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

Yui Kee Computing Ltd.

Newsletter

November 2012

Contents

Responsible Disclosure in Action: Sophos and Tavis Ormandy

<web-link for this article>

Less than two months after an embarrassing self false-positive, Sophos is again explaining its products failings. The current incident actually started earlier, on 10th September 2012, when Tavis Ormandy, a security researcher with Google, contacted Sophos to report six vulnerabilities in Sophos' security products. A month later, Mr Ormandy provided Sophos with information on two more vulnerabilities. Sophos worked on fixing the problems and updated users with fixes for seven of the problems between 22nd October and 5th November. Mr Ormandy then published his analysis, followed by Sophos issuing their own article, both on 5th November. A fix for the eighth problem is expected on 28th November.

Yui Kee's Chief Consultant, Allan Dyer, commented, "This is how responsible disclosure is supposed to work. An external researcher found vulnerabilities and gave the developer the opportunity to fix them before publishing. The developer made use of the opportunity, fixed the issues, and courteously let the researcher publish first. Both acted together for the protection of users."

However, not all is sweetness and light between Mr Ormandy and Sophos. In 2010, Sophos accused Mr Ormandy of irresponsible disclosure and in the current incident the blog postings make it clear that he and Sophos differ in their opinion of the quality of the products.

Dyer commented, "Responsible disclosure benefits everyone, but some friction between external researchers and developers is to be expected as the approach the issue from different angles. So long as it is kept polite, the friction can be beneficial, as it prevents complacency. We should all remember the common enemy are researchers that exploit their findings for dishonest gain."

More Information

[Full-disclosure] multiple critical vulnerabilities in sophos products

[Sophos products and Tavis Ormandy](#)
[Advisory: Tavis Ormandy finds vulnerabilities in Sophos Anti-Virus products](#)
[Google bod exposes Sophos Antivirus' gaping holes](#)
[Sophos Self False-Positive](#)

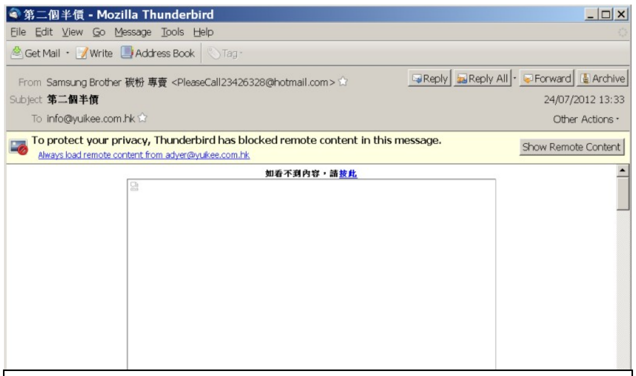
Hong Kong's Anti-Spam Law Allows Obfuscation of Unsubscribe Information

<web-link for this article>

According to advice received from Hong Kong's Office of the Communications Authority (OFCA), although the Unsolicited Electronic Messaging Ordinance stipulates that commercial electronic messages must contain a functional unsubscribe facility, it is not necessary for the facility to be visible to or usable by the recipient. Furthermore, OFCA refused to be proactive in contacting the Equal Opportunities Commissioner to get advice about inaccessibility of unsubscribe facilities.

This example shows various failings of the opt-out regime adopted by the Hong Kong Government and the untenable burden it places on recipients of unwanted messages. Unscrupulous senders can easily obstruct unsubscribe requests with impunity, whereas a fair law would make senders responsible for ensuring they are not causing a nuisance when they take advantage of cheap communications to send large numbers of messages.

