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

Yui Kee Computing Ltd.

Newsletter

June 2009

Contents

Policewoman from Hong Kong in Scottish Privacy Breach

<web-link for this article>

An Edinburgh policewoman, Anna Wong, is facing 54 charges of breaching the Data Protection Act in the Edinburgh Sheriff Court. Originally from Hong Kong, Wong claims she used the Scottish Intelligence Database and the Lothian and Borders Operational Support System to search for details of outstanding cases against two people she knew. However, faced with difficulty in recording Chinese names on the computer database, she widened the search to "Chinese" and began accessing others in the Chinese community.

Sheriff Elizabeth Jarvie QC described the breach as "very serious" and said that there was "no legitimate police purpose" for the database access. The Sheriff also called for a report on what safeguards have been put in place to protect people's private data, from the Lothian and Borders Chief Constable David Strang.

Writing in his blog, Sophos technology consultant Graham Cluley found it galling "to hear that a database being run by the authorities in a multi-cultural society cannot easily search for names which use foreign characters". He suggested that criminals could change their names to take advantage of the omission. But, more seriously, he asked, "but what practical safeguards can we put in place to police the many people who are authorised to access the data? This is going to be an enormous challenge moving forward. "

Wong will be sentenced next month.

More Information

Dodgy coppers and incompatible character sets
Sheriff demands answers after policewoman illegally accessed personal details
Data Leak Disease

Data Leak Disease Spreads to Police?
2008/03 - Why flawed privacy ordinance must be given more teeth

Baptist University Applicant Data Leak

<web-link for this article>

According to a report by vice-president (Administration) and secretary of Hong Kong Baptist University (HKBU) Andy Lee Shiu-chuen, a member of staff responsible for student recruitment of the BA (Hons) in English Language and Literature and BEd (Hons) in English Language Teaching programs accidentally attached a file containing personal data of 190 applicants to an email sent to 95 applicants. The employee then sent another email, asking the recipients to delete the previous email and attached file.

The University has reported the incident to the Office of the Privacy Commissioner for Personal Data and set up a five member team to investigate the case. Mr. Lee said that the University had called all the applicants affected to apologise.

Yui Kee Chief Consultant Allan Dyer commented, "This type of incident is very difficult to prevent, especially in a general office environment where staff use computers for many administrative tasks. The power of computers can make a simple miss-click very damaging."

More Information

Hong Kong Baptist University leaks applicants' data
Data Leak Disease
Data Leak Disease Spreads to Police?
2008/03 - Why flawed privacy ordinance must be given more teeth

Postbag

<web-link for this article>

We welcome comments from our readers and like to include different viewpoints.

Allan Dyer, Editor

Low Adoption of e-Certs

My own view on why eCerts have not been adopted is that they are just too confusing to the general public. Even IT professionals.

- How to get them
- How to use them
- How to store them

Are all just riddled with complex processes, jargon and confusing instructions.

Compare this ;

> E-Mice Solutions wrote, *"Currently, our practice is to issue e-Cert to the applicant in the storage medium of either floppy disc or File Card. Additionally, applicant may choose to have a copy of e-Cert loaded into his HKID card. We believe that this practice can provide the subscribers, who come from the general public, with the flexibility of deploying the e-Cert according to their own needs. This also allows subscribers restoring their e-Cert from floppy disc or File Card when needed, addressing the danger of losing the private key holding in a single media."*
>
> *"If an applicant wishes to request for the e-Cert to be delivered on his HKID card alone, he may raise such request through a signed e-mail or a signed instruction on the paper application form."*
>
> Thus, there are three options for storing an e-Cert:

	HKID card	File Card

Hardware Standard	ISO 7816	ISO 7816
Driver	PC/SC	PC/SC
Public-Key Cryptography Standard (PKCS)	PKCS#11	PKCS#12
Software	e-Cert Control Manager	e-Cert File Card Utility Program
PIN length	8 numeric digits	16 numeric digits
PIN lockout	Permanent on more than 5 consecutive incorrect PIN tries	none
Private key can be exported?	No	Yes

to the alternative method on offer

Your Signature________________________________

And I think you'll see the problem.

As long as it involves effort and an understanding of IT jargon it will never be widely used.

