Yui Kee Computing Ltd.

Newsletter

September 2013

Contents

Mis-use and Lack of Clarity of UEMO Opt-Out Deadlines

<web-link for this article>

Over five years after phase 2 of the Unsolicited Electronic Messages Ordinance (UEMO) came into effect, there is still confusion about the unsubscribe rules.

A recent Computerworld article, "Openrice says it's miscommunications, in response to opt-out complaint" demonstrates the confusion. OpenRice is quoted as having an opt-out procedure that takes, "14 working days", but said that a subscription opt-out received on 28 August would be effective on 12 September.

However, Computerworld does not point out that that policy would make OpenRice in contravention of the UEMO, which requires opt-out requests to be effective in "ten working days".

Was the OpenRice staff mis-quoted or mistaken? Perhaps the OpenRice policy is 14 *calendar* days, which is two 5-day working weeks and weekends, to avoid the complexity of adjusting for public holidays? The wording of their response, that it will be "14 days", not "up to 14 days", shows a certain arrogance on the part of OpenRice, that it is their right to continue up to the deadline, even though they could accomplish the removal instantly.

So there are several questions to clarify:

- Is the day of the request counted in the "10 working days"?
- Is a message sent on the 10th working day permitted or forbidden?
- Is Saturday a working day?

If the answers are No, Permitted, No, then OpenRice's effective date of 12 September for a request sent 27 August is a day late, according to the UEMO. Any other answers would make OpenRice's non-compliance worse.

If OFCA is to make the UEMO effective, it must improve public understanding of the rules.

Updated: 25th September 2013

In response to questions from Yui Kee, OFCA clarified the UEMO provisions. In short, for a request sent 27 August, the protection would start on 9 September. For the UEMO, Saturday is a working day. OFCA also point out that if you have ever registered with the sender, their messages may be exempt from the UEMO and not subject to the unsubscribe rules. Yui Kee Chief Consultant Allan Dyer commented, "Registration should not be a one-way process. Giving users the confidence that they can change their minds later encourages them to try out services, to the benefit of responsible companies. This is another area where the UEMO could be improved."

The detail of OFCA's response follows:

> The Communications Authority is empowered to enforce part of the Unsolicited Electronic Messages Ordinance ("the UEMO") which regulates the sending of commercial electronic messages ("CEMs") including pre-recorded telephone messages, short messages, fax and emails. A message will be considered as a "commercial" message if it aims at advertising or promoting services or products, etc. However, some messages are exempted from the UEMO (or part of it). For example, messages to deliver services that the recipient is entitled to receive under the terms of a transaction that the recipient has previously agreed to enter into with the sender are exempted from the sending rules stipulated under Part 2 of the UEMO. As such, if the purpose of a message is to deliver goods or services, including product updates or upgrades, that the recipient is entitled to receive under the terms of a transaction that the recipient has previously agreed to enter into with the sender, such messages will be exempted from Part 2 of the UEMO. A copy of the UEMO can be found in http://www.gld.gov.hk/egazette/pdf/20071122/es1200711229.pdf, the exemptions are under Schedule 1 and the definition of CEM is listed in Section 2.
>
> According to the information from the website of Openrice (http://www.openrice.com/english/registration/register.htm), their members may opt to receive promotional offers during registration. As explained in the previous paragraph, if a person has ever registered with the sender to receive promotional emails or entered into any agreement with the sender, the message sent from the sender may fall into one of the exempted matters; and any further opt-out arrangement may have to refer to the agreed terms and conditions.
>
> On the other hand, if a person has never registered with the sender to receive the promotional messages nor has entered into any agreement with the sender, the promotional message sending is regulated by the UEMO. 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 promotional emails. Having said that, senders are required to comply with the requirements of the UEMO when sending promotional emails in particular the rules stipulated in Part 2 of the UEMO, amongst other things, to provide accurate sender information, to provide unsubscribe facility (i.e. an email address, a web page or a web address) and to honour unsubscribe request made by using the designated unsubscribe facility in the message within 10 working days. Section 2 of the UEMO defines working day as any day other than a public holiday or a black rainstorm warning day or gale warning day within the meaning assigned by section 71(2) of the Interpretation and General Clauses Ordinance (Cap. 1). Generally speaking, if a person has submitted an unsubscribe request by using the designated unsubscribe facility in the message to a sender on 27 August 2013, the law protection will be commenced on 9 September 2013.
>
> Anyone who has never registered with a sender to receive the promotional message and suspects that sender has contravened the UEMO, such as he/she receives promotional email after 10 working days from the date on which he/she made an unsubscribe request, he/she may lodge a report with us. To facilitate our investigation, apart from providing the date of receiving email, receiving email address, the message content and the date of making the unsubscribe request, please provide the email header information for tracing the source of the email as well as the consent to disclose the case information to the sender and the related third party. In fact, all information necessary to our investigation has been clearly listed in the report form (available at http://www.ofca.gov.hk/en/consumer_focus/uemo/how_to_report/index.html). To facilitate the

