Yui Kee Computing Ltd.

Newsletter

Contents

Immigration Department Personal Data Leak

<web-link for this article>

The Police and the Privacy Commissioner are investigating the leak of Hong Kong Immigration Department documents containing personal data. A special task force headed by an Assistant Director of Immigration is conducting an internal investigation. The confidential documents have been revealed in "anonymous letters", but where the letters were discovered has not been revealed.

This is not the first time the Immigration Department has failed to keep personal data confidential. In May 2008, Immigration Department files were disclosed through the Foxy file sharing program. After the incident, the Immigration Department signed a formal undertaking with the Privacy Commissioner to make 10 changes in how it handled personal data but less than three months later, the department was in the news for further data leaks through Foxy.

Updated: 08th September 2014

Anonymous Whistleblower Revealed Leak

A more informative press release on the www.info.gov.hk website reveals details missing from the press release on the www.news.gov.hk website. Crucially, the anonymous letters that contained confidential Immigration Department documents were sent to the Immigration Department, presumably with the intent of alerting the department to the data leak.

The whistleblower has done the people of Hong Kong a service in triggering this investigation, and it is to be hoped that the investigation will pursue the flaw that allowed the leak and/or the people who intended dishonest gain from it, not the whistleblower.

More Information

Personal info theft probed
Data Leak Disease
Immigration Department Learns Information Security Management Basics
Response to data leakage by Immigration Department
Data leak points to Immigration Department
Suspected theft of personal data held by Immigration Department
Immigration Dept reports data leak

HKMA Launches Information Security Videos

<web-link for this article>

The Hong Kong Monetary Authority (HKMA) has launched a series of videos promoting "smart and responsible" use of banking services, including advice on information security. The four videos are available on the HKMA's YouTube Channel, and will be shown on the MTR, green minibuses, bus shelters and the HKMA Information Centre.

The videos have a Cantonese soundtrack. The short (33 second) versions have no English subtitles. Some 1 minute versions have English subtitles.

More Information

HKMA Launches Video Series on Consumer Education
HKMA Smart Tips Channel 金管局「智醒」頻道
Security Tips on Using Mobile Banking (1-minute version) (English subtitles)
Security Tips on Using Internet Banking (1-minute version) (English subtitles)
Security Tips on Using Automatic Teller Machines (1-minute version) (English subtitles)
Credit Cards - Minimum Payment (1-minute version) (English subtitles)

Fake Android App Targets Hong Kong Pro-Democracy Activists

<web-link for this article>

Messaging service WhatsApp was used to distribute links to an Android app that claimed to be for coordination of the Occupy Central protest. The app was supposedly created by Code4HK, a group with the aim of using programming to improve government transparency, but the link was distributed from an unknown phone number.

The link points to a server code4hk.vicp.cc, 101.55.121.36 located in South Korea. The second-level domain name, vicp.cc is registered to Shanghai Best Oray Information S&T Co.,Ltd. in Guangzhou.

The app was decompiled by Matthew Rudy Jacobs who reported that the app is designed to:

☐ Hijack the QQ app

☐ Capture outgoing call information and record the calls

☐ Use Baidu to gather location data

☐ Report to a remote server, "61.36.11.75", located in South Korea

The evidence so far suggests that unknown attackers are spreading this malware to spy on pro-democracy activists in Hong Kong.

More Information

Fake Occupy Central app targets activists' smartphones
[突發] 假佔中 app
fake-code4hk-app
Matthew Rudy Jacobs
Code for Hong Kong on Facebook

First Copyright Arrest for New LMS1+ Software

<web-link for this article>

Hong Kong's Customs and Excise Department (C&ED) arrested a 40-year old man on 26th September for online copyright infringement based on evidence collected by their new Lineament Monitoring System 1 Plus (LMS1+) software. The man was arrested in Yuen Long and two computers were seized.

The LMS1+ software is jointly developed by the C&ED and the University of Hong Kong Center for Information Security and Cryptography (CISC) and it automatically searches discussion forums and detects suspected intellectual property infringement activities. It can collect evidence of copyright offences committed by file sharing through on-line sites for storage of personal digital files (cyber-lockers).

The C&ED and CISC have had a history of development cooperation, starting from 2007 and resulting in Lineament Monitoring System I (LMSI) in 2007 and Lineament Monitoring System II (LMSII) in 2011. LMSI monitors peer-to-peer infringing activities and LMSII tracks sale of infringing goods on online auction sites. The C&ED side of the cooperation was strengthened in 2013 with the establishment of the Electronic Crime Investigation Centre (ECIC).

More Information

Customs detects first case using new system against suspected copyright infringer on discussion forum

New Tool Jointly Developed by CISC and HK Customs & Excise Dept to Fight Illegal Upload

[PDF] Replies to initial written questions raised by Finance Committee Members in examining the Estimates of Expenditure 2011-12 (page 286)

Man arrested for copyright infringement

New Weapon to Crack Down Auctioned Fakes

Lineament Monitoring System II

Chief Secretary Visits New Electronic Crime Investigation Centre