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

Yui Kee Computing Ltd.

Newsletter

March 2013

Contents

ACMA Warns Groupon about Multi-List Subscribes

<web-link for this article>

Online retail company Groupon Australia Pty Ltd has been formally warned by the Australian Communications and Media Authority (ACMA) for misleading practices in sending email newsletters to subscribers. If Groupon fails to comply, the ACMA can fine it up to Australian $1 million (over $8 million HKD) per day.

Individuals who provided an email address to Groupon were subscribed to multiple newsletters, but, if they tried to unsubscribe, they would be removed from only one of the lists. The ACMA was of the opinion that it is not "informed consent" if it is unclear what individuals are signing up to and that it was reasonable for individuals to expect they would be unsubscribed from all newsletters unless they were advised otherwise. The ACMA also found that some unsubscribe requests were not acted on within the statutory 5 days.

Yui Kee's Chief Consultant Allan Dyer reflected on the situation in Hong Kong, "Some Hong Kong-based mailing lists appear to share a common infrastructure, based on the mail headers and unsubscribe links, but there is no transparency about the organisations behind them, or how address lists are shared. It might be easy for a Hong Kong email marketer to continue to send messages to an address while appearing to comply with Hong Kong's anti-spam law."

With this in mind, Yui Kee contacted the Office of the Communications Authority (OFCA) with these questions:

> Does OFCA regard the practice of signing customers to multiple newsletters, but only offering the chance to unsubscribe one by one as a contravention of the UEMO?
>
> Does OFCA have any system to detect when companies are doing this?
>
> Does OFCA have any statistics on the prevalence of this practice in

> Hong Kong, and has any company been warned or prosecuted for it here?

At the time of writing, no response has been received from OFCA.

Updated: 27th March 2013

OFCA has provided a detailed reply, first emphasising that OFCA's enforcement powers are limited to commercial messages with a Hong Kong link; the full Ordinance is available at the Government Logistics Department website. OFCA continued:

> As refer to the article provided in your email, please be informed that the practice is not applicable to Hong Kong as the unsubscribe request under section 9(4) of the UEMO is sender based. Under the UEMO, Hong Kong has adopted an opt-out regime under which senders are not required to get prior consent from the recipients before the sending of CEMs. Having said that, senders are required to comply with the requirements of the UEMO when sending CEMs in particular the rules stipulated in Part 2 of the UEMO. Section 9 of the UEMO stipulates that CEMs must contain unsubscribe facility and subsection (4)(a) defines "unsubscirbe request" as a message to the effect that the registered user of the electronic address to which the message is sent does not wish to receive, at that electronic address, any further commercial electronic messages from or authorized by that individual or organization. Section 10 of the UEMO further stipulates that CEMs must not be sent after unsubscribe request is sent by using the designated unsubscribe facility provided in the message, subsections (2)(a) and (b) also state that the individual or organization shall cease sending or authorizing the sending of any CEMs to that electronic address in respect of which the unsubscribe request was sent within 10 working days.
>
> As the UEMO adopts a different approach in the regulation on the sending of commercial emails, we do not maintain any system to detect the practice under your mentioned criteria, nor do we have any statistics in this respect. If you are interested in our enforcement statistics, you may visit our website at http://www.ofca.gov.hk/en/media_focus/data_statistics/figures/index.html.

Since the commencement of the UEMO in December 2008, OFCA (and its predecessor, OFTA) have issued 525 warning letters, 17 enforcement notices and zero prosecutions.

Dyer asked for further clarification:

> You state that unsubscribe requests under the UEMO are sender based. I would like to clarify the full meaning of sender because it has a direct and important consequence for marketing companies in Hong Kong. You state that an unsubscribe request is a message to the effect that the recipient does not want to receive further messages, "from or authorized by that individual or organization". From this, it appears that the originator of a message and the agent authorised to actually send the message on their behalf are both covered by a single unsubscribe request.
>
> This has various consequences, which it will be easier to discuss with an example. Suppose company A specialises in providing email marketing services, and they work for three clients X, Y and Z who wish

to promote their different products. Client X authorises A to send me a message, and I reply to A with an unsubscribe request. Then:

i. As A is the sender, A must not send further messages to me, even if they are authorised by Y or Z.

ii. As X authorised the message, X must not send further messages to me, whether directly or through another agent (e.g. rival marketing company B). Therefore, A must communicate to X which recipients have unsubscribed.

