The Latest Cybersecurity Landscape in Hong Kong

FinTech Security Conference - 2018

Frankie Li
You heard a lot ... Like this
But not from Hong Kong
The analysis of the latest APT attacks in HK

Frankie Li

2014-2015
OUR WORLD INTERCONNECTED
OUR SYSTEMS INTERCONNECTED
OUR SECURITY VULNERABLE
OUR IDENTITIES VULNERABLE
OUR HOMES VULNERABLE
OUR MONEY VULNERABLE
This is not about money
this is about politics
2016:

Hong Kong government hacked by Chinese cyberspies: FireEye

• APT 3 targeted the organizations with "spear-phishing" attacks
• "Relevant security measures had already been put in place to block the suspicious e-mails," Government office confirmed in a statement
2016: The SWIFT Attacks – Hong Kong?

- Attacker activated 2 servers on 20 March and 28 March
- 28 April 2016, unnamed bank in Hong Kong was robbed
- Bank used Customer-hosted SWIFT connectivity
- This took one month once inside the compromised bank for preparation and organization of money laundering
- Attack was sophisticated and to accomplish it attackers developed tools specifically for this bank
ATM Hacks extend to the Great China Regions

Three Russians were Alexei Starostin (36 years), Sergey Arustamov (32 years) and Farid Kerimov (25 years). They are accused of hacking ATMs and stealing money from users. The alleged hack involved tampering with software and硬件 components to divert money from bank accounts.

The suspects were arrested and are currently being held in custody. The investigation is ongoing and further details will be released as they become available.
Exchange hacking occurs regularly

<table>
<thead>
<tr>
<th>Date</th>
<th>Event</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mar 2012</td>
<td>Bitcoin was exposed to the hosting site vulnerability. The funds were stolen and the exchange was closed</td>
</tr>
<tr>
<td>Sept 2012</td>
<td>Bitfinex tokens (BFX) for users who lost their funds</td>
</tr>
<tr>
<td>Feb 2014</td>
<td>Mt. Gox was hacked through phishing. The platform was completely reorganized. Losses were covered from reserve fund</td>
</tr>
<tr>
<td>Jan 2016</td>
<td>Bitstamp was hacked through phishing. The platform was compromised. Partial compensation was paid to users</td>
</tr>
<tr>
<td>Aug 2016</td>
<td>The exchange did not use cold storage. The exchange issued Bitfinex tokens (BFX) for users who lost their funds</td>
</tr>
<tr>
<td>Jul 2017</td>
<td>The hacker could access the backup key. The exchange was closed and funds partly refunded to users</td>
</tr>
<tr>
<td>Jan 2018</td>
<td>The exchange suspended trading, closed its website and exchange services, and filed for bankruptcy protection. Users did not receive compensation</td>
</tr>
<tr>
<td>Jun 2018</td>
<td>The exchange reported a hack on its website. Reserves had been moved to a cold wallet</td>
</tr>
<tr>
<td>Feb 2018</td>
<td>The exchange just announced the tokens were missing. They announced that it appear to be related to BitGrail’s software</td>
</tr>
<tr>
<td>Mar 2018</td>
<td>Coincheck hasn’t disclosed how their system was breached, just saying that it wasn’t an inside job. It kept customer assets in a hot wallet. Users are partially refunded in Mar 2018</td>
</tr>
</tbody>
</table>

The BitGrail hack is a bit complicated. The exchange just announced the tokens were missing. They announced that it appear to be related to BitGrail’s software.

The Coincheck hasn’t disclosed how their system was breached, just saying that it wasn’t an inside job. It kept customer assets in a hot wallet. Users are partially refunded in Mar 2018.

The exchange reported a hack on its website. Reserves had been moved to a cold wallet.
2016: Security Landscape changed?

Money is now Data
2016: Cyber Fortification Initiative
2017: Hong Kong travel agent WWPKG

• One of Hong Kong’s largest travel agencies, revealed its customer database was hacked, putting at risk personal information such as ID card numbers and credit card

• The police source said that the hackers were likely to be based overseas
2018: Hong Kong Broadband Network
2018: Unpublished Attack Incident

Watering Hole Attack on Leading Hong Kong Telecom Site Exploiting Flash Flaw (CVE-2018-4878)

Posted by Michael Gorelik on March 23, 2018 at 2:01 PM

Find me on:

On March 21, 2018, Morphisec Labs began investigating the compromised website of a leading Hong Kong Telecommunications company after being alerted to it by malware hunter @PhysicalDrive0. The investigation, conducted by Morphisec researchers Michael Gorelik and Assaf Kachlon, determined that the Telecom group’s corporate site had indeed been hacked. Attackers added an embedded Adobe Flash file that exploits the Flash vulnerability CVE-2018-4878 on the main home.php page.
Cathay Pacific data leak warrants formal investigation, Hong Kong ex-privacy chief says in break with successor

- Allan Chiang says it is not the first time watchdog under Stephen Wong has failed to adequately investigate companies
- Number of investigations by privacy commissioner fell from 106 in 2014 to only one last year

PUBLISHED: Saturday, 03 November, 2018, 4:52pm
UPDATED: Saturday, 03 November, 2018, 10:51pm
The Legislative Council ("LegCo") has requested Cathay Pacific Airways Limited ("Cathay") to attend a joint meeting of the Panel of Constitutional Affairs, Panel on Information Technology and Broadcasting and the Panel on Security on Wednesday, 14 November, 2018. LegCo has also requested a written response to questions prepared by the Hon. Charles Mok to be provided on or before noon, 12 November 2018. Our written response to the questions prepared by the Hon. Charles Mok is set out below.

