YUI KEE
銳基電腦顧問有限公司
Anti-Virus, Network Security & Education

Yui Kee Computing Ltd.

Newsletter

March 2017

Contents

COMPELSON Labs Release MOBILedit Forensic Express 4.0

<web-link for this article>

Pioneers in phone forensic tools, COMPELSON Labs say that MOBILedit Forensic Express has entered a new era by adding physical extraction and analysis for Android. The tool is now a native 64-bit application and Version 4.0 has a total of 359 improvements.

MOBILedit Forensic Express is a phone extractor, data analyser and report generator in one solution. Its capabilities include deleted data recovery, advanced application analyser, wide range of supported phones including most feature phones, fine-tuned reports, concurrent phone processing, physical acquisition and easy-to-use user interface. It can be used as the only tool in a lab or as an enhancement to other tools through its data compatibility. When integrated with COMPELSON Labs' Camera Ballistics tool, it scientifically analyses camera photo origins.

New features

- Android physical data extraction, allows extraction of physical images from investigated phones.
- Physical analysis allows opening image files, either generated by Forensic Express or 3rd party tools, and recover deleted files plus all other deleted data.
- Native 64-bit application, improves speed and stability.
- New File Manager to copy, move, and work with complete export folders, it solves problems with long filenames – which Windows File Explorer or Total Commander usually cannot handle.
- Import of Cellebrite UFD files for both logical and physical analysis.
- Rich MS Excel report allows custom data analysis using Excel features.

Improvements

- Improved Android 7.0 support
- Wi-Fi connection now also supports app analysis and physical extraction for rooted Android phones
- New report sections for Notes, Tasks, and deleted iOS applications
- ADB and iTunes backup password can be included in reports and exports
- More information from iOS, including itunesmetadata.plist analysis, better keychain decryption, more iCloud information
- Additional phone information presented, such as cell info, device name, serial number and unique id
- Option to also pack binary files linked to PDF and HTML reports to create more compact reporting
- Memory usage optimizations
- More reliable cancelling of operations

New and updated application analysers

myMail, Verizon messaging app, ASUS Browser, ASUS Email, Play Store, Chrome Canary, BBM, eBay, Mi Fit, Opera Free VPN, WowApp, BlackBerry Hub+ Services, 360 Browser, Blendr, Hide My Text, ZOOM Cloud Meetings, Wikipedia, Textie, TextMe Up Free Calling & Texts, Google Quick Searchbox, Blocked Number, WhatsApp, Telegram, Viber, Hangouts

More Information

- MOBILedit Forensic Express

How Important is the Theft of Hong Kong Voter Information?

<web-link for this article>

Allan Dyer

This morning I accessed the voter registration data that was stolen from the Registration and Electoral Office (REO), later I visited a bank website that required the same information for online banking signup.

Before I'm arrested, I should clarify that the voter registration data I accessed was a copy kept for public checking at my local District Office, and it was my own details that I checked. Now you're thinking that the theft was unimportant, the data is public anyway, but the situation is more complicated, with multiple stories. First, we must understand how public a lot of our personal information is, and how the Information Society is changing what that means. Second, how do we think about security, how security is in conflict with itself, and how Defence in Depth fails. Third, how do supposedly responsible organisations misuse our sensitive data.

A quick recap. Earlier this week, the story broke that a laptop belonging to the REO containing details of 3.7 million Hong Kong Registered Voters and a second laptop containing the details of 1,194 Election Committee Members had been stolen from a locked room at the AsiaWorld-Expo on Lantau Island. Police are investigating. The laptops had been stored as preparation for a "fallback venue" for the Chief Executive Election on Sunday 26 March, and the theft was discovered when REO staff went to pick up the materials on Monday. The information was protected: REO staff required access cards to enter the room, there were surveillance cameras, and the REO said in a statement, “The information is protected by multiple encryptions which are extremely difficult to break through." IT Sector lawmaker Charles Mok said, "Do not trust the so-called security experts who say [the data] will be safe with encryption." Why the full register was on the laptop when only the details of the Election Committee Members were required for the Chief Executive Election has not been explained.

The Truth is Out There

I demonstrated this morning that the voter registration data is freely available, and the same sensitive personal data are available from other sources. I am a Company Director, so my name, identity document number and home address are publicly available from the Companies Registry for a small fee. We disclose our sensitive personal information to other people through our normal social activities: inviting friends to our birthday party reveals our home address and date of birth.