As I noted in the article, some Hong Kong-based mailing lists appear to share a common infrastructure, so my example is directly relevant to those agents.

1. Has OFCA clearly communicated these responsibilities to Hong Kong organisations?
2. Does OFCA have any system to detect when companies are not fully complying with the transitive nature of unsubscribes?

More Information

Groupon warned by ACMA about its email unsubscribe process
Groupon deal spam slapped by Australian regulator
Hong Kong's Anti-Spam Law Allows Obfuscation of Unsubscribe Information
Unsolicited Electronic Messages Ordinance [pdf]
Enforcement Statistics of Unsolicited Electronic Messages Ordinance (UEMO) [pdf]

Mailing List Management Changes

<web-link for this article>

The administration of this newsletter mailing list is changing. The change affects subscribers who are receiving the newsletter by email, and it changes the commands used to subscribe and unsubscribe.

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

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

We have been using the Ecartis mailing list management software since the retirement of our Netware server, and the Mercury mail server that ran on it, but two things have prompted the retirement of Ecartis. First, it became apparent that Ecartis was not accepting commands that were base64 encoded. This can make it difficult for users of non-Latin character set languages (including Chinese) to subscribe or unsubscribe, depending on their mail client configuration. Second, Ecartis is no longer supported, the development team has gone silent.

Mailman has been chosen as a replacement, it correctly handles base64 encoded commands, is well-supported, and has some improved features.

We are committed to changing over without causing disruption to subscribers, and anticipate no difficulties. However, subscribers can always contact us with their concerns or problems.

More Information

Mailman, the GNU Mailing List Manager

Chief Secretary Visits New Electronic Crime Investigation Centre

<web-link for this article>

Figure 1 Mrs Lam (second left) tours the Electronic Crime Investigation Centre. Photo: news.gov.hk

Highlighting the growing importance of technology crime, Hong Kong's Chief Secretary for Administration, Mrs Carrie Lam, visited the headquarters of the Customs and Excise Department and saw the newly-established Electronic Crime Investigation Centre (ECIC).

The ECIC, set up at a cost of $4 million and located at the Customs Headquarters Building, came into operation early in 2013, although it was originally expected to start work in 2012 with 15 staff. It will strengthen research into technology crime methods, formulate enforcement strategies and procedures for front-line enforcement officers, and conduct digital evidence retrieval and preservation training courses for front-line officers. It will also develop information systems to improve Custom's capability in monitoring and investigating Internet crimes.

Mrs Lam encouraged the staff to continue to provide quality services.

More Information

CS visits Customs and Excise Department
Customs spares no effort in combating illegal activities and protecting consumer rights
Hong Kong tries to stay ahead of the infringers

HKMA Warns of Fraudulent HKMA Email

<web-link for this article>

The Hong Kong Monetary Authority (HKMA) has issued an alert concerning fraudulent emails purporting to be sent by the HKMA from the email account hkma_invoice@hkma.gov.hk. The emails have an attachment that the HKMA says might contain viruses. The HKMA has no connection with the fraudulent emails.

The Hong Kong Police Force is investigating the case, and anyone who has received the email should contact any local Police Station or the Commercial Crime Bureau of the Hong Kong Police Force at 2860 5012.

More Information

Fraudulent emails purporting to be issued by the HKMA

March Hong Kong Honeypot Report

<web-link for this article>

This is the fifteenth monthly report from West Coast Labs's honeypot in Hong Kong, providing some indication of the type and level of malware threat in Hong Kong, but it is only based on a single honeypot, so the conclusions should be treated with caution. The number of attacks has risen since February.

Average Time To Infect: 18 hours ten minutes

The average time to infect is an indication of how long it would be before a vulnerable computer connected to the internet in Hong Kong became infected.

Summary

- Total number of attacks : 37
- 11 are brand new to this honeypot.

Source of Attacks

The following breaks down where these attacks have come from by use of IP geolocation.

