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

Yui Kee Computing Ltd.

Newsletter

November 2007

Contents

Shanghai Observatory Officials Learn the Importance of BCP

<web-link for this article>

Officials at the Shanghai Observatory have decided to buy a backup power system, after a power transmission failure at the Minhang power station in the city left the Observatory's 25-metre antenna blind for 100 minutes on Saturday 27 October. The Observatory was in charge of monitoring the status and data transmission of Chang'e, China's moon probe, though the observatory said no data was lost and the probe's operation was unaffected.

The power failure also affected Metro lines 1, 2 and 4 in the city, and areas near Xujiahui and Longcao Road.

More Information

3 Metro lines resume service after power failure
Blackout at monitoring station

Vendor Launches Anti-Malware Comparison Site

<web-link for this article>

Commtouch Software Ltd., a vendor of email security products, has launched their "Malware Outbreak Center", a website that compares the detection implementation time of 27 anti-virus products against their own detection of the same threat. Products that already detect a threat at the time that Commtouch first detects it are shown as having "zero hour detection".

The site is very interesting for comparing the performance of different anti-virus products, but should not be used to compare those products with Commtouch's products. Firstly, as Commtouch emphasises on its site, its products are specialised for use on email, and they are a complement to, not a replacement for desktop anti-virus products. An email-only tool can look for "things that are not normal in email", rather than the more complicated, "things that might do bad things", so the comparison is not like-for-like. Secondly, as detection by Commtouch is used as the benchmark, no other product can beat Commtouch's score: the best they can do is "zero hour detection", meaning, as good as Commtouch. These two limitations are combined in a third question: what happens if Commtouch gets it "wrong". At the time of writing, the site shows a threat detected by Commtouch on 2nd November 2007 at 07:58 is still undetected by **all** the anti-virus products, after over ten days delay. No information is given about what this "threat" really is, perhaps it is something not normal in email, but not a threat either.

Testing anti-virus software is difficult, and anything that can give users more information to make informed decisions is to be welcomed.

More Information

Malware Outbreak Center
Virus database tracks vendor performance

Beware of the "Man in the Browser"

<web-link for this article>

Finnish information security company F-Secure warns that a technique called "Man in the Browser" is being actively used in an upsurge of bank fraud attacks. The technique intercepts the personal data of bank customers in the browser.

Historically, there has been a trend of increasing sophistication in attacks used by cyber-criminals attempting to steal personal and bank data of internet users. The earliest method was software that was capable of retrieving the data typed into the computer keyboard ("keyloggers"), and then more complex mechanisms arrived on the scene, such as phishing and pharming. Phishing uses emails that the sender disguises to look as if they come from a financial establishment. When the web user clicks on the link contained in the mail, he finds himself on a bogus site that invites him to log into his account. Pharming consists in automatically redirecting the web user to a false site (imitating the site of his bank) when the user wishes to visit the real site, but without the user having to click on a link of any kind, since the usurping of the address takes place at internet level. The "Man in the Middle" technique consists of the cyber-criminal pretending to be the bank's site, intercepting the data passed by the user, and then using that data to access the real bank site to gain access to the account.

The latest technique used for these attacks is known as "Man in the Browser". Once the PC has been infected, the malicious code is only triggered when the web user visits his online bank site. This type of malware is capable of retrieving the information (login and password) that is entered by the web user on the real web page of the bank site by intercepting the HTML code on his web browser. This personal data is then sent directly to an FTP site where the cyber criminal stores it, before selling it on to the highest bidder on other web sites used by cyber-criminals.

Security products using behavioural analysis are the best solution against such attacks, as the malicious code is designed specifically for certain banking sites. They are not distributed en masse, unlike attacks using phishing, for example. This restricted distribution constitutes a real challenge for security software publishers when it comes to referencing these malware and using signature recognition.

"With the enhancements that banks have deployed in terms of authentication security on their online banking sites, phishing attacks are becoming less and less effective, and attacks of the 'Man in the Browser' type are set to increase," says Mikko Hypponen, the Chief Research Officer at F-Secure.

F-Secure security solutions feature behavioural analysis, the dedicated F-Secure Deepguard engine being an example of this.

More Information

F-Secure Informs of an Upsurge in Attacks for Stealing Personal Banking Details

Tor used for Man-in-the-Middle Attacks

<web-link for this article>

Following last month's news of Dan Egerstad's collection of POP3 and IMAP passwords using a sniffer on a Tor exit node, MW-Blog has found evidence that malicious Tor exit nodes are being used for Man-in-the-Middle attacks on SSL sessions.