Ralph Magro
Director, STFS

More Information

The Hongkong Post eCert and the State of Digital Signatures in Hong Kong

Great Firewall extended to Green Dam, to Protect Nation's Youth

<web-link for this article>

From July 1st, computer vendors in Mainland China will be required to install, or provide on CD-ROM, "Green Dam Youth Escort", a program claimed to block sites with pornographic content. The software is designed by Jinhui Computer System Engineering, which won a government tender for the project last year. The software detects pornographic images by comparing them to a database of sample porn. Bryan Zhang, the general manager of the company said that it blocks only sites with pornographic content, and parents can turn it off.

However, despite the reassurances, commentators have expressed concern that this is an extension of China's censorship of the internet. Speaking to the BBC, Charles Mok of the Internet Society speculated that the Chinese Government was getting worried by more sophisticated internet users bypassing the "Great Firewall" by using circumvention software. He argued that the specification of one particular software suggested censorship was the true aim; other jurisdictions such as France or Australia merely require ISPs to provide a choice of certified software.

Whether or not the software censors additional content at the moment, the fact that it prevents the use of proxies or other circumvention mechanisms would make it more difficult to bypass the "Great Firewall" when it is active. Having a large user-base dependant on a centrally-managed blocking list would allow the Chinese Government to quickly change which sites were accessible in future, perhaps in response to "sensitive dates".

Under the "One Country, Two Systems" policy, the legislation does not affect Hong Kong or Macau.

12th June 2009

Bryan Zhang, the general manager of Jinhui, has said that his company's deal with the Chinese Government is just commercial, not linked with wider censorship, and the government wouldn't need to use his software to block access to non-pornographic content.

A report in Computerworld Hong Kong stated that, on 10th June, banned websites, such as those of Free Tibet and the Falun Gong spiritual movement, could still be accessed in China through a virtual private network with the porn filtering software running. This casts doubt on earlier reports, including ours above, that indicated Green Dam prevented the use of proxies and other circumvention mechanisms.

Phelim Kine, an Asia researcher for New York-based Human Rights Watch, said that the danger still exists that the program could be updated to block new content in the future. However, the reasons for thinking this is an attempt to increase Government censorship control look increasingly weak. Chinese computer buyers will get the software free, pre-installed with a one-year license, after that they will need to renew the license with Jinhui. There doesn't appear to be any barrier to uninstalling it, so, if a new update did start blocking sensitive sites, users could let the license lapse. The case looks more like genuine concern about pornography linked to an anti-competitive software deal.

15th June 2009 More Confusion over Green Dam

A new report in Computerworld Hong Kong suggests that Green Dam does block access to sites referring to the Falun Gong and "evil Jiang Zemin," according to research by the University of Michigan.

This directly contradicts an earlier Computerworld Hong Kong report by the same reporter, Owen Fletcher, that said, "Web sites usually banned in the country, such as those of Free Tibet and the Falun Gong spiritual movement, could still be accessed in China through a virtual private network with the porn filtering software running on Wednesday." Mr Fletcher did not provide any possible explanations for the different findings, or even note that the difference with his earlier report existed. Bryan Zhang said that he was unaware Green Dam's keyword blacklist included non-pornographic terms.

Yui Kee's Chief Consultant commented, "The possibilities at the moment are confusing: who is attempting to smear who, or is it a comedy of errors? Further details about the tests would help - can the results be repeated? Perhaps the results reflect different testing methodologies - use of proxies or the precise terms used or sites visited. Maybe different versions of the blocklists were used, or the results vary according to location. Unfortunately, clearing up the confusion is not to the advantage of either Beijing, or Beijing's critics - everyone can believe what they want, according to their prejudices."

More Information

China defends screening software
China defends screening software
China demands new PCs have Web site-blocking program
China's computers at hacking risk
Chinese developer surprised by backlash to porn filter
China wants parental control of all PCs
Pressure group demands UK apes China net filter plan
China's porn filter blocks Falun Gong sites; could turn PCs into botnets
China's Green Dam blocks more than sex – OpenNet
Cracks in China censorware patched

Related Articles

Forget Secret Questions

<web-link for this article>

Researchers at Microsoft have published a paper on the security of personal questions used a backup passwords. They asked participants to answer the questions used by the biggest webmail providers: AOL, Google, Microsoft, and Yahoo!, and then asked acquaintances of the participants to guess the answers. The acquaintances were able to guess 17% of the answers. The participants forgot 20% of their own answers within six months. 13% of the answers could be guessed within five attempts by guessing the most popular answers of other participants.