18	Japan
5	China
4	Taiwan
3	United States
1	Hong Kong
1	Bangladesh
1	Russia
1	India
1	New Zealand
1	France
1	South Korea

Malware

Checksum (md5)	This month	Previous count	Detection*
14a09a48ad23fe0ea5a180bee8cb750a	4	14	Y (W32/Trojan5.DCW w32/backdoor.zzr , Backdoor.Win32.Rbot.bqj Backdoor.Win32.Rbot.aftu Backdoor.Win32.DsBot.v d , ,)
15965bb88165d1eb06851d8f076130ba	4	21	Y (w32/sdbot.otr , Net-Worm.Win32.Kolab.aefe Backdoor.Win32.Rbot.bqj , ,)
98eb0fdadf8a403c013a8b1882ec986d	2	2	Y (W32/Trojan5.DCW w32/backdoor.zzr , Backdoor.Win32.Rbot.kez Backdoor.Win32.Rbot.aftu , ,)
e3d75d2a41a99c84cacfd926b42ee179	1	0 ***NEW	Y (w32/rahack.a.gen!eldorado , Net-Worm.Win32.Allaple.e , ,)
ec513abb61c99fce74072789bb61bc72	1	1	Y (w32/genbl.ec513abb!olympus , , ,)
b82698a30e07fc71349f06750cae2664	1	8	Y (w32/sdbot.otr , Net-Worm.Win32.Kolab.aefe Backdoor.Win32.Rbot.bqj , ,)
f56dd5d433de134162f9e1a4feb468fb	1	0 ***NEW	Y (w32/virut.7116 , Backdoor.Win32.Rbot.adqd , ,)
865915650a85e7c27cdd11850a13f86e	1	17	Y (w32/sdbot.otr , Net-Worm.Win32.Kolab.aefe Backdoor.Win32.Rbot.bqj , ,)
74e2f7eda0031b1a0e157bebaab3f84f	1	0 ***NEW	Y (w32/virut.7116 w32/virut.7116 , Backdoor.Win32.Rbot.adqd , ,)
3875b6257d4d21d51ec13247ee4c1cdb	2	42	Y (W32/Sdbot.AEFV W32/Malware!44f4 , Backdoor.Win32.Rbot.bni , W32Rbot!I2663.exe ,)
6e2fa9031a05b9649da062c550d14a3d	2	6	Y (w32/sdbot.otr , Net-Worm.Win32.Kolab.aefe Backdoor.Win32.Rbot.bqj , WL-dc1ca4287875927725689f45b31ba338-0 ,)
d0fe93eceb4a8a0235c7f9721dd1773a	1	0 ***NEW	Y (W32/Allaple.H , Net-Worm.Win32.Allaple.e , ,)
f9dc3945bdd7406bd8db06a47963ec14	2	25	Y (W32/Sdbot.OTR , Net-Worm.Win32.Kolab.aefe

			Backdoor.Win32.Rbot.bqj , ,)
ed60aa83836ba6691817a6d8a8b9ae45	1	0 ***NEW	N (w32/virut.7116 , Virus.Win32.Virut.av , ,)
bbb5034e33568e100dd3dadabb5a57e9	1	26	Y (w32/sdbot.otr , Net-Worm.Win32.Kolab.aefe Backdoor.Win32.Rbot.bqj , ,)
33fdb683c37fe3d87a403a5db0cbe821	1	2	Y (w32/sdbot.otr , Net-Worm.Win32.Kolab.aefe Backdoor.Win32.Rbot.bqj , ,)
27e0cb71d5229bf0290590dc9eef70ba	1	3	Y (w32/allaple.h , Trojan.Win32.Genome.rioo Net-Worm.Win32.Allaple.e , ,)
f8815cdca238ad5ab566f05f5a6335a4	1	5	Y (W32/Trojan5.DCW w32/backdoor.zzr , Backdoor.Win32.Rbot.voe Backdoor.Win32.Rbot.aftu , ,)
9b175f5f727bcf1153e1aaf99798556a	1	1	Y (w32/trojan-sml-sdcw!eldorado , Email-Worm.Win32.Updater.j , ,)
1d419d615dbe5a238bbaa569b3829a23	1	12	Y (W32/Trojan5.DCW w32/backdoor.zzr , Backdoor.Win32.Rbot.bqj Backdoor.Win32.Rbot.aftu Backdoor.Win32.DsBot.v d , ,)
5719dfeb7839ee13b41cb8eb99d31125	1	0 ***NEW	N (, , ,) no details available
0a278f8d72e4d3d2d44485764398c84d	1	0 ***NEW	Y (w32/virut.7116 , Backdoor.Win32.Rbot.adqd , ,)
971fc83bef2c493ba22e650fc6fe790d	1	0 ***NEW	N (, , ,) script
b4d9dd3a19e7fdd2211d81983f8e4d75	1	5	Y (w32/allaple.h , Trojan.Win32.Genome.rioo Net-Worm.Win32.Allaple.e , ,)
b429bc5ce3bcd6bfe443fd9f9a0ec625	1	0 ***NEW	Y (, Net-Worm.Win32.Allaple.a , ,)
3a70fc79a5813f04ae415273acacf661	1	0 ***NEW	Y (, Net-Worm.Win32.Allaple.e Virus.Win32.Virut.av , ,)
0f052cf643ba0c3be1dbe3319652516e	1	0 ***NEW	Y (, Net-Worm.Win32.Allaple.b , ,)

