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

Yui Kee Computing Ltd.

Newsletter

September 2016

Contents

Major Anti-Virus Conference in Tianjin

<web-link for this article>

Tianjin Grand Hall

China's National Computer Virus Emergency Response Centre (CVERC) held the **2016 1st International Anti-Virus Conference** on 22 and 23 September in Tianjin. Law enforcement, foreign experts, academics and anti-virus developers spoke to an audience of over two hundred at the Tianjin Grand Hall (天津大礼堂).

The Tianjin Vice Major welcomed the participants and introduced the 600 year old city as a centre for manufacturing and river transport. Lu Ming, the Deputy Director of the State Administration of Foreign Experts Affairs spoke about the importance of information security for the country's development, China's cyber-security framework and the theme of the conference: Sharing, Innovation, Breakthrough. Leaders from the Ministry of Industry and Information Technology and the Office of the Central Leading Group for Cyberspace Affairs explained the size of the problem, its international nature and the need for a multi-pronged approach.

2016 1st International Anti-Virus Conference Stage

Sergey Novikov from Kaspersky Labs classified the problem as a cyber-threat pyramid with three layers. The lowest is garbage and spam, the second is crime and financial fraud and the top layer, only about 1-3% of the total, is nation-sponsored attacks. However, the border between the top two layers is disappearing. He identified Microsoft building a new data-centre just for Windows 10 telemetry as a privacy disaster. Enterprise will see increasing numbers of targetted attacks. Governments will suffer attacks on critical infrastructure, and false flag attacks will be an issue. For protection he advocated, "Education, Education and Education", emphasising the need to educate people, establish processes and implement technology.

Costel Ion from the INTERPOL Global Complex for Innovation (IGCI) in Singapore explained his work in coordinating the identification of cybercrime and criminals and producing actionable reports for national law enforcement agencies. Their major activities include focus on the use of Tor by criminals, Bitcoin analytics and training on the Darknet. Their facilities include a training network of Raspberry Pis to simulate the Darknet.

2016 1st International Anti-Virus Conference Audience

Liu Xinyun, Director of the Network Security Protection Bureau of the Ministry of Public Security (MPS) explained that the conference was a joint effort of the MPS and the Tianjin Municipality. In previous years they had organised a China National conference on anti virus, but this was the first year it had been broadened into a international conference with the aim of strengthening international cooperation. During the G20 conference in Hangzhou they succeeded in arresting several people for cyber attacks. He emphasised the need for public/private cooperation, a rating system for systems and a comprehensive defence system with new standards.

Ni Guangnan (乐华建) of the China Academy of Engineering, but probably best known as the CTO of ICTC, which became Legend and then Lenovo, talked about the billions of global netizens and IoT devices and the publicity week for national cyber-security. Wu Jiangxing, Director of the China National Cyber Switching System Engineering and Technological R&D Centre said that it was impossible to eliminate vulnerabilities, that China was mainly a victim of cyber attacks because of too many backdoors, particularly hardware backdoors.

Allan Dyer, Chairman of the Association of Anti-Virus Asia Researchers, challenged the conference to secure "Layer Eight", asking, "What are we telling users". Frank Law, Superintendent of the Cyber Security Division of the Hong Kong Police revealed that Hong Kong was the 4th most prolific source of phishing attacks worldwide in 2015. He also highlighted the Anonymous Asia DDoS attacks during the 2014 Umbrella Movement and the Police's annual cyber security workshop.

Chen Jianmin, Executive Director of CVERC highlighted the rise of the importance of App security since 2006, with the current App download market reaching 250 billion Yuan this year. Dennis Batchelder, Head of the Anti-Malware Testing Standards Organization, introduced his organisation and the importance of agreed standards for independent testing of solutions.

Other speakers included Qi Xiandong, CEO of Qihoo 360, Ma Bin of Tencent, Holloy Stewart of Microsoft, Lin Xiaodong of BaiDu, Tony Ning of Asiainfo, Igor Zdobnov of Doctor Web Labs, Christopher Covert of Symantec and Paul Robinson of Intel. Many of these speakers highlighted the current rise of ransomware, the difficulties in detecting and preventing it and the difficulties faced by users in China in obtaining Bitcoins to pay the ransoms.

The second day of the conference split into two streams: Network Threat Management and Mobile Applications.

Ransomed to Death

<web-link for this article>

Allan Dyer

In *The Adventures of Huckleberry Finn* by Mark Twain, Tom Sawyer and his gang of boys have decided to take up a life of adventure, becoming highwaymen, capturing their victims and ransoming them. But they encounter a problem, none of them know what ransom means:

> *"Well I don't know. But per'aps if we keep them till they're ransomed, it means that we keep them till they're dead."*

The prospects for their endeavour are dim and nothing comes of it.

Perhaps the ransomware that plagues our computers today is about to fall to a similar misunderstanding. I will make a bold prediction, that perhaps will haunt me in years to come: **2016 is the year of Peak Ransomware**. I don't mean that ransomware will disappear entirely, just that the prevalence and the money made from ransomware will be at its highest this year.

Malicious software that demanded a ransom has a long history, starting with the AIDS diskette in 1989. The idea of using public key cryptography emerged in 1996 but it was the utilisation of Bitcoins for untraceable payments that led to the current epidemic of ransomware that started in 2013. The criminals that started the trend knew their business, they were successful because:

1. Victims were unprepared.
2. Strong, public key cryptography made the data inaccessible without the key.
3. Bitcoins made the payments essentially untraceable.
4. The criminals valued their reputation and provided "customer" support (F-Secure has a fascinating review of ransomware customer support services).