The advice was given in relation to an unsolicited message report made by Allan Dyer on 25th July 2012, assigned case number 125009726 by OFCA. Mr Dyer reported the email for not containing an unsubscribe facility. On 6th August, OFCA replied that there was an unsubscribe facility, and they had tested that it was functional. Mr Dyer replied on 8th August, including a screenshot of the message as it appeared in his email client, saying:



From Samsung Brother 碳粉 專賣 <PleaseCall23426328@hotmail.com>
Subject 第二個半價
To info@yuikee.com.hk
24/07/2012 13:33

To protect your privacy, Thunderbird has blocked remote content in this message.
Always load remote content from adyer@yuikee.com.hk

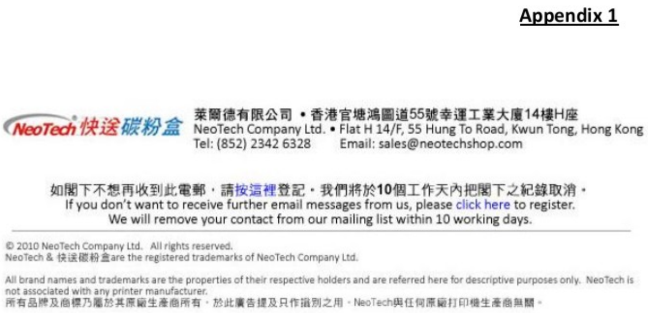
如看不到內容，請按此

Unsolicited message, as it appeared in the recipient's email client.

> Thank you for your reply. I think you are not considering the full picture. Please find attached a screenshot of the offending message in my email client. As you can see, it appears as the Chinese text "如看不到內容，請按此" and a series of remotely-hosted images that my company's security policies recommend that my email client be configured not to load. There is no visible, English unsubscribe facility.
>
> If the Chinese text is an unsubscribe facility, then the sender is remiss in not including English text as well.
>
> Please confirm whether failure to provide a bilingual unsubscribe facility is an offence under the UEMO.
>
> If there is an unsubscribe facility in the images, please note that:
> 1. These are not part of the email message sent to my server.
> 2. They are not accessible to users of email clients configured not to load remote images.
> 3. They are not accessible to blind people.
>
> Please state clearly whether the UEMO allows unsubscribe facilities to be described outside of the message sent, and in a form inaccessible to many users.

On 9th August OFCA replied:

> We note that the complained message did contain the unsubscribe facility in both Chinese and English as shown in Appendix 1. As the UEMO does not prohibit senders using different technology of sending email messages, one might configure the email client to load the remotely-hosted images to find the unsubscribe facility as shown in Appendix 1.



Appendix 1

萊爾德有限公司 • 香港官塘鴻圖道55號幸運工業大廈14樓H座
NeoTech Company Ltd. • Flat H 14/F, 55 Hung To Road, Kwun Tong, Hong Kong
Tel: (852) 2342 6328 Email: sales@neotechshop.com

如閣下不想再收到此電郵，請按這裡登記，我們將於10個工作天內把閣下之紀錄取消。
If you don’t want to receive further email messages from us, please click here to register.
We will remove your contact from our mailing list within 10 working days.

© 2010 NeoTech Company Ltd. All rights reserved.
NeoTech & 快送碳粉盒are the registered trademarks of NeoTech Company Ltd.

All brand names and trademarks are the properties of their respective holders and are referred here for descriptive purposes only. NeoTech is not associated with any printer manufacturer.
所有品牌及商標乃屬於其原廠生產商所有，於此廣告提及只作識別之用，NeoTech與任何原廠打印機生產商無關。

Appendix 1 of OFCA's 9th August letter, showing the image linked to from the message

> In your email, you asked if the Chinese text “如看不到內容，請按此” is the unsubscribe facility. This statement in English means “if the content cannot be seen, please click here”, and it is not the unsubscribe facility.
>
> Section 7 of the Unsolicited Electronic Messages Regulation (“UEMR”) stipulates that the unsubscribe facility statement must be given in both Chinese and English, unless the recipient has indicated to the sender that the statement may be given in that language. It is therefore a contravention of section 7 of the UEMR for failure of providing a bilingual unsubscribe facility in a commercial electronic message, if the recipient did not indicate the language preference before.