Note:

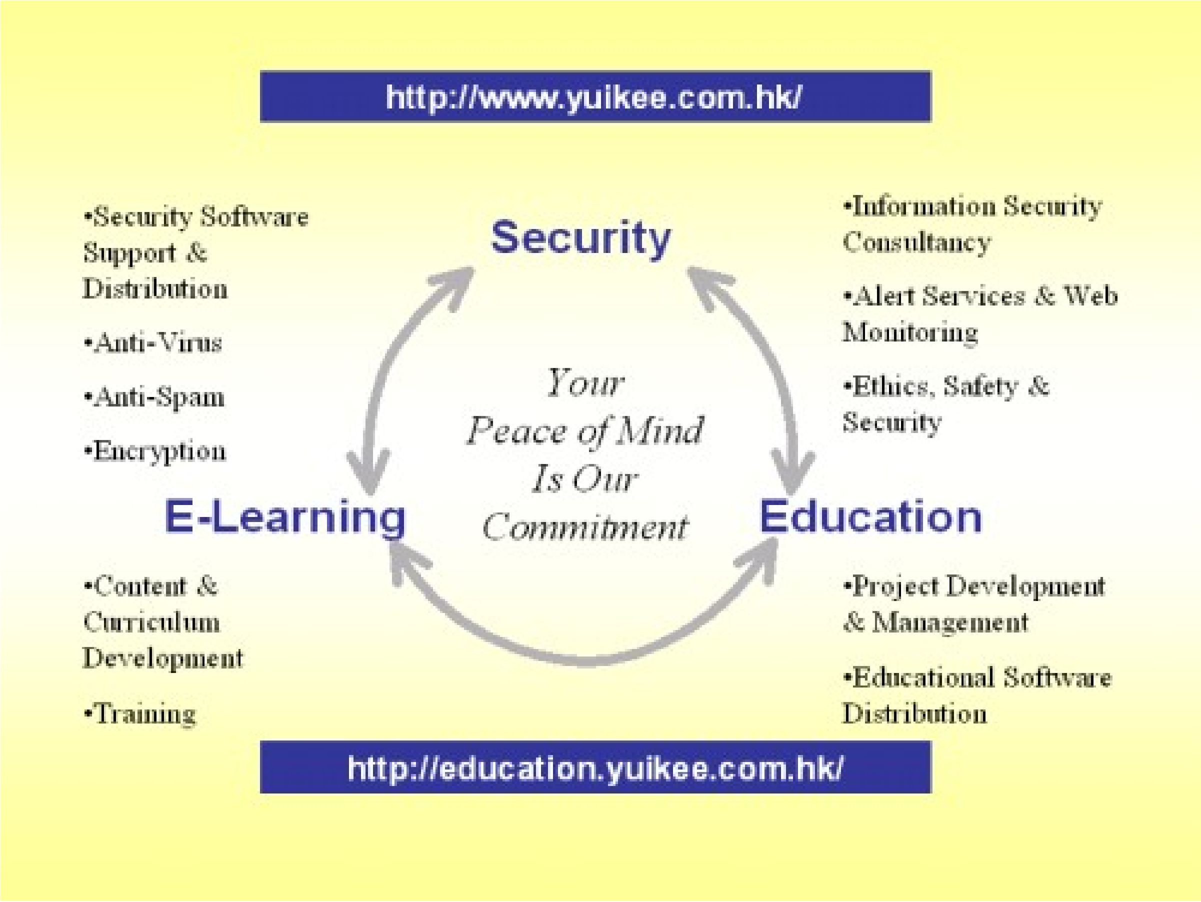
The parameter 'Detection' here relates to whether one or more scanners was able to associate a name with this checksum.

More Information

West Coast Labs
January Hong Kong Honeypot Report

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/