Therefore, victims could only get their files back by paying and catching the criminals was unlikely. However, if the victim paid, then they would get the help they needed to recover their data, so paying the ransom was a viable way out for many victims.

What has changed?

1. Criminals that don't understand the business model have entered the "market":
   - Some ransomware has predictable or crackable keys, so decryptor tools are available.
   - Fake ransomware that just trashes the victim's files before demanding a ransom has emerged.
2. INTERPOL and police forces are endeavouring to analyse Bitcoin transactions.

Victims therefore see more chance of data recovery without paying the ransom, and the possibility of not getting their data after paying, so fewer victims will pay. The lazy and incompetent criminals ruin the reputation of the competent criminals too, reducing their profits. Add the threat that the police might soon trace the transactions, and smart criminals will be abandoning ransomware and looking for new opportunities. The remaining ransomware will deteriorate in quality.

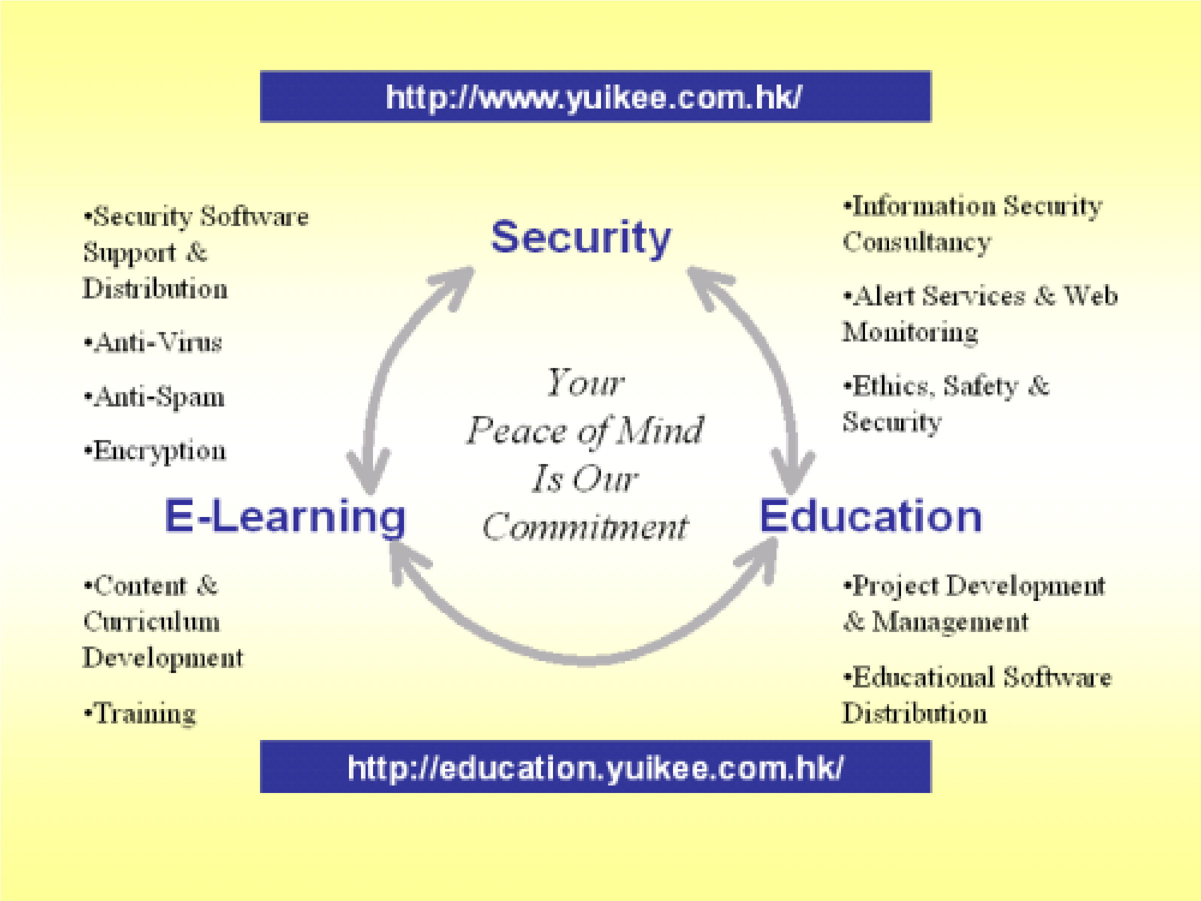
How do you become part of the victory over ransomware? Take regular **backups**! With recent, offline backups to rely on, you can laugh at the ransom demand.

More Information

- AIDS (Trojan horse)
- Got Ransomware? Negotiate

- List of free Ransomware Decryptor Tools to unlock files

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 Software Support & Distribution
•Anti-Virus
•Anti-Spam
•Encryption
Security
•Information Security Consultancy
•Alert Services & Web Monitoring
•Ethics, Safety & Security
Your Peace of Mind Is Our Commitment
E-Learning
Education
•Content & Curriculum Development
•Training
•Project Development & Management
•Educational Software Distribution
http://education.yuikee.com.hk/