1. How did you know your systems had suspicious activities in March? How did the monitoring system pick up the suspicious activity/attack? The time suspicious activity surfaced and was the system continuously attacked after the detection? If so, how long was the system continuously being attacked? In May how did you confirm the details of passenger details accessed?

Cathay became aware of suspicious activity on its network related to the attack in March 2018. Initially, the only evidence of known suspicious activity pertained to a brute force attack on user accounts. At this stage, an initial evaluation commenced and following this analysis, a thorough investigation launched with the assistance of a leading cybersecurity firm. Cathay immediately took action to contain the incident based on known activities at that time and commenced an internal investigation. Cathay was subject to further attacks which were at their most intense in March, April and May but continued thereafter. By early May, evidence of unauthorised access and/or exfiltration of data by the attackers was confirmed based on forensic evidence. This was the first phase of the Incident.
2018: Smart Banking Initiatives

Financial Institution is now a Software Company ;)

Seven Smart Banking Initiatives

- Virtual Banking
- Fintech Supervisory Sandbox
- Cross-border collaboration
- Research and talent development
- Faster Payments
- API

Dragon Advance Tech
2018: Cybersecurity and Technology Risk

Protected by C-RAF

The seven domains of maturity assessments
Is Your Online Banking Infrastructure Secure?
2018: New Cybersecurity Incidents

- On Oct 31, 2018 HKMA has requested to all e-wallets operators to suspend the automatically top-up via the Fast Payment System because they found a number of customers had suffered loss of fraud cases on electronic Direct Debit Authorization (eDDA)
2018: HSBC e-payment app PayMe Under Fire

• Simple verification procedures for HSBC e-payment app PayMe allowed hackers to carry out unauthorised transactions after luring victims into disclosing their email passwords using phishing scams.
Short Near Future we shall have eKYC
Latest Development of Virtual Banks

【明報專訊】虛擬銀行是金管局去年9月提出的「金融科技7招」之中重要的一環，從提出到完成諮詢不足半年，再在今年5月發出認可指引，至8月收到首批約30個申請，一直雲屬風行。然而近日尚未發出任何牌照，卻已把三分之一的申請打回頭。有業內人士指出，與近日一連串網絡安全事件不無關係。

由於近日國泰（0293）泄露客戶資料事件，加上相繼有電子錢包被盜用。社會對於發展金融科技的共識，是要先做好網絡保安。有申請者因此估計，當局在處理虛擬銀行申請變得更審慎，尤其會着重審視申請者的資訊保安系統與管控措施。

指引要求聘獨立專家評估系統

事實上，金管局在虛擬銀行指引中亦強調科技相關風險的要點，要求申請人須聘用合資格的獨立專家，獨立評估其計劃中的科技管治及系統是否足夠，並向當局提交評估報告。虛擬銀行在開業前，亦須就其電腦硬件、系統、保安、程序及管控措施作更詳細的獨立評估。

除網絡安全事件外，有申請者亦估計，人手不足是一大問題。由於金管局處理虛擬銀行申請的部門只有約5名員工，因此採取較保守策略，先行擋置文件不足的申請，集中精力處理其餘申請。
Smart FinTech | Exposing more attack service
Safe House or Sweet Home?
Safe House or Lake Resort on the cliff?
Encryption = Security?
Firewall == Network Security?
How is your Security being Implemented?
Building Cybersecurity Capacity for Hong Kong

**Legal Measures**
- Legal Measures Strategy
- Government Legal Authority
- Adequate and harmonized legal frameworks

**International Cooperation**
- Enhanced collaboration (multi-stakeholder, Bi/Multi lateral)
- Inter-Agency Collaboration

**Technical/Procedural Measures**
- Governmental lead Cybersecurity Goals and Framework
- Secure Government Infrastructure
- Global Technical Collaboration

**Capacity Building**
- Cybersecurity Skills Development
- Culture of Cybersecurity
- Cybersecurity Innovation

**Organizational Structures**
- Government Coordination
- Governmental Focal Point
- Sectoral CIRT
- Public-Private Partnerships

**Human Capacity Building**
- Curricula and Training Program
- Bespoke Training

---

Dragon Advance Tech
Thank you

Q & A