Yui Kee Computing Ltd.

# Newsletter

August 2009

## Contents



## Criminals Love Social Networking

*<web-link for this article>*

The hugely popular social networking sites like Facebook and Twitter have become attractive targets for phishing and scamming attacks as online criminals follow the latest Internet trends that are attracting the most users.

The latest criminal action against social networking sites including Facebook and Twitter was reported by the F-Secure Response Lab on Friday. Pro-Georgia blogger Cyxymu's accounts were targeted by a widespread DDoS (distributed denial of service) attack, causing millions of users of Facebook and Twitter to experience problems with the sites slowing down or being completely offline on Friday.

F-Secure advises that separate passwords for e-mail and social networking are an essential precaution.

Mikko Hyppönen, Chief Research Officer at F-Secure says: "Although this attack was targeted at a specific person, it affected the whole community. We may never know who was behind the Cyxymu attack, however they had access to significant bandwidth." However, other commentators have cast doubt on whether Cyxymu was the target, Rob Rosenberger of VMyths tweeted, '*@Cyxymu speculated Russia ordered Twitter/FB attacks ... and the media reported it as a "fact."*'.

Nevertheless, communication through Facebook is all about personal connections and communities of friends. It involves a high level of trust. When you receive a message on your Wall from one of your Facebook friends, it's very different to receiving an anonymous e-mail or spam message. It is precisely this trusted environment – and the 250 million users – that makes Facebook such a tempting target for criminals. Phishing and financial scams are based on creating a false sense of trust with the target of the attack, enabling the criminals to gain access to valuable information or direct financial gain.

Sean Sullivan, Security Advisor at F-Secure says: "Weak passwords provide a common way for criminals to hack into social networking sites. Their aim is to harvest contact lists, phone numbers and other information which they can sell to spammers or use in targeted attacks to make money."

The damage caused by a hacked Facebook account is all the greater if the same password is also used for the user's e-mail account. This means the criminals can easily reset all the user's online passwords, get information about banking details and find answers to security challenge questions. Sometimes the answers to personal security questions, for example middle names, house addresses and pets' names, can even be found directly on Facebook.

"As the Facebook user name consists of an e-mail address, it is essential that different passwords are used for logging into personal e-mail accounts and for logging into Facebook and other social networking sites. It's also a good idea to have different primary e-mail, business e-mail, social network e-mail accounts," Sullivan advises.

This year there has been a series of bogus messages on Facebook from "friends" asking for financial help. Facebook users should always treat such requests with caution and make a thorough identity check before sending any money, even when the messages appear to come from a family member or other trusted person.

"There is also a positive security aspect to the social networking sites. Unlike classic e-mail scams like chain letters which can run for years, the wisdom of the networked Facebook crowd means that users can quickly become aware of the latest security threats. The community is good for publicizing useful security information and for taking rapid self-corrective action against security vulnerabilities," says Sullivan.

F-Secure's Tips for safer social networking

- ALWAYS have separate and secure passwords for your e-mail and social networking sites.
- If you become aware of a Facebook security problem, post about it on your Wall so the community can take preventive action.
- Pick your friends wisely and have a security guru among your friends!
- If you are on Facebook, Fan the "F-Secure" page to get the latest news

**More Information**

Why are criminals targeting Facebook and other social networking sites?
VMyths: Truth about computer security hysteria
Researchers close in on Twitter suspects

# Li Yizhong Admits Green Dam Directive was a Mistake

*<web-link for this article>*

Li Yizhong, minister of industry and information technology, said that the choice of words in the directive about "Green Dam" was unclear, leading to the misunderstanding that the filtering software had to be installed on all new computers. However schools and internet cafes would still be required to install Green Dam on all computers.

He added that the central government welcomed criticism on Green Dam-Youth Escort software and that Green Dam's developers were improving the software's performance and closing its security loopholes.