OFCA translates the plain text in the message as “if the content cannot be seen, please click here”, but Google translate renders it as “if you are not content, please click here”.

Mr Dyer was unsatisfied with OFCA's response and replied on 9th August:

> Thank you for your clarification of your interpretation of the UEM, although I note that you do not completely address all the points I raised in my email of 7 August 2012.
>
> Given that the sender of the message did not provide an unsubscribe facility that was visible to me, the intended recipient, can you now confirm that you will be pursuing the sender for their contravention of the UEMO?
>
> In your reply, please address the following issues:
>
> 1. The SMTP email message delivered to my mail server did not include an unsubscribe facility, it only contained a link to an unsubscribe facility.
> 2. The linked facility provided was in the form of an image of text and therefore inaccessible to blind people. What does the Equal Opportunities Commissioner say about the accessibility of unsubscribe facilities?
> 3. As the UEMO requires the sender of a message to provide an unsubscribe facility, surely it is the sender's duty to ensure that the facility is provided to the recipient in the message, in a form that they can use. The sender should not assume anything beyond the facility to receive the basic protocol (in this case, SMTP) and understanding of Chinese or English.
>
> I reiterate, sending a link is not the same as providing the linked information, in just the same way that telling you an ISBN is not the same as giving you a book.

On 27th August, OFCA replied:

> The gist of your email is that if the unsubscribe facility is not absolutely text based it would be discriminatory since a person with visual impairment would not be able to unsubscribe the commercial electronic message (“CEM”) if his or her computers are installed with the security settings that can block remotely-hosted images in messages that were received.
>
> As far as the requirements for unsubscribe facility is concerned, section 9 of the UEMO provides inter alia that a person shall not send a CEM that has a Hong Kong link unless the message includes the unsubscribe facility. Section 2 of the UEMO defines, “electronic message” as a message includes a message in any form sent over a public telecommunications service to an electronic address and includes, but is not limited to—
>
> (a) a text, voice, sound, image or video message; and
> (b)a message combining text, voice, sound, images or video.
>
> Thus, as far as sections 2 and 9 of the UEMO are concerned, they do not strictly prohibit any action of including an unsubscribe facility within an image. The law does not specifically require that all unsubscribe facilities have to be text based. Regarding the question whether the sender has

> contravened the provision of the Disability Discrimination Ordinance, you may wish to consult the Equal Opportunities Commission.

Mr Dyer responded the same day:

> Thank you for your reply. Unfortunately, I feel that it does not address the multiple issues I raised.
>
> You have over-simplified the issues by condensing them into a single "gist" that covers three separate points. I include those points from my previous email below, with further explanatory information and questions:
>
> "In your reply, please address the following issues:
>
> 1. The SMTP email message delivered to my mail server did not include an unsubscribe facility, it only contained a link to an unsubscribe facility."
>
> "I reiterate, sending a link is not the same as providing the linked information, in just the same way that telling you an ISBN is not the same as giving you a book. "
>
> Let me remind you that, the message in question contained a link to an image of the text of the unsubscribe instructions. Thus, the message delivered to my mail gateway did NOT contain the unsubscribe instructions. If you contend that including a link to the instructions is equivalent to including the instructions, would you also contend that including a link to a link to a link to the instructions is equivalent? How far would you say this can be extended without making yourselves and the law look ridiculous?
>
> I also note that, in your reply you state, "unless the message includes the unsubscribe facility". The message in question did not INCLUDE the facility.
>
> "2. The linked facility provided was in the form of an image of text and therefore inaccessible to blind people. What does the Equal Opportunities Commissioner say about the accessibility of unsubscribe facilities?"
>
> This is the only point that you actually addressed, and you merely suggested that I could contact the Equal Opportunities Commissioner. However, I am not blind, so I have no grounds to make a complaint under the Ordinance. If I did contact the Commissioner, and he replied that there was cause for concern, what use would the reply to me be? I am not authorised to be an intermediary between OFCA and the EOC. On the other hand, you are charged with the responsibility of correctly implementing the UEMO and, now that a member of the public (me) has raised this question, it would be responsible of you to contact the Commissioner for advice. Based on that advice, you could update your Guidelines for senders of messages. I think you should be pro-active in the discharge of your duties, do you disagree?
>
> As a counter-example, what would your view be if a message contained a link to an image of Braille text of the unsubscribe instructions?
>
> "3. As the UEMO requires the sender of a message to provide an unsubscribe facility, surely it is the sender's duty to ensure that the facility is provided to the recipient in the message, in a form that they can use. The sender should not assume anything beyond the facility to receive the basic protocol (in this case, SMTP) and understanding of Chinese or English."
>
> I do not think you addressed this point. While the law does not specify that all unsubscribe facilities have to be text based, it is still the duty of the sender to PROVIDE the facility. If they do not have prior knowledge of the recipient's capabilities and equipment, they should not assume anything other than the the minimum for the communications medium.
>
> I hope that you can provide a more reasonable answer to the points I have raised, without unjustified oversimplification.

