Yui Kee Computing Ltd.

Newsletter

November 2013

Contents

AVAR 2013 Conference Preview

<web-link for this article>

The 16th Association of Anti-Virus Asia Researchers (AVAR) International Conference 2013 will be held in Chennai, Tamilnadu, India. The AVAR Conference is the largest Asia Pacific conference on anti-malware. It has previously been held in Japan, China, Australia and this year it returns to India for the second time.

The conference runs from the 4th to 7th of December, 2013, starting with the Welcome Reception on Wednesday evening to the post-conference city tours on Saturday. The keynote speech is by Dennis Batchelder, Partner Program Manager at the Microsoft Malware Protection Centre.

The speeches cover a wide variety of topics, here they are grouped into a somewhat arbitary classification:

Testing and Cooperation

- "Real World Testing", Peter Stelzhammer, Philippe Rodlach, AV-Comparatives
- "The Real Time Threat List", Righard Zwienenberg, ESET, Philipp Wolf, Avira
- "CMX: Clean File Metadata Exchange System", Igor Muttik, McAfee & Mark Kennedy, Symantec

Analysis and Intelligence

- "Top Asia-Pacific cyber threats based on DNS data analysis", Erik Wu, Nominum
- "In-depth analysis of Cutwail botnet", Dragos Gavrilut, Cristina Vatamanu, Razvan Benchea, Octav Minea, Alexandru Maximciuc, Doina Cosova, Bitdefender

- "Automated Malware (mis) Classification & Challenges", Rajesh Nikam, Quick Heal Technologies Pvt. Ltd.
- "Are you ready for Game-rue" , Hrushikesh Kalburgi & Jyotsna Jain, Quick Heal Technologies Pvt. Ltd.
- "Hey Android, are you Frightened of FakeAV plus Ransomware", Rowland Yu, SophosLab

Detection and Removal

- "From DNA sequence variation to NET bits and bobs", Andrei Saygo, Eoin Ward, Mathieu Létourneau, Microsoft
- "Generic System Cure", Tsahi Carmona & Alex Polischuk, Total Defense Inc.
- "Antivirus UltraSound Your Baby Is A Breach Detection System", Randy Abrams, NSS Labs
- "More Sand than Box", Gregory Panakkal, K7 Computing
- "Mobile Web Reputation: Addressing Evolving Mobile Threats", Paul J.S. Oliveria, Trend Micro

Social, Business and Surveillance

- "The Social Media Connection", Righard Zwienenberg, ESET
- "Death of a Salesforce whatever happened to anti-virus", David Harley, ESET & Larry Bridwell
- "Hiding from the Big Brother", Evgeny Kolotinsky, Kirill Blazhennov, Kaspersky Lab

Cloud

- "Security from the Cloud - How Big Data Helps Us Protect You", Benjamin S. Rivera, Trend Micro
- "Fast data delivery from a clouds", Lukas Hasik, Petr Chytil, AVAST

The line-up has a lot to offer anyone involved in protecting their organisation against information security threats, and specialists in the anti-malware field.

Formerly called Madras, Chennai is on the Coromandel coast of southern India. Chennai has a rich heritage and is one of the prettiest metropolitan cities in India, mixing the elegance of the past with the vibrancy of today. Also referred to as "the Gateway to the South India" and the "Cultural Capital of South India", the Institute of Competitiveness declared it the most liveable city in India.

Conference details and registration can be found on the Chennai 2013 section of the AVAR website.

More Information

AVAR 2013 : Chennai

Fake ANZ Bank Website Warning

<web-link for this article>

The Hong Kong Monetary Authority (HKMA) has warned about a fraudulent website with the domain name "http://xzxtys.com/zl/secure.anz.com.htm". The website mimics the official website of Australia and New Zealand Banking Group Limited (ANZ). ANZ has no connection with the fraudulent website.

At the time of writing, the registration of the xzxtys.com has been revoked. The domain was registered in January 2013, supposedly by ChunJian Wang of XuZhou in China.

