
Yui Kee Computing Ltd.

# Newsletter

March 2006

## Contents



## Editor's Notes

The major theme for March is personal data and spying. Since the revelation that confidential details of 20,000 police complaints were available on the Internet there seems to be no end of further revelations of mishandling of personal data.

An interesting aspect of the US laptop thefts is that the data included Social Security Numbers. It is common practice for these unique identifiers to be used whenever convenient, opening the door for identity theft. Hong Kong readers will notice the similarity to the HKID number, which is often mis-used as a default password (e.g. for activating credit cards or accessing websites).

The news of an unpatched Internet Explorer vulnerability that is being actively exploited is also of critical concern.

## Incident Update

Thu Mar 2 17:16:22 2006 FSC: First J2ME virus found 4
Mon Mar 6 13:16:22 2006 CA: Win32.Lovgate.AB Medium
Wed Mar 29 07:31:09 2006 CA: Win32.Mytob.X Medium

## IE Exploit

A critical vulnerability in Internet Explorer that is being actively exploited by malicious websites and emails is still unpatched after more than a week. Microsoft says that a cumulative security update to fix the problem, "is on schedule to be released as part of the April security updates on April 11, 2006, or sooner as warranted".

The bad guys appear to have been reading the Microsoft advisory, which tries to downplay the seriousness of the vulnerability, saying it, “could not be exploited automatically through e-mail messages … Customers would have to click on a link that would take them to a malicious Web site…”. Some of the exploit attempts are using excerpts from actual BBC news stories and offer a link to "Read More". Naturally, the link leads to a fake site that looks like the BBC site but which contains the TextRange exploit.

Users should disable Active Scripting in Internet Explorer, or use another browser.

More information:

http://www.hkcert.org/salert/english/s060324_msie_createtextrange.html

http://secunia.com/advisories/18680/

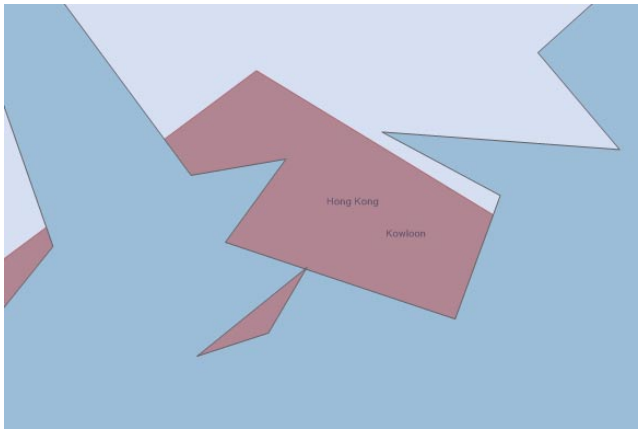
http://www.frsirt.com/english/advisories/2006/1050

http://www.microsoft.com/technet/security/advisory/917077.mspx

http://www.theregister.com/2006/03/31/ie_exploit_bbc_bait/

http://www.kb.cert.org/vuls/id/876678

# World Virus Map




F-Secure has launched a comprehensive online tool for everybody interested in understanding the world virus situation at a glance. The resource, which was developed for research purposes at F-Secure is now available to the general public in four languages, respectively English, French, German and Finnish.

Visitors to the above addresses will first see the full world map situation but will quickly be able to drill down for information based on a geographical area or country.

Colour representations of infection levels from quiet to epidemic give the viewer an immediate overview of a country or region. Another measure enables the viewer to understand virus alert levels from an overall global perspective.

Related graphs and statistics help users to understand the broader context of the infection based upon time lines ranging from the last hour to the last year as well as a breakdown of the viruses in question.

Speaking about the new resource, Mikko Hypponen, Chief Research Officer at F-Secure said, "The world virus map is an excellent resource for quickly understanding the virus situation at any given time. For anybody interested in understanding the 'bigger picture' behind a virus in the news and charting its course, this is a good place to start."

The resource also offers a unique perspective on Hong Kong, as can be seen from the map above. Obviously, the map reflects the future shape of Hong Kong, when the harbour reclamation is complete.

More information:

http://worldmap.f-secure.com/vwweb_1_2/en/

http://worldmap.f-secure.com/vwweb_1_2/vwm/map/clen/de200606000/ds200605900/dt3/gnhk/ic10/if0/ii0/is2/ly100/ro0/rtpage/zz.html

# Speaking Events

Our Chief Consultant, Allan Dyer, has made a few appearances during March:

| | |
|---|---|
| 17 March 2006: | Spoke at the Legislative Council Panel on Information Technology and Broadcasting about the Proposals to Contain the Problem of Unsolicited Electronic Messages |
| 20 March 2006: | Briefed the National Information Security Center of Japan |
| 27 March 2006: | Panelist at the Telecoms InfoTechnology Forum, "e-Security in the Broadband Age" |

# Sophos Moves to Five Minute Anti-Spam Updates

In a recent notice to customers, Sophos has announced that their flagship gateway security product, PureMessage for Unix, will have data updates published every five minutes, four times more frequently than previously. The data updates will change to being incremental: instead of downloading the entire anti-spam data package for each update, only changes since the last update will be downloaded.