OFCA responded on 8th November:

> We refer to your email dated 27 August 2012 and thank you for your comments. We however do not wish to comment further on your email regarding unsubscribe facility or hypothetical questions. Suffice to say here is that as and when we receive real case, report or complaint about accessibility of unsubscribe facilities, we will handle them, with the information and evidence provided by the complainant, in accordance with the relevant requirements stipulated in the UEMO.
>
> Regarding the captioned report, we would like to reply as follows:
>
> As explained in our previous letters, sections 2 and 9 of the UEMO do not prohibit the inclusion of an unsubscribe facility within an image, i.e. in this case, a web link associated with an image. Nor does

> the UEMO require that all unsubscribe facilities have to be text based. In fact, it has been a prevalent practice among the industry to include web links in email messages or other web contents for recipients to access the content at the receiving end. In this regard, senders of commercial email do not necessarily include unsubscribe facilities as simple text, but can also include text and web links as well. As shown in the complaint, the concerned sender had provided an unsubscribe facility when it sent out the concerned message.

Mr Dyer responded:

> While I would not go as far as to say that the use of web links in email messages for access to the message content is prevalent, I would agree that it is not uncommon, particularly among senders of unsolicited messages that wish to avoid blocking at gateways. However, I think that your reasoning is seriously flawed when you say that, because it exists, it must be permitted by the UEMO.
>
> I think that such practices put unnecessary barriers to recipients unsubscribing and goes against the spirit of the UEMO, whether this is intentional or unintentional on the part of the senders. Furthermore, I think it can be argued that the practice is against the letter of the UEMO, because the SMTP message received by the recipient does not include the means to unsubscribe. I think it would be appropriate for you to update your guidelines to clarify your position on the practice.
>
> I note in the footnote to your messages you say, "REMARK: This letter is intended for the use of the intended recipient(s) only. No unauthorized disclosure or use of this letter is permitted. If you are not the intended recipient(s), please notify us immediately and destroy this letter." Thank you for your permission for me, as the recipient, to use your letters. I have decided to use them as part of a public article on this case and the issues involved, that you can find in my company's newsletter: *link to this article*

HKEx DDoS Businessman Moves Out of Mother's Home

<web-link for this article>

RTHK reports that Tse Man-lai, the owner of an information technology firm, has been jailed for nine months for two counts of accessing computers with dishonest or criminal intent.

Mr Tse was arrested following Distributed Denial of Service (DDoS) attacks on the Hong Kong Stock Exchange's regulatory disclosure website, HKExnews on 10th to 12th August 2011. The attacks led to shares in several companies being suspended for a short time because they had made price-sensitive announcements when communications were disrupted.