The researcher accessed a known SSL server via a variety of Tor exit nodes and looked the SSL certificates received "via" different nodes. One node, in Germany, provided a fake certificate. It was reported to the German authorities, and the node is no longer available. However, this highlights the potential for abuse of the Tor technology.

More Information

MW-Blog » Blog Archive » On TOR
MW-Blog » Blog Archive » TOR exit-node doing MITM attacks
MW-Blog
Testing TOR Nodes for Man-in-the-Middle Attacks
Anonymity and Secrecy: Why Sin Chung Kai Should Apologise

Tenth AVAR Conference in Seoul Discusses Changing Threats

<web-link for this article>

The Association of Anti-Virus Asia Researchers tenth international conference was held in Seoul, Korea on 28thth November, with 219 participants from around the world. In his keynote speech, Vincent Weafer (Symantec) reminded us of the changing threat landscape. Previously, we saw increasing involvement in malware from criminals looking to make a financial gain, now the trend is towards small attacks with small gains - if they make enough of them, they still get the same amount of loot. Vincent also warned us that our current testing methods are failing to keep up.

Several papers looked at the threats in online games. Igor Muttik (McAfee) looked at massively multiplayer online role-playing games (MMORPGs or MMOGs) including World of Warcraft, Lineage, Second Life and Club Penguin. Because of the time and effort spent by players acquiring them, virtual possessions have a real value, and, naturally, criminals try to take advantage of that. There are large numbers of data stealing trojans, phishing attacks and viruses targeting games. The games also bring their own vulnerabilities, many games allow players to write their own game objects in the game's own scripting language. The scripts may be run on the client or server, Igor analysed the potential dangers, and the restrictions necessary to make these environments safer. Second Life has even seen a virtual terrorist attack. Deokyoung Jung and Howoong Lee (AhnLab) also looked at online games, describing hacking of the games.

Another theme was detection strategies. Amir Lev (Commtouch) discussed server-side polymorphic malware, and blocking these attacks by identifying patterns in email and cross-referencing with additional data. Itshak (Tsahi) Carmona (CA) discussed generic detection. Mario Vuksan (Bit9) looked at the complement of the detection problem: false positives.

Crime was never far from the agenda, Eugene Kaspersky (Kaspersky Lab) discussed the trends in cybercrime: botnets, bank attacks, DOS attacks, ransomware, MMORPG attacks and social networking.

A couple of papers picked up on the testing issued touched on in Vincent's keynote. David Harley (author & consultant) and Andrew Lee (ESET) looked at the difficulties

More Information

AVAR International Conference in Seoul
Is Hong Kong's new Anti-Spam Law Effective?

Is HK Ready for Phase 2 of the UEMO?

<web-link for this article>

The second phase of the Unsolicited Electronic Messages Ordinance (UEMO) will come into effect on the 22nd December but not all Hong Kong's company's and organisations have adapted to the requirements yet.

Some organisations appear to have reviewed and improved their procedures, for example, for several years the mailing list of the Hong Kong Institute of Marketing has had a broken unsubscribe mechanism - using the provided link would return a webpage reporting that the recipient had been unsubscribed, but the messages did not stop. However, in a recent posting, the unsubscribe procedure had changed, and it appears to have been effective. Did HKIM check and fix this as a result of the UEMO, or is this a coincidence? Either way, it is an improvement.

Unfortunately, other organisations seem less well prepared. HSBC uses email to send promotional messages to customers who have provided their email address. The messages appear to fail to comply with some supplementary rules issued by OFTA. Commercial email messages are required to include the sender's name, address, telephone number and email address, HSBC does not include their address. The unsubscribe mechanism involves calling the bank's "Direct Financial Services Hotline" at a number listed in the message, where bank staff ask for personal information, such as HK ID card number and account numbers, in order to verify that the person calling is the owner of the account(s) that the email address is linked to. This does not comply with OFTA's rules because they say that the unsubscribe mechanism must be reachable from the device used to read the message. Also, the hotline reports that processing the unsubscribe request takes 4 to 6 weeks, longer than the 10 days required by the UEMO. Ironically, the promotional message also states, "HSBC will never contact you by email or otherwise to ask you to validate personal information such as your user ID, password or account numbers. If you receive such a request, please call our Direct Financial Services hotline on...", yet, in order to unsubscribe, they instruct customers to call a number provided in the email, where the customer will be asked for HK ID number and account numbers. Are they unaware that a criminal could send fake messages with a different phone number, and ask customer who call for these important details? Why hasn't the HKMA issued guidelines forbidding banks from requestion sensitive data by phone? In summary, the HSBC marketing email appears to fail to comply with the UEMO rules in these ways:

The address of HSBC is not included

It is not possible to unsubscribe from a computer

The unsubscribe mechanism is not easy to use

The unsubscription takes more than 10 days

With less than four weeks until phase 2 comes into force, there is very little time for companies to fix problems like these.