However, there is a difference in accessibility. When I visited my District Office, I was presented with the relevant section of the register as a thick file of fanfold paper. I could search through it for my address to check my entry, and I could even snoop a little on my neighbour's entries. I had to sign a declaration that my purpose in checking the register was permitted. I hope I would have been challenged if I started copying the entries, or taking photos. Copying the entire register was infeasible.

Access to the entire, unencrypted, database gives other opportunities. Records can be quickly searched and correlated to other sources of information to gather sufficient details, for example, to fraudulently register for online banking. The Hong Kong Police have a list of frauds to beware of, some of those could be made more believable using details from the electoral register. Searching by address could reveal the names of family members to use in "relative in trouble" phone scams. Criminals could tailor the scam to the wealth of the victim, revealed by the home address.

It is not that such analysis and targeting is impossible with the paper records, it is the ease of misuse of electronic records that make it a game-changer.

I Thought It Was Secure

What is adequate security? The REO kept the database encrypted (multiple layers), on a laptop in a locked room with surveillance cameras at a venue with security guards. They were there to provide security (specifically, availability of the valid voters) in the event of the fallback venue of the Chief Executive Election being used. This is Defence in Depth. Was this sufficient?

Now, the cameras, the guards and the lock did not prevent the theft, so we are dependant on the remaining layer of defence: the encryption.

If you imagine the circumstances when the fallback venue would need to be used, everyone has hurriedly moved from the primary venue and an official retrieves the laptop, what is their concern? Probably, "Do I remember the password?", so, what are the chances the password was written down and stored with the laptop?

In the recent incident where a long escalator at Langham Place suddenly failed, injuring people, the initial information is that there were two faults: the drive chains broke, and the safety brake failed to work. An official was quoted as saying that double failures are very rare. Unfortunately, this misses the point: the brake could have failed at any time since it was last tested. It was a single failure, creating an accident waiting to happen when there was a second failure. It is very easy for Defence in Depth to fail the same way, slowly degrading as each layer fails, is bypassed, or is weakened. Unless every layer is tested regularly and independently, no-one will notice until the catastrophic failure occurs.

Standard Practice

There are three general methods of authenticating someone, usually described as something you have (e.g. a key), something you know (e.g. a password) and something you are (e.g. a fingerprint). Each must be used correctly, you cannot authenticate someone with information that is not secret, and your fingerprint reader should check the finger is alive. Using multiple, different factors improves the reliability of the authentication.

Phonebanking is an example of a very poor security system: the medium restricts you to a single factor: something you know. Even worse, the phonebanking PIN is transmitted over an open communications channel with no encryption. A chip to decode phone tones is readily available and costs less than a lunchbox.

An ATM card with a PIN is a good example of two-factor authentication: something you have and something you know. Relying on either one alone is dangerous, a card is easy to steal or clone and a 4 or 6 digit PIN is a very weak password, but together they are difficult for an attacker to circumvent... as long as the user keeps the PIN secure.

HSBC's online banking registration page requires the bank account number (available on every cheque you write), either the ATM or the Phonebanking PIN, and the identification document number (now available in the encrypted registered voter database, and elsewhere). This amounts to a single, weak, factor of authentication.

When challenged about their security arrangements, responsible organisations usually refuse to discuss their internal measures or risk assessments (security through obscurity) and fall back on saying they follow industry standard practice and regulator's guidelines. However, we cannot continue to consider the security of applications in isolation. Identity document numbers are being misused as both Unique Identifiers and as Authentication Tokens and information in an application considered "low risk" can be re-used in a high value attack on a different application. The theft of two laptops is a reminder of how vulnerable we all are.

Updated: 31st March 2017

Also Online

Voters can also check their entry on the register at the REO's Online Voter Information Enquiry System. The system is protected against bulk harvesting of voter information. The user is warned that they must have written permission to check someone-else's information using the system. The user must input their Hong Kong Identity Card number, their name, in English or Chinese or Chinese Commercial Codes, and complete a Captcha. Then they must select their correct street name and flat unit from short lists. They are then shown their full name, registered address, and constituencies they are eligible to vote in.

