
<th>Source Application</th>
<th>Timestamp-Date</th>
<th>Timestamp-Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>+37360299835 Марих</td>
<td>Я там</td>
<td></td>
<td>我到了</td>
<td></td>
<td>iMessage: +79687029995</td>
<td>10/3/10/19</td>
<td>11:21:02(UTC-8)</td>
</tr>
<tr>
<td>2</td>
<td>+79687029995</td>
<td>Зайди в Tim</td>
<td></td>
<td>那你要赶紧去TEAM SPEAK</td>
<td></td>
<td>iMessage: +79687029995</td>
<td>10/3/10/20</td>
<td>09:15:25(UTC+8)</td>
</tr>
<tr>
<td>3</td>
<td>+37360299835 Марих</td>
<td>Зайди обратно в tim</td>
<td></td>
<td>那你要进去一趟</td>
<td></td>
<td>iMessage: +79687029995</td>
<td>10/3/10/20</td>
<td>09:26:02(UTC+8)</td>
</tr>
<tr>
<td>4</td>
<td>+37360299835 Марих</td>
<td>ruderman aleksandr new york usa money gram om</td>
<td></td>
<td>是用money gram寄他754美金,因为這個人都會準備</td>
<td></td>
<td>iMessage: +79687029995</td>
<td>10/3/10/20</td>
<td>10:53:27(UTC+8)</td>
</tr>
<tr>
<td>5</td>
<td>+79687029995</td>
<td>Через money грам</td>
<td></td>
<td>是透過money gram</td>
<td></td>
<td>iMessage: +79687029995</td>
<td>10/3/10/20</td>
<td>10:57:34(UTC+8)</td>
</tr>
<tr>
<td>6</td>
<td>+37360299835 Марих</td>
<td>Да</td>
<td></td>
<td>是的</td>
<td></td>
<td>iMessage: +79687029995</td>
<td>10/3/10/20</td>
<td>11:32:01(UTC+8)</td>
</tr>
<tr>
<td>7</td>
<td>+79687029995</td>
<td>Понял</td>
<td></td>
<td>了解</td>
<td></td>
<td>iMessage: +79687029995</td>
<td>10/3/10/20</td>
<td>11:35:22(UTC+8)</td>
</tr>
<tr>
<td>8</td>
<td>+79687029995</td>
<td>Я завтра иду в одно тур агентство по поводу визы в Америку! Скажи помогут 100%</td>
<td></td>
<td>我明天要去一家旅行社处理美国签证,你哪有时间可以帮忙</td>
<td></td>
<td>iMessage: +79687029995</td>
<td>10/3/10/20</td>
<td>11:53:28(UTC+8)</td>
</tr>
<tr>
<td>9</td>
<td>+37360299835 Марих</td>
<td>Возьмите меня с собой</td>
<td></td>
<td>那你带我一起去</td>
<td></td>
<td>iMessage: +79687029995</td>
<td>10/3/10/20</td>
<td>11:54:00(UTC+8)</td>
</tr>
<tr>
<td>10</td>
<td>+37360299835 Марих</td>
<td>))))</td>
<td></td>
<td>(笑哭)</td>
<td></td>
<td>iMessage: +79687029995</td>
<td>10/3/10/20</td>
<td>11:54:06(UTC+8)</td>
</tr>
<tr>
<td>11</td>
<td>+79687029995</td>
<td>Я посмотрю завтра что толку запланировать и на конец недели в посольстве</td>
<td></td>
<td>我看看要处理什麼,签证一定要去辦事處</td>
<td></td>
<td>iMessage: +79687029995</td>
<td>10/3/10/20</td>
<td>11:55:16(UTC+8)</td>
</tr>
<tr>
<td>12</td>
<td>+37360299835 Марих</td>
<td>В багаж бери если что))))</td>
<td></td>
<td>把我孩內裡面</td>
<td></td>
<td>iMessage: +79687029995</td>
<td>10/3/10/21</td>
<td>12:05:58(UTC+8)</td>
</tr>
<tr>
<td>13</td>
<td>+79687029995</td>
<td>88888888888</td>
<td></td>
<td></td>
<td></td>
<td>iMessage: +79687029995</td>
<td>10/3/10/21</td>
<td>12:06:17(UTC+8)</td>
</tr>
<tr>
<td>14</td>
<td>+37360299835 Марих</td>
<td>Зайди в tim спимк</td>
<td></td>
<td>進去TEAM SPEAK</td>
<td></td>
<td>iMessage: +79687029995</td>
<td>10/3/10/21</td>
<td>03:32:55(UTC+8)</td>
</tr>
<tr>
<td>15</td>
<td>+37360299835 Марих</td>
<td>+37259611029 мой вайбер</td>
<td></td>
<td>nilbe的煩事</td>
<td></td>
<td>iMessage: +79687029995</td>
<td>10/3/10/22</td>
<td>04:36:16(UTC+8)</td>
</tr>
</tbody>
</table>
Passport photos from confiscated mobiles