So, these 'secret questions' are not secure, and they don't do the job. Commentators, including Bruce Schneier and Allan Dyer have pointed out perceived weaknesses of these schemes before, but it is good to see some actual research on the issue.

More Information

It's no secret: Measuring the security and reliability of authentication via 'secret' questions
The curse of the secret question
Questioning Password Resets

Goodbye OneCare, Hello Morro - Can Microsoft Get AV Right?

<web-link for this article>

Microsoft is preparing to release a new anti-virus program, code-named "Morro", by September 2009. A limited beta will be available from 23rd June to users in Israel and Brazil, followed by China in mid-July. Microsoft has announced that "Morro" will be free and released as Microsoft Security Essentials. Microsoft's current consumer anti-virus product, Windows Live OneCare, will be discontinued this month, though definition updates and support will continue for existing customers through the life of their subscriptions.

Microsoft also currently offers two other anti-virus programs: Forefront, for business users, and the Malicious Software Removal Tool, free and aimed at removing the most common malware.

Reaction has been mixed, competitor Symantec criticised its capabilities, "Morro is essentially a stripped-down version of Microsoft's failed OneCare product. It didn't offer adequate protection when it was payware, and it offers even less as freeware," said Dave Cole, senior director of product management at Symantec. Some readers at were more enthusiastic, commenting, "I cant wait to get rid of my 3rd party AV".

David Coursey at ComputerWorld Hong Kong noted that Morro would, "route all the URLs you want to visit by Microsoft first for a check against known malware sites", but this feature was not described in quite the same way in Microsoft's press release, or on other sites. If this URL blocking is a feature, maybe Microsoft is planning to compete with Jinhui Computer System Engineering for the Chinese Government youth protection tender?

Microsoft has a history of not taking the anti-virus marketplace by storm, long before Morro, OneCare, Forefront and the Malicious Software Removal Tool, Microsoft bundled "Microsoft Anti-Virus" (MSAV) free with MS-DOS 6, it was widely regarded as the worst anti-virus software available, and Microsoft quickly discontinued updates.

More Information

Windows Malicious Software Removal Tool
Microsoft's free antivirus: Is this an apology?

Symantec director criticizes Microsoft's new anti-virus 'Morro'
Microsoft Announces Plans for No-Cost Consumer Security Offering
Microsoft 'Morro' Nears Beta With New Name
Great Firewall extended to Green Dam, to Protect Nation's Youth
icrosoft Security Essentials Antivirus Software (Codename: Morro) Available on June 23rd
Microsoft's Morro: What We Know
Microsoft's Morro: Does It Stand a Chance?
Microsoft Forefront
Malicious Software Removal Tool
Microsoft Security Essentials
Microsoft set to beta Microsoft Security Essentials June 23
Exclusive: Microsoft's new Anti-Virus, 'Morro', revealed
Windows Live OneCare

ATM Malware Steals Card Details

<web-link for this article>

Security researchers at SpiderLabs, a computer forensics research centre in London and a part of Trustwave, a computer security firm, have uncovered a 50-kilobyte piece of malware disguised as a legitimate Windows program called lsass.exe in Russian and Ukrainian ATM machines. The malware recognises when a “trigger” card is inserted, and uses the machine’s receipt printer to produce a list of all the debit card numbers used that day, including their start and expiry dates – and their PINs. In some cases, it may allow the machine’s banknote storage cassette to be ejected.

SpiderLabs was asked to investigate when a banking group from eastern Europe noted a rise in levels of card cloning and strange ATM behaviour across its branches.

Installing the software would require physical access to inside the ATM. Along with the fact that the printed list of card details is encrypted, it points to the existence of a highly-organised gang, including bank staff, programmers, and low-level, untrusted members who visit the machines.

SpiderLabs found multiple variants and speculated that new variants might be worms: able to utilise the trusted, encrypted bank network to spread from machine to machine. SpiderLabs also said that it had evidence the scheme was being distributed to other parts of the world, but would not reveal what that evidence was.