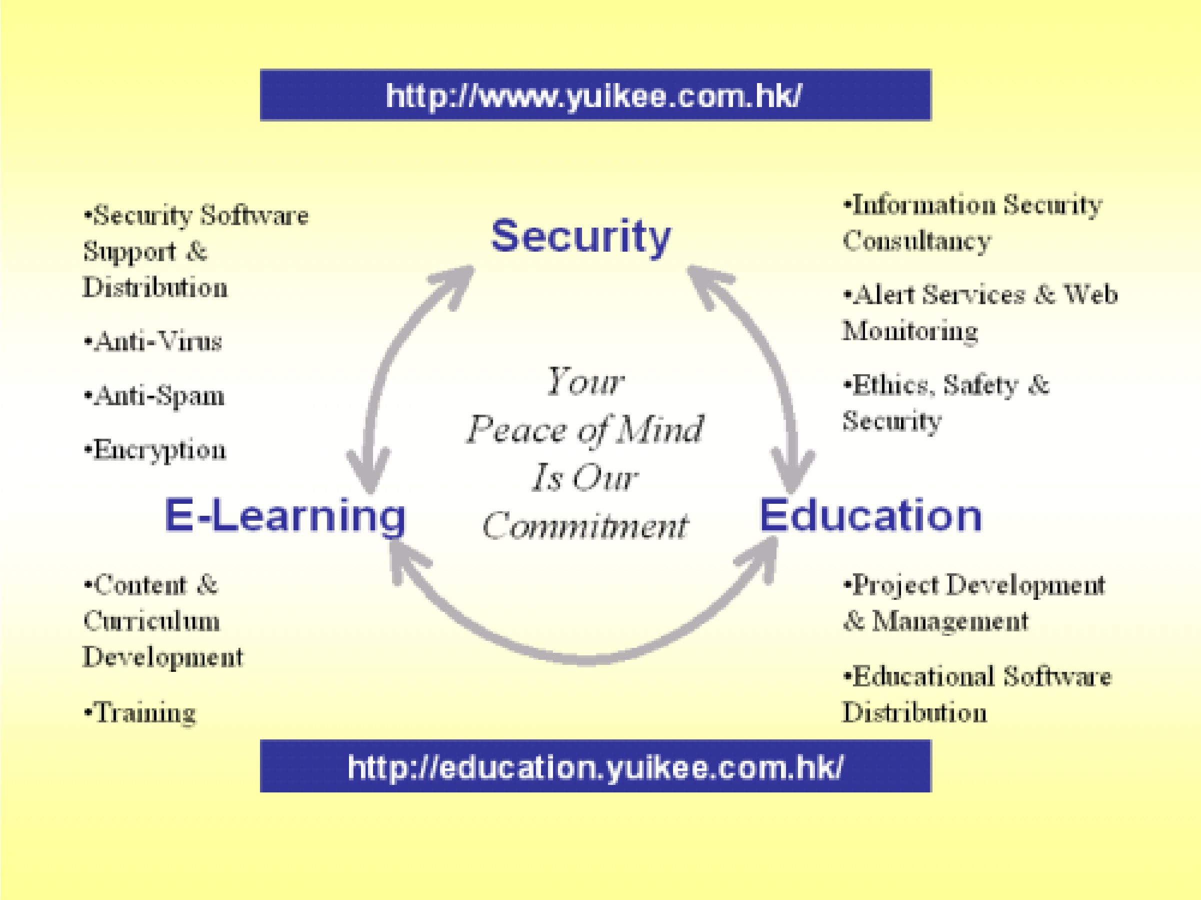
Whether these measures are sufficient to prevent bulk harvesting should be regularly tested by security consultants authorised by the REO.

More Information

- Hong Kong gov't loses computers with personal data of all registered voters
- Laptops containing 3.7 million Hong Kong voters' data stolen after chief executive election
- Hong Kong gov't says lost election computers are encrypted and 'extremely difficult to break through'
- Companies Registry
- Beware of Deception
- HOLTEK HT9170D-18SOPLF IC, DTMF RECEIVER, SMD, SOP18
- Online Voter Information Enquiry System

YUI KEE
銳基電腦顧問有限公司
Anti-Virus, Network Security & Education

Suite C & D, 8/F, Yally Industrial Building
6 Yip Fat Street, Wong Chuk Hang, Hong Kong
Tel: 2870 8550 Fax: 2870 8563
E-mail: info@yuikee.com.hk
http://www.yuikee.com.hk/



http://www.yuikee.com.hk/

Security

- Security Software Support & Distribution
- Anti-Virus
- Anti-Spam
- Encryption

- Information Security Consultancy
- Alert Services & Web Monitoring
- Ethics, Safety & Security

Your Peace of Mind Is Our Commitment

E-Learning

- Content & Curriculum Development
- Training

Education

- Project Development & Management
- Educational Software Distribution

http://education.yuikee.com.hk/