reporting and our investigation, it is advised to provide the relevant information by filling in the on-line report form.

More Information

Unsolicited Electronic Messages Ordinance [pdf]
How to report a suspected contravention of the UEMO?
Openrice Member Registration
Openrice says it's miscommunications, in response to opt-out complaint
How to know if a message sender contravenes the UEMO?
Is HK Ready for Phase 2 of the UEMO?

Information Security Summit 2013 Approaches

<web-link for this article>

Trust and Privacy in the Cyber Era 2.0; Securing Borderless Data is the theme of the Information Security Summit this year. With a keynote by Mr Graham Ingram, General Manager of AusCERT, the speakers will cover this year's hot topics.

Now in its 11th year, the Information Security Summit is a Regional Event with the aim to give participants from the Asia Pacific region an update on the latest development, trends and status in information security. This year, the main conference takes place on Wednesday 23 October at the InterContinental Grand Stanford Hong Kong, and supporting workshops run from the 21 to 29 at the Hong Kong Productivity Council Building.

Online registration is available at the Information Security Summit website.

More Information

Information Security Summit 2013

September Honeypot Report

<web-link for this article>

This is the twentieth 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 shown a slight increase.

Average Time To Infect: 21 hours 15 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 : 35
- 13 are brand new to this honeypot.

Source of Attacks

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

8	United_States
6	Japan
4	China
3	Ukraine

2	France
1	Hong Kong
1	Puerto Rico
1	Taiwan
1	Canada
1	Argentina
1	Mexico
1	Venezuela
1	Russia
1	Thailand
1	Italy
1	Germany
1	Colombia