More Information

ATM Cash Machine Malware Spyware To Spew Out Card Details
ATM Attacks Cash-In on Vulnerable E-Life
ATM Malware Continues to Spread
ATM Malware Surfaces as Hackers Target Banks in Eastern Europe

Dangerous - The Time To Exploit a Singer's Death

<web-link for this article>

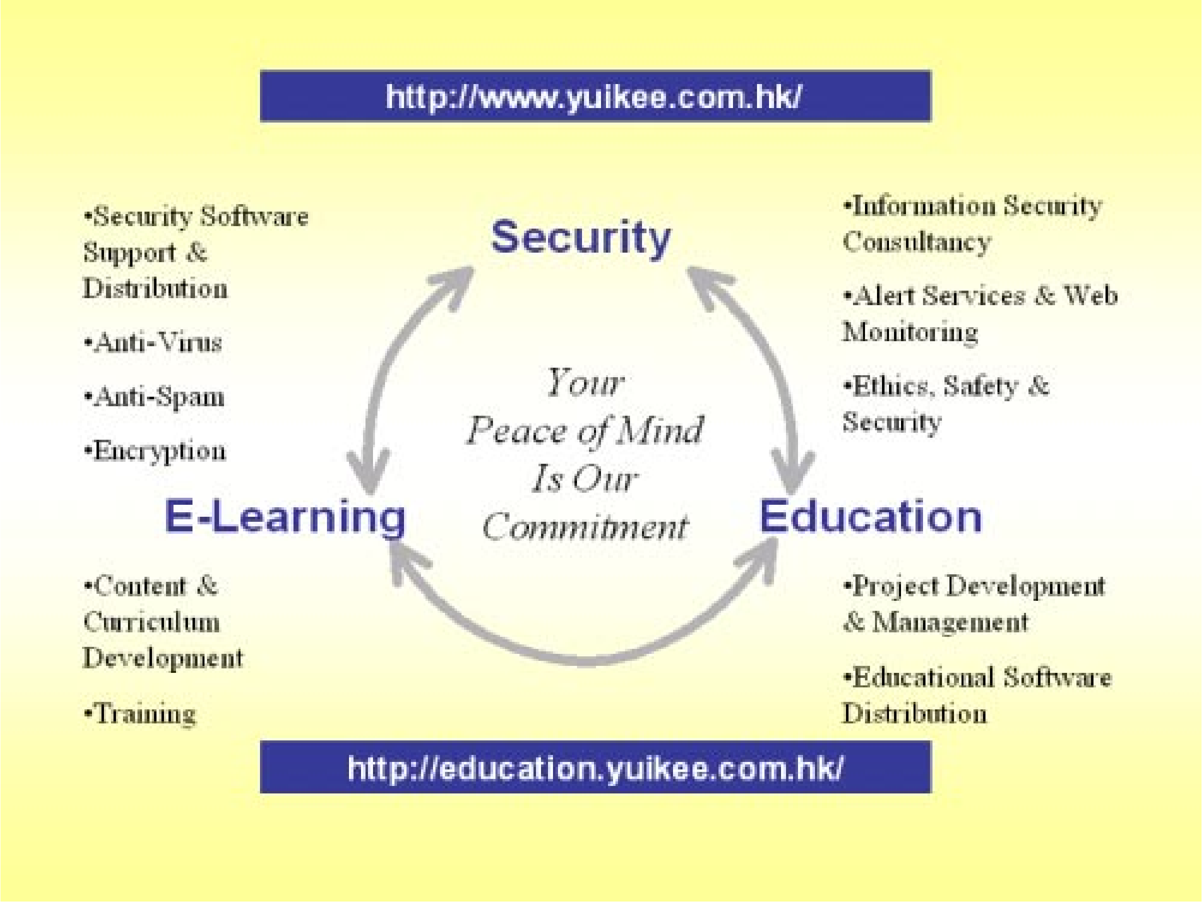
Allan Dyer

Michael Jackson died at 2009/06/25 21:26 GMT, the first email about his death, with a fake YouTube link to malware arrive in my mailbox 2009/06/26 04:09 GMT. A delay of less than 7 hours. Arrival of second email: 04:32. Perhaps the number of fake messages, and the speed of their arrival is giving us a new measure of the significance of media events.

Farewell, Michael Jackson. Everyone else, don't get fooled by fake emails.

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/