The Hong Kong Police are investigating, anyone who has entered information on the website or used it for financial transactions should contact ANZ at 2176 8888 and any local police station or the Commercial Crime Bureau of the Hong Kong Police Force at 2860 5012.

More Information

Fraudulent website: http://xzxtys.com/zl/secure.anz.com.htm

Fraudulent Emails Sent from Hong Kong Treasury Account

<web-link for this article>

The Treasury of Hong Kong has warned that fraudulent emails were sent from their email account ra@try.gov.hk, and that a document attached to the emails contained "computer viruses". The Treasury claims it has no connection with the emails. The Police are investigating.

Yui Kee Chief Consultant Allan Dyer commented, "It is well-known that email messages are trivial to spoof, sending a message that has any arbitrary address in the From: field is easy, but the Government press release specifically says the messages were sent from their email account. This, and the Police investigation, seem to indicate that Government computers were used to send the messages, so this might be an extremely serious security breach. Hopefully, this is just sloppy writing by a non-technical press officer".

More Information

Alert issued on fake emails

OFCA Ignores Evidence of Wrongdoing

<web-link for this article>

Under the UEMO, generating electronic addresses by automated processes to send a commercial electronic message is an offence punishable by up to 5 years jail and a fine of up to HK$1,000,000. However, it is not easy to detect. How do you establish that a company has an automated process? The results are indistinguishable from manual collection methods, unless the addresses generated have never been used.

On 1st March 2013, Yui Kee's mailserver received over thirty messages, all advertising the services of "BL Consultants Company Limited", sent to different addresses. Most of the messages were sent to admin or enquiry at a .com.hk domain that Yui Kee administers, the rest were sent to other addresses in the yuikee.com.hk domain. The domains where the admin and enquiry mailboxes were targeted are used for websites, and are defined with a domain mailbox. Thus, the email addresses that were targeted had never been published or used. It appeared likely that the sender had taken two common mailbox names, admin and enquiry, and merged them with a list of .com.hk domain names.

The messages were reported to the Office of the Communications Authority (OFCA) as contravening the Unsolicited Electronic Messaging Ordinance, which prohibits generating electronic addresses by automated processes to send a commercial electronic message.

On 27th September 2013, OFCA reported its findings:

> We have approached the sender concerned for investigation. The sender replied that your 19 email addresses in question were manually collected from public websites by its staff during the past years. Meanwhile, we do not have sufficient evidence to prove the allegation that the sender had used automated means to generate electronic addresses that contravened Part 3 of the Ordinance.

Yui Kee responded:

> You report that the sender concerned in the captioned cases claimed to have collected the addresses from public websites. Please note that most of the addresses, all those with the 'admin' and 'enquiry' username, have NEVER been published anywhere.
>
> ...
>
> The sender concerned is therefore lying, and you should ask them to show you the public websites where they found those addresses. I hope that you take a very serious view on senders lying to you to avoid the provisions of the UEMO.

On 18th October, OFCA replied:

> As explained in our letter dated 27 Sep 2013, we do not have sufficient evidence to substantiate the allegation that the sender has used automated means to generate electronic addresses that contravened Part 3 of the UEMO. In this regard, we could not proceed further on the case.

Yui Kee responded:

> As for evidence, you have the statement of a Hong Kong resident, myself, that most of the addresses have not published. Against this, you say you have a statement from the sender that they collected the addresses manually online. Investigators, of course, do not merely wait for evidence to drop into their laps, they actively make enquiries to gather further evidence. You have not indicated that you have investigated to corroborate or disprove those statements. Two obvious routes for investigation would be to ask the sender for details of where the addresses were found, or the process used by their staff to find addresses, and to search for the addresses yourself.

Yui Kee also asked some questions, OFCA replied, making reference to a document available on the OFCA website, Enforcement Statistics of UEMO. The questions, answers and statistics are combined here in a readable form:

1. Have you conducted enquires to corroborate or disprove the statements by myself and the sender? What were they?

   We will enforce the UEMO in accordance with a due process and we do not have sufficient evidence to substantiate the allegations.