Malware

Checksum (md5)	This month	Previous count	Detection*
576368ad34669938fd2f23afd619c26d	1	0 ***NEW	Y (w32/allaple.d , Net-Worm.Win32.Allaple.b , ,)
fd28c5e1c38caa35bf5e1987e6167f4c	1	1	Y (w32/backdoor.zzr W32/Trojan5.DCW , Net-Worm.Win32.Kolabc.dls Backdoor.Win32.Rbot.aftu , ,)
93486e1d652b2325312fb732760da445	1	0 ***NEW	Y (w32/allaple.a.gen!eldorado , Net-Worm.Win32.Allaple.e , ,)
bbb5034e33568e100dd3dadabb5a57e9	1	27	Y (w32/sdbot.otr , Net-Worm.Win32.Kolab.aefe Backdoor.Win32.Rbot.bqj , ,)
62c6067eba03fe066984817f2ef1d5a2	1	0 ***NEW	Y (w32/virut.7116 , Backdoor.Win32.Rbot.adqd , ,)
2fa0e36b36382b74e6e6a437ad664a80	1	2	Y (w32/backdoor.zzr W32/Trojan5.DCW , Backdoor.Win32.Rbot.yqj Backdoor.Win32.Rbot.yol Backdoor.Win32.Rbot.wjd Backdoor.Win32.Rbot.sds Backdoor.Win32.Rbot.aftu , ,)
d2c403b6a11627267af5415ef1819c0f	1	0 ***NEW	Y (w32/rahack.a.gen!eldorado , Net-Worm.Win32.Allaple.b , ,)
3228f8bc721572422c268f244476dbb8	1	2	Y (w32/backdoor.zzr W32/Trojan5.DCW , Backdoor.Win32.Rbot.bqj Backdoor.Win32.Rbot.aftu Backdoor.Win32.Rbot.abpn , ,)
df51e3310ef609e908a6b487a28ac068	1	15	Y (w32/backdoor.zzr W32/Trojan5.DCW , Backdoor.Win32.Rbot.rgk Backdoor.Win32.Rbot.aftu , ,)
bb39f29fad85db12d9cf7195da0e1bfe	1	9	Y (w32/backdoor.zzr W32/Trojan5.DCW , Net-Worm.Win32.Kolabc.eia Backdoor.Win32.Rbot.aftu , ,)
4c3123dbfeaed4baeff53436e9c48dba	1	1	Y (w32/virut.ag , Backdoor.Win32.Rbot.adqd , ,)
57d8a1d90b8e40c6325c55655f900cef	1	X	Y (W32/Sdbot.AEFV W32/Malware!44f4 , Backdoor.Win32.Rbot.bni , ,)
f42243f3f5b2b68be2f480bc3f5f146e	5	0 ***NEW	Y (w32/genbl.f42243f3!olympus , Trojan.Win32.VBKrypt.ubmz , ,)
cf7ac5aced5de80b8e336e5866571617	1	0 ***NEW	Y (w32/allaple.a.gen!eldorado , Net-Worm.Win32.Allaple.e , ,)
49fe29f09b7c232451dc339696f7cb9c	1	0 ***NEW	Y (w32/virut.7116 , Virus.Win32.Virut.av Net-Worm.Win32.Allaple.e , ,)
33959bb2c48363ddd3637ea78c048b6c	1	3	Y (W32/Sdbot.AEFV , Virus.Win32.Suspic.gen

			Virus.Win32.Virut.n Type_Win32 , ,)
617335b4b1f0fd67b2ea418fe8a15001	1	0 ***NEW	Y (w32/allaple.j , Net-Worm.Win32.Allaple.e , ,)
9b175f5f727bcf1153e1aaf99798556a	1	2	Y (w32/trojan-sml-sdcw!eldorado , Email-Worm.Win32.Updater.j , ,)
3a438aa17b291c9b445ebeeed65a286b	1	0 ***NEW	Y (W32/Sdbot.AEFV , Virus.Win32.Suspic.gen Type_Win32 , ,)
cbf11a3a71081784ae85cb53095b44e7	1	0 ***NEW	Y (w32/allaple.a.gen!eldorado , Net-Worm.Win32.Allaple.e , ,)
6fec7d509c2f494a506e3f22851de2ff	1	0 ***NEW	N (, , ,) script file
c4af6e846c046ae87f4be59685405f49	1	1	Y (w32/trojan.mex , Backdoor.Win32.Rbot.bni , ,)
d41d8cd98f00b204e9800998ecf8427e	1	13	N (, , ,) invalid file - download interrupted.
b0b39f058a958778b15a5c4589a2938d	1	2	Y (W32/Sdbot.AEFV W32/Backdoor2.AJVO , Backdoor.Win32.Rbot.bni , ,)
306e5a5f9cc19380ae646964939da82a	1	0 ***NEW	Y (w32/allaple.a.gen!eldorado , Net-Worm.Win32.Allaple.e , ,)
539a1db8a5adcc1f9a6ccde90e4c5ebc	4	0 ***NEW	N (, , ,) an old file with little detection
1e8d20c9638fdb165514f557bb20fbc3	1	1	Y (w32/virut.7116 , Backdoor.Win32.Rbot.adqd , ,)
f5fbd1189db83db22d7e6cdb55eed193	1	2	Y (w32/downloader.n.gen!eldorado w32/injector.a.gen!eldorado W32/Backdoor!d75d , Net-Worm.Win32.Allaple.e Backdoor.Win32.Rbot.bni , ,)