The admission has attracted headlines around the world, some saying that the Chinese Government has "backed down" or "dropped" the idea. Some commentators are already anticipating the next version of Green Dam.

**17th August 2009**

In a recent blog post, security guru Bruce Schneier discussed Green Dam, similar "security" initiatives around the world, in countries often regarded as less restrictive, and why such developments are worrisome for anyone who is concerned about freedom and security.

**21st August 2009**

In a further twist to the Green Dam saga, a survey initiated by the China Youth Internet Association claims that over 80 percent of primary school students, aged 6 to 12, don't care about the Green Dam software. However, the South China Morning Post reports that official mainland media claims only 5% of the children were against the software, suggesting that this was giving an unjustified impression of support when only 14% were in favour. The English-language Beijing newspaper China Times reported the story with the headline, "Primary school children shrug off Green Dam escort".

The survey was conducted in recreational centres, residential compounds and parks and questioned over 1,000 children and their parents. The children were questioned separately from their parents, specially-trained interviewers explained what Green Dam is, the reason for it and what pornography is. Almost half of the parents said they would not install Green Dam on their household computers, either because they believed it was ineffective or was disagreeable.

Some critics of the Green Dam software have created a cartoon character, Green Dam Girl, to mock the filtering plan.

**More Information**

Great Firewall extended to Green Dam, to Protect Nation's Youth
China drops Green Dam web filtering system
Green Dam launch 'not handled well': official
China will not enforce Green Dam porn filter plan
China backs down over Green Dam internet monitoring software
Green dambusters
Building in Surveillance
Anger in China over web censorship
The "Green Dam Girl" – Netizens Spoof the Censorship Software
Primary school children shrug off Green Dam escort

# Return of the Macro Virus: Watch Out AutoCAD Users

*<web-link for this article>*

Sophos Senior Threat Researcher Paul Baccas has recently encountered two viruses that target AutoCAD: AL/Utax-A and AL/Logo-A. AutoCAD viruses were reported in 2005, but there has been little activity since. However, AL/Utax-A in particular shows malicious intent: creating new users.

Most anti-virus software has been updated to detect the viruses, and the AutoCAD developers, Autodesk are responding.

**More Information**

Autocad attacks return after four years in wilderness
AutoCAD malware: ACAD.VLX
AutoCAD Malicious Code / Virus Alert "acad.vlx" and Solution
AL/Logo-A

# Bot Herders Go Social

*<web-link for this article>*

Jose Nazario, the manager of security research at Arbor Networks, reports finding a Twitter-based botnet command channel. The channel, since shut down by Twitter, uses base64-encoded posts to direct bots to download additional malware from various URLs... helpfully shortened using a url shortening service. Nazario found that the downloaded malware looked like an information stealer.

A basic challenge for bot herders is how they stay in charge of their network of compromised machines, without leaving a trail that law-enforcement can use to locate them. Previous command and control channels have included chat protocols, such as ICQ and IRC. In this case, bots subscribed to the Twitter account by RSS.

Nazario also suspects two other Twitter accounts are being used in the same way, but further analysis is needed to confirm this.

To point out the obvious, any communications channel can be utilised for malicious purposes, and the more popular a method is, the easier it is for the bad guys to hide in the stream of messages.

**More Information**

Twitter-based Botnet Command Channel
Twitter transformed into botnet command channel
Twitter Turned Botherder

# Nigerian 419 Scam Achieves Cult Status

*<web-link for this article>*

The stereotype of unscrupulous email scams originating from Nigeria has achieved some sort of cult status with the appearance of a YouTube video of Prince Obi Matumbe Akumbe making an appeal for help. Various clues suggest this is a joke, including the references to other correspondent's disbelief, and using YouTube for a public appeal, rather than a more "personal" appeal in email. There is also a response from a "victim", and Prince Obi has a twitter account.