More Information

L.N. 108 of 2007 Unsolicited Electronic Messages Regulation

Unsubscription Information

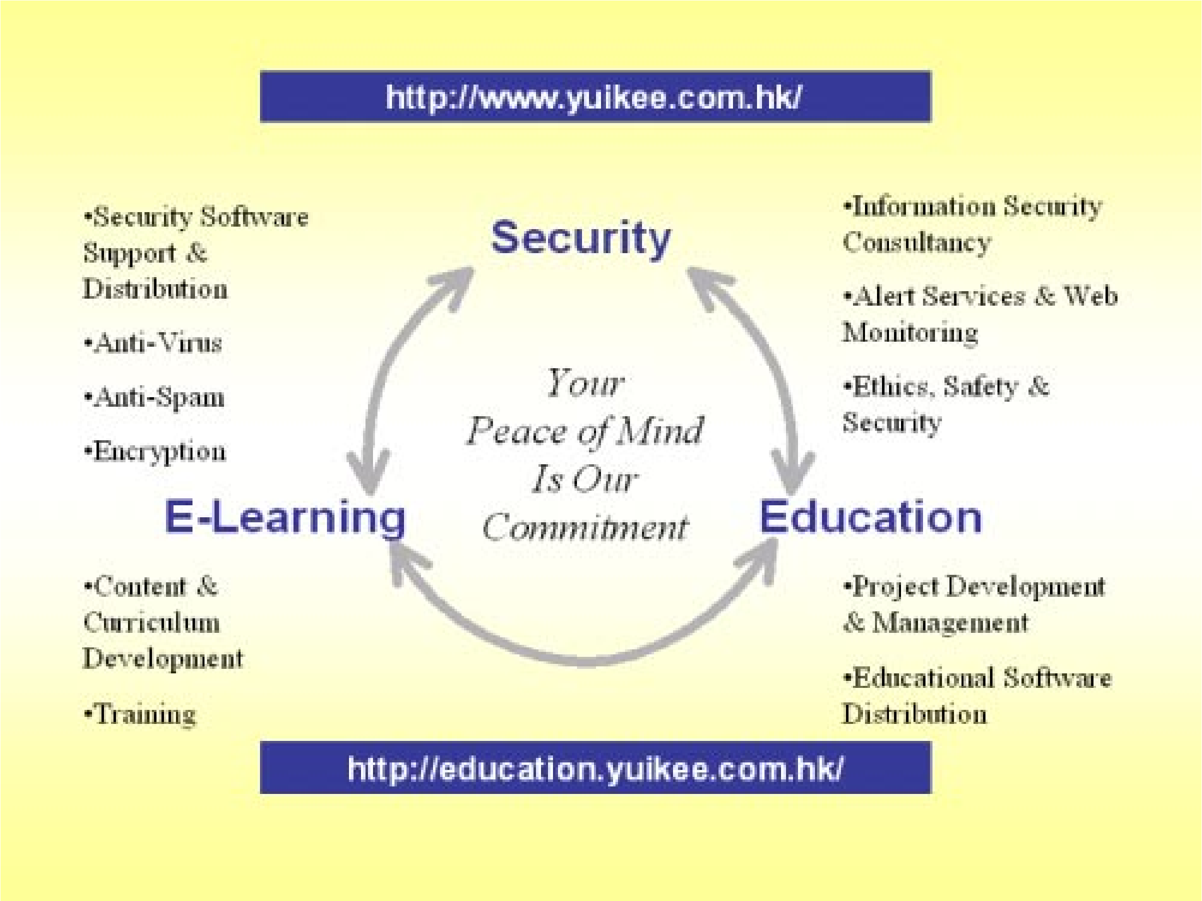
To subscribe, send an email to Maiser@yuikee.com.hk with subscribe newsletter in the message body. The Subject can be anything. Send the subscription email now. If successful, you will receive a welcome message.

To unsubscribe, send an email to Maiser@yuikee.com.hk with unsubscribe newsletter in the message body. The Subject can be anything. Send the unsubscription email now. If successful, you will receive a farewell message.

You can only subscribe or unsubscribe the address you are emailing from. If you need to add or remove another address from the list (eg. you have changed email addresses and want to unsubscribe the old address), or you have any other problems concerning the operation of the list, please contact the Postmaster.

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

- Content & Curriculum Development
- Training

Education

- Project Development & Management
- Educational Software Distribution

http://education.yuikee.com.hk/