Yui Kee Computing Ltd.

# Newsletter

December 2011

## Contents

Contents ..... 1
Strong Pan-Democrat Result in IT Subsector ..... 1
2011 Review ..... 2
- Identification and Authentication ..... 2
- Social Engineering and User Education ..... 3
- Malware ..... 3
- Government ..... 3
- DDoS ..... 3
- AVAR Conference ..... 4

## Strong Pan-Democrat Result in IT Subsector

*<web-link for this article>*

The 2011 Election Committee Subsector Elections took place on 11th December and pan-democrat candidates won the most seats.

In the confusing area of Hong Kong politics, the top politician is the Chief Executive and the election for Hong Kong's third Chief Executive will take place on 25th March 2012. Instead of being directly elected, the Chief Executive is elected by 1200 people who are members of the Election Committee. The Election Committee is, itself, elected by members of the Functional Constituencies and it was these elections that occurred on 11th December. Each Functional Constituency represents an industry or special-interest group, such as Finance, Medical, Religious etc. The Information Technology Functional Constituency gets to elect 30 members of the Election Committee and there were 61 candidates standing.

Only one candidate declared affiliation with a political party (Sin Chung Kai, Democratic Party), but he was one of a twenty-strong group, IT Voice, that shared a platform of pan-democratic ideals. IT Voice also advocated appointing a Chief Information Security Officer for Hong Kong, and promoting strong information security. All twenty of the IT Voice candidates were elected. A second Group, ICT Energy, fielded twenty-four candidates, many well-known members of IT professional associations, and won eight seats.

The candidate with the most votes was Charles Mok (1466). Just six votes separated the lowest winning candidate (Witman Hung, 605) and the highest loosing candidate (Louis Ma, 599).

The full list of winners is:

- Mok Charles Peter (IT Voice) 1466
- Sin Chung Kai (IT Voice, Democratic Party) 1462
- Bradbeer Robin Sarah (IT Voice) 1121
- Leung Siu Cheong (IT Voice) 1078

- Huang Erwin Steve (IT Voice) 1072
- Soong Tak Kar Chester (IT Voice) 1071
- Fong Po Kiu (IT Voice) 1071
- Yip Yuk Fai (IT Voice) 1053
- Ng Kee Yin Joseph (IT Voice) 1028
- Wong Wai Kay Ricky 1028
- Yau Cho Ki Joe (IT Voice)1026
- Young Wo Sang (IT Voice) 1023
- Tsui Chi Ying (IT Voice) 1010
- Tsang Kin Fung (IT Voice) 999
- Tang Wing On (IT Voice) 979
- Yueng Lam Fat (IT Voice) 970
- Kwan Tak Wah (IT Voice) 956
- Lam Yat Ming (IT Voice) 948
- Mak Chi Lit (IT Voice) 938
- Leung Ho Yin (IT Voice) 926
- Cheng Pan Pan (IT Voice) 922
- Lau Stephen Ka Men (ICT Energy) 760
- Lee Sunny Wai Kwong (ICT Energy) 744
- Wong Kam Fai William (ICT Energy) 723
- Quat Elizabeth (ICT Energy) 709
- Tang Shuk Ming Winnie (iProA) 706
- Mak Tang Pik Yee Agnes (ICT Energy) 694
- Lee Woon Ming Wendy (ICT Energy) 657
- Ho Pui Tak (ICT Energy) 646
- Hung Wai Man Witman (ICT Energy) 605

# 2011 Review

*<web-link for this article>*

*Allan Dyer*

I don't think that 2011 can be characterised as "The Year Of..." anything in information security, there have been incremental changes in many areas, but nothing really outstanding. Perhaps the message is Stay Vigilant.

## Identification and Authentication

We are still searching for new methods of identification and authentication, probably because all our current methods have obvious weaknesses. I discussed some of the weak authentication used in Hong Kong in a November article.

January saw reports of Chinese research into gait identification from pressure pads, but it seems a long way from practical deployment.

In March, I discussed the advantages and disadvantages of SMS authentication. In the same month, ElcomSoft showed that Nikon's Image Authentication System, essentially linking a photo with the camera that took it, is broken.

The extent of problems with SMS authentication became clear with malware including the ZeuS variant Mitmo and the Symbian trojan Spitmo intercepting the authentication codes and sending them to attackers.

## Social Engineering and User Education

The problems of users being tricked into doing things they shouldn't, of course, continue. Calls from fake "support technicians" were highlighted by David Harley in January. The major 11th March earthquake in Japan led to a variety of scams and hoaxes capitalising on the disaster.

The Hong Kong Police tried to address user-based problems by developing internet usage guidelines for their officers. The Council of Europe has a similar internet safety game aimed at children.

## Malware

Microsoft announced the success it had in tackling malware families such as Taterf, Rimecud and Conficker, reducing infection rates by 82% on Windows Vista SP 2. Significantly, this was achieved by turning off Autorun. Remember, starting unidentified software without the user's knowledge is a bad idea.

In August, I discussed the issue of mining bots undermining Bitcoin and since then the price of Bitcoins has dropped still further, making legal Bitcoin mining very uneconomic.

## Government

Botnets are important for criminals in monetising their crimes, but our response is usually limited to disinfecting the endpoints. In April, US authorities controversially took command of the Coreflood botnet when they obtained a court order allowing them to establish a substitute Command and Control system.

In a rather different controversial move, the Chinese Government admitted having a "cyber-army" in May. Whether it is purely defensive, or has offensive capabilities too, was left to speculation. The following month, Chinese military academics compared cyber war to nuclear war and called for a cyber non-proliferation treaty like the Nuclear Non-Proliferation Treaty. The feasibility of this, when, unlike nuclear weapons, anyone with a computer can develop a "cyber weapon", is doubtful. Video footage of apparent Chinese military attack software surfaced in July. The UK and the US both made aggressive announcements on cyber war.

## DDoS

The suspension of the Hong Kong Stock Exchange on 10th August because of a DDoS attack highlighted the dangers of taking a too limited view of which systems are mission critical. The trading systems were not attacked, but the regulatory disclosure website, HKExnews became unavailable, thus creating a situation where some investors might be unaware of information that others knew, triggering the suspension. After the attack, alternative news channels were made available and publicised, allowing greater resilience in future. A Hong Kong businessman was arrested later the same month in connection with the attacks.

Cryptography

Cryptanalysis continues to improve, with weaknesses in AES found.

## AVAR Conference

It was a personal privilege for me to welcome participants to the [fourteenth Ant-Virus Asia Researchers Annual Conference](), held in Hong Kong.


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/