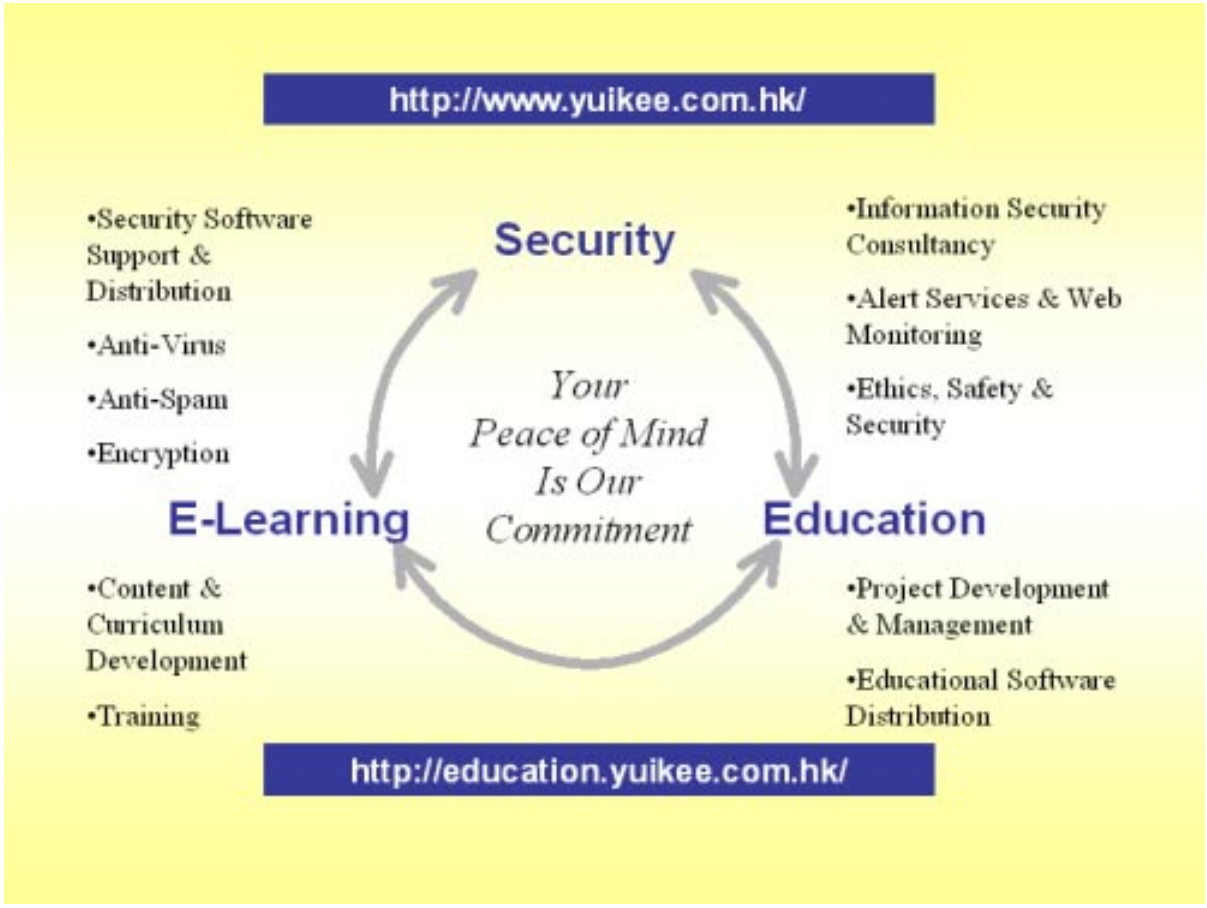
While laughing at these well-produced jokes, people should remember that scammers are using a wide variety of stories to hook victims, and they are certainly not limited to one country.

**More Information**

PRINCE OBI - International Appeal
Lad from Lagos makes YouTube pitch
Prince_Obi (twitter)
JamesAlexanderSmith's Channel

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/