Notes:

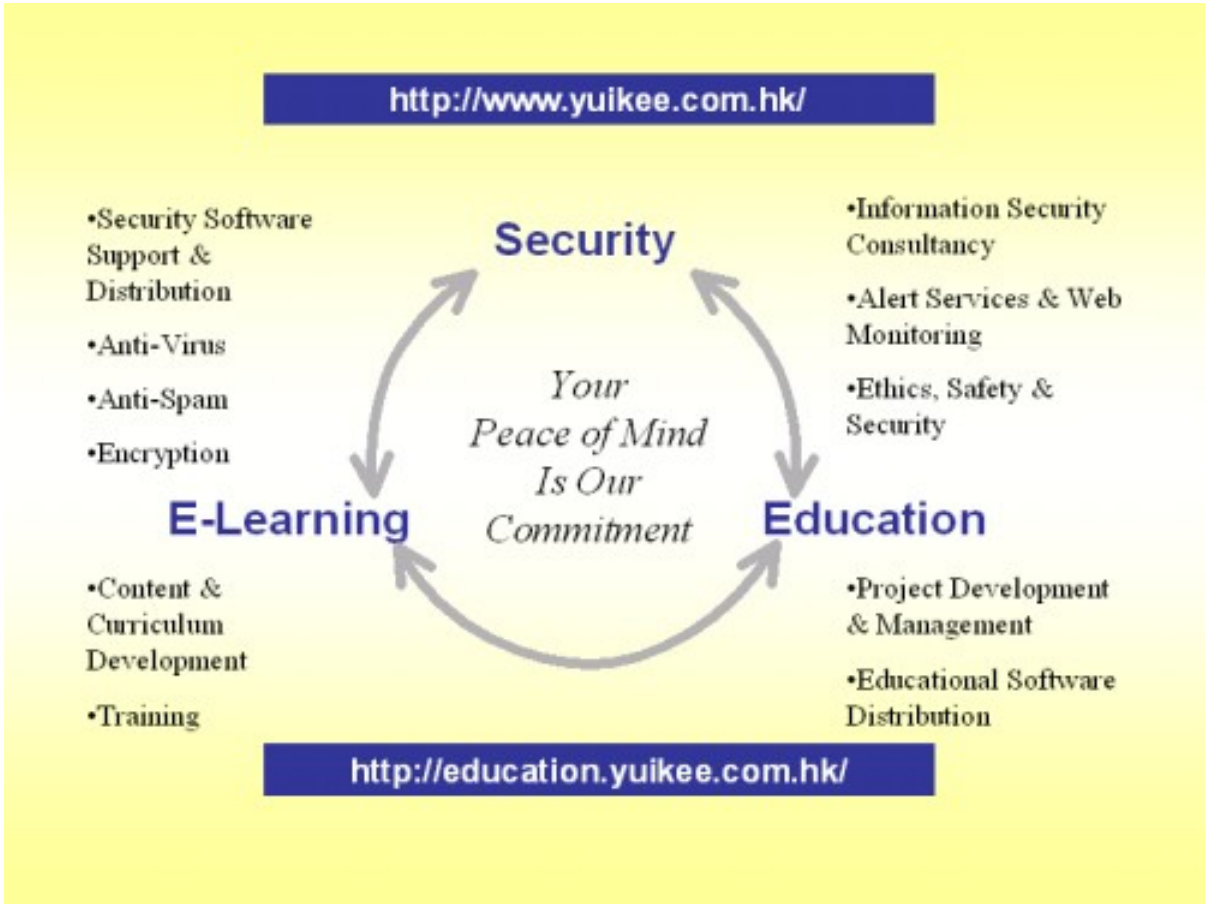
The parameter 'Detection' here relates to whether one or more scanners was able to associate a name with this checksum.

Where an X is shown under Previous, the file has been seen before in this honeypot but the relevant logs are not available

More Information

West Coast Labs
January Hong Kong Honeypot Report

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/