Yui Kee Computing Ltd.

Newsletter

May 2011

Contents

Through The Wild Web Wood Game Review

<web-link for this article>

"Through the Wild Web Woods" is an online internet safety game for children aged 7-10 produced by the Council of Europe. The game uses a simple maze and puzzle format to introduce online security concepts.

Concepts such as privacy, children's rights and awareness are introduced through well-known fairy tale characters, such as Snow White, and suffering children that can be helped by scrolls covering various rights of children. Mini-games and "websites" give practical examples of situations to be aware of, such as websites harvesting visitor's email addresses or strangers asking for personal information in chat rooms.

After completing all the levels of the maze, players can re-play the mini-games, and view information on useful organisations. If all the suffering children have been helped, there is a bonus game. The play is not too difficult, and the games are interesting for a few minutes. The information on rights is described in simple terms, but might still be too abstract for the intended audience. In one place, a dialogue popped up with the close button under the map icon, making it impossible to close the dialogue and proceed. The only workaround was to restart the level, and position the character slightly differently so that the dialogue appeared in a different location, without the close button obscured.

The Council of Europe has done well to produce this resource in a form that children can access. There is an online teaching guide to support the game.

More Information

Through the Wild Web Woods

Defensive or Offensive, Beijing has Genius Cyber-Army

<web-link for this article>

Beijing has, for the first time, admitted that it has an internet security army, which it says is defensive. Speaking at a regular press briefing, Colonel Geng Yansheng said that China is still relatively weak in internet security protection and increasing the ability to safeguard online security is an important exercise for the military.

The admission came when Colonel Geng was asked about the offensive capabilities of a thirty-strong "blue team" that Guangzhou Military Region had spent tens of millions of yuan (millions of US dollars) equipping, reported in the People's Liberation Army Daily in April. The "blue team" is reported to have engaged in exercises to attack multiple targets with techniques such as computer viruses, junk messages and infiltration to steal an enemy's sensitive data. However, Colonel Geng downplayed the exercises, saying, "This is just a training program based on our needs" and "The Blue Army's main target is self-defence. We won't initiate an attack on anyone".

However, retired major general Xu Guangyu said that blue meant offensive in mainland military jargon. He also commented that, with the world's largest number of internet users, the army is looking for talented recruits to train professionally, and they are "all geniuses".

These statements will do nothing to confirm or quell the rumours of Chinese cyber-aggression. Some analysts claim that China is orchestrating a vast army of hackers that infiltrate established western economies to disrupt business with DoS attacks and conduct cyber-espionage. Last year, Symantec found that more than a quarter of all attempts to steal sensitive corporate data "originated" in China, and intelligence sources claim that these are State-sponsored. Conversely, this could be seen as evidence of the poor level of online security in China, with millions of novice broadband users not realising their machines are infected.

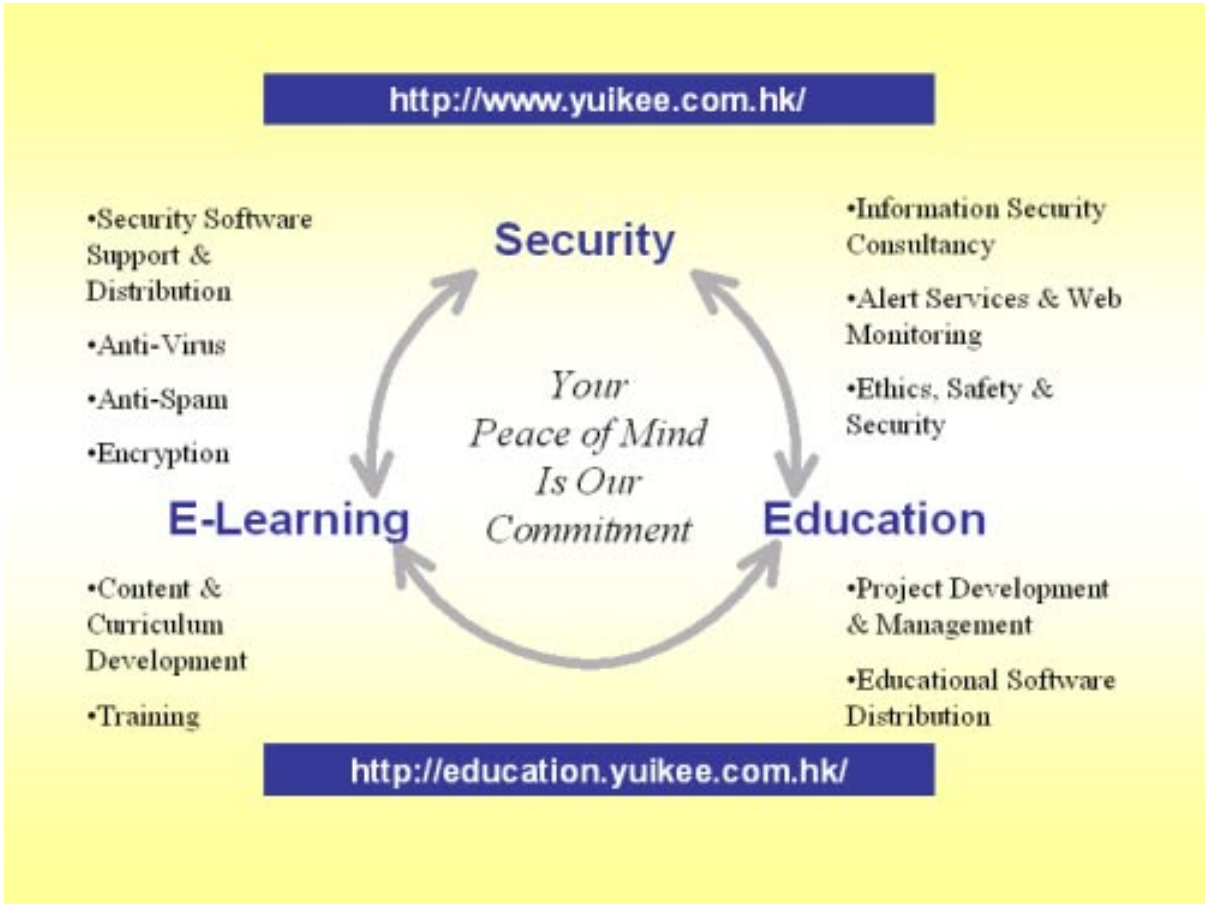
China is not the only country suspected to have an offensive cyber-warefare capability. Last year's Stuxnet worm was seen as a State-sponsored attack on Iranian nuclear capabilities, with the backer variously identified as the USA, Israel, Germany or others, and Russia has been accused of cyber-warfare in Estonia and Georgia. One of the main attractions of cyber-warfare for Governments must be the plausible deniability.

More Information

"Cyber blue team" established to safeguard Internet security: Defense ministry spokesman
Military experts share views on “cyber defense” and national defense
PLA creates cyber-defense program
China Acknowledges Existence of Cyberwarfare Unit
China establishes cyber PLA
China's Blue Army of 30 computer experts could deploy cyber warfare on foreign powers
Malware: The Anti-Personnel Mine of Cyberwar
Collateral Damage in Someone's Cyberwar
Critical Questions on Critical Infrastructure

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
Education
•Content & Curriculum Development
•Training
•Project Development & Management
•Educational Software Distribution
http://education.yuikee.com.hk/