2. What, in your view, would be sufficient evidence to substantiate a claim of address generation?

   We will enforce the UEMO in accordance with a due process and we do not have sufficient evidence to substantiate the allegations.

3. Since the introduction of the UEMO, in how many cases was address generation alleged?

   Please note that we do not have statistics for a particular allegation, such as address generation.

4. What are your standard procedures for investigation when address generation is alleged?

   We will enforce the UEMO in accordance with a due process and we do not have sufficient evidence to substantiate the allegations.

5. How many cases of address generation have been prosecuted?

   Zero. Since the UEMO fully commenced on 22 December 2007, there have been no prosecutions for any offence it defines.

6. What other statistics or information can you provide to demonstrate your effectiveness in enforcing the UEMO?

Enforcement Statistics of UEMO. In the 12 months from November 2012 to October 2013, OFCA has dealt with 2540 reports, issuing 87 warning letters and 8 enforcement notices.

Allan Dyer, Yui Kee's Chief Consultant, commented, "The receipt of the same message at multiple email addresses that have never been used is the *Smoking Gun* for the offence of automated address generation. OFCA should be following up with detailed questioning of the sender and recipient, to establish the veracity of the conflicting claims, and searching for electronic evidence. Instead, OFCA claims it is using 'a due process' without explaining what that process is."

More Information

Enforcement Statistics of Unsolicited Electronic Messages Ordinance (UEMO)

Fake Royal Bank of Scotland Website Shut Down

<web-link for this article>

The Hong Kong Monetary Authority (HKMA) has issued an alert about a fraudulent website with the domain name "http://www.rbsfx.co.uk". The website copied the official website of The Royal Bank of Scotland PLC (RBS), the bank has no connection with the fraudulent website.

At the time of writing, the registration of the rbsfx.co.uk has been revoked. The domain was registered on 11th November 2013 at the popular GoDaddy registrar, using obviously fake contact information.

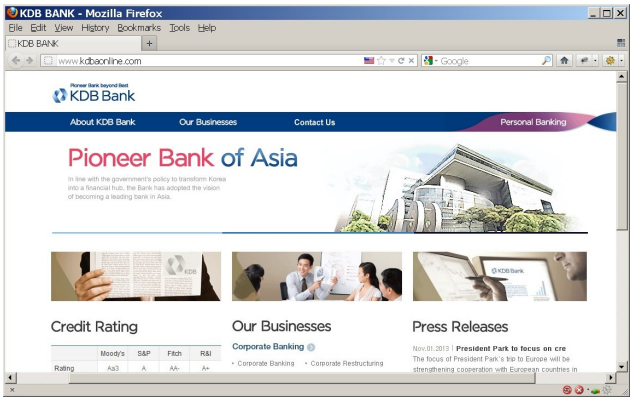
The Police are investigating and anyone who has provided information to the website or conducted financial transactions through it should contact RBS at 3988 7050 and any local police station or the Commercial Crime Bureau of the Hong Kong Police Force at 2860 5012.

More Information

Warning issued on bogus website
Fraudulent website: http://www.rbsfx.co.uk

HKMA Warns About Fake Korea Development Bank Website

<web-link for this article>



The Hong Kong Monetary Authority (HKMA) has issued a warning about a fraudulent website with the domain name "www.kdbaonline.com". The website copies the official website of Korea Development Bank (KDB) but the bank has no connection with the fraudulent website.

The kdbaonline.com domain name was registered in July 2013, supposedly by Rick Iwinsom of Lagos, Nigeria. The website was still active at the time of writing and hosted at SingleHop, a Chicago-based hosting company.

The Hong Kong Police are investigating and anyone who has provided personal information to the website or has conducted any financial transactions through the website should contact

KDB Asia Limited at 2524 7011 and any local police station or the Commercial Crime Bureau of the Hong Kong Police Force at 2860 5012.

More Information

Fraudulent website: www.kdbaonline.com
Alert issued on sham website

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/