This change brings the anti-spam data currency into line with that of the anti-virus data, which moved to five minute updates in January 2006. These changes require no action on the part of PureMessage 5.x customers.

# IPCC Data Leak

*Allan Dyer*

The front page of the Government's InfoSec website informs us, "Information Security is Everybody's Business", but it appears that the message is not getting through. The leak of highly confidential data about complaints against the Police from the Independent Police Complaints Council (IPCC) is a dramatic demonstration of failure.

David Webb, editor of webb-site.com, an independent site that monitors Hong Kong's corporate and economic governance, discovered and reported the leak, and it has been covered in detail in the Hong Kong press. This brief summary is for overseas readers and is based on what has been revealed so far. It should be noted that the investigation is ongoing: About three years ago, the IPCC engaged a contractor to work on the data that the IPCC receives from the Complaints Against Police Office (CAPO). The contractor delegated the job to a sub-contractor, who requested test data. The IPCC provided the sub-contractor with data on 20,000 real cases. The sub-contractor transferred the data to a site on the Internet, so that he could work on the data elsewhere. On 9th March 2006, David Webb was using Google to search for a property address when he stumbled on the data. He quickly realised the significance of the data and decided to report it to an independent body with investigatory powers, the Independent Commission Against Corruption, and to the press. Since then, a number of other leaks of personal data (from an insurance company and a phone company) have been revealed.

How could this happen? The Government has extensive guidelines on information security, the Privacy Commissioner has even run T.V. adverts to educate everyone about the importance of personal data privacy, and the IPCC itself, on its' website includes, "Strict observance of the code of confidentiality" in its' values. Perhaps they are using "observance" to mean "watching" instead of "conformance to"?

In addition to the obvious questions about respect for and care of personal data, I would like the underlying issues to be addressed:

- The IPCC is a small organisation, with less than 20 members and without dedicated IT staff. There are many other similar bodies, how can their IT needs be met safely and securely?
- The Government has detailed guidelines on information security, which were, presumably, available to the IPCC. Perhaps one reason they were not followed was because they are too detailed, and therefore look like a technical IT document that the organisation's executive just passed on. Would a much shorter policy document be more effective at informing executives about their responsibilities?
- Many Government contracts are awarded to large companies, probably because they are seen as having an established reputation, and a size to take responsibility. However, in this case, the contractor has distanced itself from the actions of the sub-contractor. Do the supposed benefits of contracting to large companies really exist if they routinely delegate the work to either their junior staff or sub-contractors, without sufficient oversight and monitoring?
- The current appearance is that IPCC staff made the biggest blunder, when they sent real data in response to a request for test data. However, surely it was clear to the sub-contractor that the data received was real, not test? Someone might make up a handful of fictitious names and cases, but not 20,000 fully-detailed records.

Loosing confidentiality is a one-way process: there is no way of recalling the data from general circulation, or erasing details from the minds of people who have seen it. However, the Government should make its' best efforts to minimise the adverse effects on those affected, and to provide compensation where appropriate.

## Learning the Wrong Lessons

Naturally, there is a lot of discussion about the incident, but not all of it addresses the core issues. At a local security conference I was told, "this would not have happened if they had been using <*cool new security product*>". In fact, almost any security product could have prevented the leak, but the failure was that no–one recognised that security was required.

Mr Ken Ng, the Managing Director of EDPS, also provided some examples, in my opinion, while speaking at the ISSG Special Forum: One concerned protecting data appropriately on ftp sites… by using a username and password – doesn't he know ftp is an insecure protocol, the passwords are sent in–the–clear! Another came when Mr Ng reported that his company's current practice was to always deploy staff on-site, because of the dangers. This seems to be a knee-jerk over-reaction – encryption technology can protect data in transit and in storage, so a blanket rule is unnecessary. It might also lead to other risks being over-looked, and it will probably increase costs. Security is not a one-size-fits-all proposition, the particular circumstances, the threats and the sensitivity should be taken into account.

## Conclusion

Looking to the future, I hope that this case awakens everyone to the importance of personal data, and their responsibilities towards it. This case it probably the tip of the iceberg, there are almost certainly far more cases of breech of confidentiality of personal data waiting to be found. The Privacy Commissioner needs some teeth, and everyone needs to realise the importance of information security.