He initially pleaded not guilty in the District Court on 24th September 2012, where the prosecution claimed that a DDoS attack was launched from a computer at Tse's mother's home, and a blog post titled, "Ernest Networking teaching", that demonstrated the attack on HKExnews, asked people to subscribe to the author's DDoS prevention method and included the web address of Pacswitch Globe Telecom. Tse admitted that he was the only user of the computer at the home he shares with his mother, which was used to launch the attacks.

A police spokesman welcomed the ruling.

More Information

Stock Exchange hacker jailed
Stock Exchange hacker gets nine months jail
HKEx hacker jailed for nine months: RTHK
Businessman Convicted of Crashing Hong Kong Stock Exchange Website from Mother's Home
Businessman Denies DDoS Attack on Hong Kong Stock Exchange
Businessman Arrested for Stock Exchange Attack
Trading at Hong Kong Stock Exchange Suspended after Cyber-Attack

AVAR 2012 Conference Report

<web-link for this article>

The city of Hangzhou, China, was the venue of the 15th annual conference of the Anti-Virus Asia Researchers Association (AVAR) on the 13th and 14th of November. Hangzhou is the capital of Zhejiang province, has a population of about 7 million and is famed for the beautiful West Lake area.

Mobile malware, and, in particular, Anroid malware, was covered by several speakers. Andreas Marx and Maik Morgenstern described the approach of AV-TEST to test and certify Android security products. They first described the problems with existing tests, and took a user-centric view of how they would evaluate the products. This leads to consideration of peripheral criteria, such as the effect of the security application on battery life, and remote lock or wipe features, that are not tested on other, static platforms. They plan to test twenty to thirty of the most common Android security applications every two months, and to continually improve their testing.

Zhang Jian reported on the situation in China, as seen from the National Computer Virus Emergency Response Centre and Computer Anti-Virus Products Testing Centre. Most of the respondnts to an online survey of 196 million users were using anti-virus software (85%) and a firewall (78%) but still 68% witnessed security issues, often related to vulnerabilities or lack of proper password or access control. Malware transmission was mainly by online, mobile or email channels. In a survey of over 7000 Government websites, 29% were found to have security holes.

Dennis Batchelder explained how a healthy anti-virus ecosystem was important to Microsoft. The Microsoft Malware Protection Center (MMPC) uses four metrics to evaluate their performance: False Negative Impact; Time To Protect; Actives Per Month (systems where an infection had to be removed); and Fast Sourced (the percentage of samples Microsoft collected itself, as opposed to received from their anti-virus partners). The MMPC strategy to protect their brand is to ensure all systems using Microsoft's products are protected (though not necessarily by a Microsoft product); to disrupt the malware ecosystem by reducing the reach and time to live of malware, making it difficult for criminals to get a return on their investment; and to encourage, paradoxicly, diversity, unity and value in the anti-virus ecosystem. Diversity means no monoculture of anti-virus products, thus increasing the difficulty of creating effective malware. Unity means cooperation within the anti-virus industry. Value means users being happy to pay for the protection they get from anti-virus products.

Igor Muttik and Mark Kennedy introduced the IEEE Software Taggant System. This industry-cooperation system addresses the problem of the high volume of obfuscated malware by allowing software packer vendors to mark their product's output with license-specific markers. Then, if a license is found to be being used for packing malware, it can be blacklisted and anti-virus products can block accordingly. False positives on packed software are eliminated, and packer vendors can continue to sell their products to legitimate users. Only malware authors loose out, when they find their expensive (or pirated) packing software quickly gets blacklisted.