2BAC5856-C383-4748-8E63-4F8956415A9F_original.jpg
FirstImageOrigin.jpg
IMG_0584.png
IMG_0597.jpg
IMG_0598.jpg
IMG_0603.jpg
IMG_0604.jpg
IMG_2843.png
IMG_2844.png
IMG_2901.jpg

IMG_3209.jpg
IMG_4092.jpg
IMG_4574.jpg
IMG_4594.jpg
IMG_4595.jpg
IMG_4596.jpg
IMG_6009.png
IMG_6341.png
IMG_6357.png
IMG_6735.png

IMG_7934.jpg
IMG_7034.jpg
IMG_7034_1.jpg
IMG_7054.jpg
IMG_7324.jpg
IMG_7341.png
IMG_7377.png
IMG_7877.png
IMG_7896.jpg
IMG_8502.jpg
IMG_8523.jpg

IMG_8595.jpg
IMG_8596.jpg
IMG_8723.jpg
IMG_9363.jpg
IMG_9364.jpg
IMG_9431.jpg
IMG_9878.jpg
стра.png
stra.png
stra.png
stra.png
stra.png
stra.png
stra.png
stra.png
stra.png
stra.png
Passport photos from confiscated mobiles
Cash Photos found in confiscated mobiles
Indictment

• Sep. 9, 2016, prosecutor Lee YenLin indicted 3 defendants for 12 accounts of charges violating the criminal law:
  §339-2 fraud ATM
  §358 invading others’ computer
  §359 changing others’ computer record without reason
  §360 interfere others computer with a computer program without reason
  §362 make computer programs to obstruct computer uses
• Issued want warrants for other 19 defendants
• 3 defendants detained in Taipei Detention Center
District Court Judgement

- 3 defendants denied as members of the Carbanak fraud group and argued that they only received instructions to come to Taiwan but had no idea with any illegality.
- Judging from their mobiles records and the fact that 3 defendants actually actively involved in money laundering before they came to Taiwan, Court overruled their arguments.
- Taipei District Court sentenced each defendants for 5 years incarceration plus NTD 100,000 fines (i.e. 3300 USD) on January 25, 2017.
- 3 judge tribunal disagreed with prosecutor’s 12 accounts charges but decided only for 1 account of charges.
- The court judgment also mentioned they felt sorry that the maximum sentencing of the charges was only
World First Carbanak Case established

- Thailand, Romania, Belarus, Moldova, and Europol contacted for mutual legal assistance.
- Romania and Europol sent polices to Taiwan to interrogate Mihail and Andrejs for more information
- Babii was later arrested by Belarus police and Romania is negotiating for extradition
- Penkov Nicolae may involve in case in Moldova and under investigation
- More Mutual Legal Assistance is coming.
Future task of computer crimes

- Symantec: (Internet Security Threat Report, 2016) 430 million malwares newly discovered in 2015; 429 million ID leaked (at 15% report rate); encrypted ransom ware increased
- Kaspersky Lab: April, 2016, hackers attack industrial control system to steal gasoline and coal
- Kaspersky Lab: June, 2016, discovered xDedic black market, selling infected server licenses at the price of 6 US dollars; 70624 serves in 174 countries, by 416 dealers
- Kaspersky Lab: malware “Darkhotel”, hackers attack hotels’ wifi to steal business secrets
Fighting Against Enemy Like Shadow