More information:

http://www.scmp.com/ (Registration required)

http://webb-site.com/articles/IPCC.htm

http://www.pco.org.hk/english/infocentre/press_20060313.html

http://www.theregister.com/2006/03/28/hk_data_leak_rumpus/

http://www.hkcs.org.hk/en_hk/doc_event/HKCS_ISSG_Forum31_03_06_2_.pdf

http://www.ipcc.gov.hk/

http://www.infosec.gov.hk/

http://flagrantharbour.com/?p=198

http://www.thestandard.com.hk/news_detail.asp?pp_cat=11&art_id=15337&sid=7266549&con_type=1

# Ernst & Young Leaked Customers Data from Five Lost Laptops

The accounting firm Ernst & Young has recently lost five laptops containing confidential data. An Ernst & Young spokesman has confirmed that one laptop had tens of thousands of Sun, Cisco, IBM and BP staff data, including their ages, social security numbers, tax identification numbers and addresses. Ernst & Young continues to maintain that the laptop poses little risk, as it was password protected.

Jeff Moran, the husband of an IBM worker told of the data breach commented, "Ernst & Young has a policy that this type of information is not supposed to be on a laptop, yet these guys download the data because it's convenient for them."

Password protection would be trivial to bypass, unless the actual data was encrypted.

More information:

http://www.theregister.com/2006/02/25/ernst_young_mcnealy/

http://www.theregister.com/2006/02/26/ey_laptops/

http://www.theregister.com/2006/03/04/ey_letters/

http://www.theregister.com/2006/03/15/ernstyoung_ibm_laptop/

http://www.theregister.com/2006/03/23/ey_bp_laptop/

http://www.theregister.com/2006/03/30/ey_nokia_lapop/

# Fidelity Joined the Lost Laptop Party, Leaked HP Staff Data

A laptop lost by Fidelity Investments has exposed 196,000 current and former HP employees. Apparently, Fidelity loaded the data onto a laptop in order to support discussions for a meeting at HP, during which Fidelity demonstrated a new software product they believed would assist HP in addressing some administrative issues related to the HP retirement plans.

More information:

http://www.theregister.com/2006/03/22/fidelity_laptop_hp/

http://www.theregister.com/2006/03/24/hp_fidelity_laptop/

# Thai Spy Company Challenges Finnish AV's "Trojan" Evaluation

F-Secure, the Finnish Anti-Virus developer, have classified a commercial product, FlexiSPY, produced by the Thai company Vervata, as the first Ttojan spy for Symbian Phones. Vervata has challenged this assessment:

> "FlexiSPY is not a Trojan, nor a virus and does not require the purchase of F-Secure Mobile Anti-virus products to remove it. An uninstall option is provided for the user, so the application can be removed at any time. Configuration settings are also available to allow frequency of connections, thereby allowing the user to minimise network connections to once daily if required."

However, they fail to note that the "user" they refer to is the purchaser of the spy program (Vervata is quite clear that the product is intended for spying), who has a special code to access a hidden user interface.

The product records details of all voice call and SMS information, and then later sends those details to the FlexiSpy server, where the purchaser can access them. So, personal data would be collected without authorisation, and stored on a third-party's system (probably in Thailand). F-Secure notes, "spying on people's private communication is illegal in most countries around the world", including Hong Kong.

More information:

http://www.f-secure.com/weblog/archives/archive-032006.html#00000844

http://www.theregister.com/2006/03/30/flexispy/

http://www.f-secure.com/v-descs/flexispy_a.shtml

# Domain Name Registrars are not Protecting Consumers

Phishers often use domain names that are similar to a well-known bank's name, so F-Secure decided to look into the number of domains that mimic banks. Mikko Hypponen reports that the number is, "Well, lots."

Mikko asks, "When someone in, say, Nigeria wants to register a domain name that starts with the name of a well known bank, why are the registrars so willing to let them register it?"

Some registrars do have reasonable rules, for example, the Hong Kong Domain Name Registration Company Limited (HKDNR) restricts third level domain names:

- .idv.hk for individuals of age 11 or above with HKID card
- .com.hk for commercial entities with valid business registrations
- .net.hk for network service providers with PNET licenses
- .org.hk for non-profit making organizations
- .edu.hk for tertiary institutions and schools
- .gov.hk for government entities

So, whatever domain names are issued within these, the user has some assurance that there is an identifiable entity in Hong Kong to hold responsible. However, HKDNR's policy for second-level domain names (.hk) is that no documentary proof is required in general (though applications for domain name consisting of or containing a reference to words like 'bank', 'insurance' or 'assurance' will require additional documents issued by relevant authorities). Is this sufficient? Some banks do not use the work "bank" in their name (the HSBC is an obvious, local example), so possibilities for deception still exist.

More information:

http://www.f-secure.com/weblog/archives/archive-032006.html#00000845

https://www.hkdnr.hk/instructions/new_domain.html

http://www.hkdnr.hk/eng/faq/2ld.html

http://www.hkdnr.hk/eng/faq/new_reg.html#5

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/