Aleksandr Matrosov and Eugene Rodionov won the Best Speaker award for their technical analysis of the Festi botnet. Festi is one of the most powerful botnets for sending spam and performing DDoS attacks and it has stiking features that distinguish it from other malware with similar functionality

Sometimes it seems that there is a lot of low-end activity, compromising end-user machines for botnets or tricking users into installing fake anti-virus products, and some very high-profile, military grade attacks like Stuxnet, Duqu, Flamer and Gauss. Righard Zweinenberg reminded us of the middle range, with a case study of Medre.A and industrial espionage. ACAD/Medre.A is a worm written in AutoLISP, a programming language used in AutoCAD, the popular Computer-Aided Design software. ESET's malware collection system detected an outbreak of the malware in Peru and investigation showed that it was stealing designs from infected systems and emailing them to accounts in China. In a demonstration of effective cooperation, ESET contacted Tencent, the ISP for the destination addresses, the Chinese National Computer Virus Emergency Response Center (CVERC) and AutoCAD. The accounts were swiftly blocked and a free stand-alone cleaner was made available.

Checking that a Windows executable is signed gives assurance that we know which company created the program, and that it has not been modified after it was signed. Unfortunately, Igor Glücksmann reported on flaws in the Windows Authenticode Portable Executable Signature Format that allow modified executables to execute an arbitary payload without invalidating the signature. Microsoft has issued a partial fix (MS12-024), but the underlying design fault remains, and it is an important reminder that there is more to security design than adding a signature.

Other presentations covered rootkits, the implications of IPv6 and IDNs, Windows 8 and social network exploits.

The panel discussions reflected the hot topics: mobile malware, false positive reduction, advanced persistent threats and user issues.

The Gala Dinner featured Chinese entertainment: drumming, dancing and singing. After the conference, a bus tour took some of the participants to the highlights of the West Lake area.

November Hong Kong Honeypot Report

<web-link for this article>

This is the eleventh 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 continues to fall slowly.

Average Time To Infect: 49 hours 36 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 : 15

8 are brand new to this honeypot.

Source of Attacks

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

4	Japan
4	Canada
2	Spain
2	Vietnam
1	Taiwan
1	United_States
1	China

Malware

Checksum (md5)	This month	Previous count	Detection*
74aa4e07b4265d7669dca3050c7a180d	1	0 ***NEW	Y (w32/rbot.b.gen!eldorado , Backdoor.Win32.Rbot.bni , ,)
3875b6257d4d21d51ec13247ee4c1cdb	1	33	Y (W32/Sdbot.AEFV W32/Malware!44f4 , Backdoor.Win32.Rbot.bni , W32Rbot!I2663 ,)
95262bd40b2be4a9c2ef328e14286d00	1	2	N (, , ,) old file with no detection
f9dc3945bdd7406bd8db06a47963ec14	1	19	Y (W32/Sdbot.OTR , Net-Worm.Win32.Kolab.aefe Backdoor.Win32.Rbot.bqj , ,)
30289051393a82eac311fa400d250de1	1	0 ***NEW	Y (w32/allaple.a.gen!eldorado , Net-Worm.Win32.Allaple.e , ,)
e7673740800b60855706871a3d30ee5f	1	0 ***NEW	Y (w32/rahack.a.gen!eldorado , Net-Worm.Win32.Allaple.b , ,)
9a1cd8224b71dae733a2a95fa24d88d8	1	0 ***NEW	Y (w32/genbl.9a1cd822!olympus , Backdoor.Win32.Azbreg.ngb , ,)
a99b098e0f41fd41fda492606d8c3355	1	0 ***NEW	Y (w32/virut.ag , Backdoor.Win32.Rbot.adqd , ,)
15965bb88165d1eb06851d8f076130ba	2	16	Y (w32/sdbot.otr , Net-Worm.Win32.Kolab.aefe Backdoor.Win32.Rbot.bqj , ,)
8301d449e872c833d90660894a32edf6	1	0 ***NEW	Y (w32/virut.ag , Virus.Win32.Virut.at Net-Worm.Win32.Allaple.e , ,)
d739340ac12e45ba28ead7213e72a712	1	0 ***NEW	Y (w32/virut.7116 , Backdoor.Win32.Rbot.adqd , ,)
1d53fb866c27a421f7557e3cda0592ac	2	8	N (, , ,) old file with low detection
df155696b3af7da8b18896fe6377eab6	1	0 ***NEW	Y (w32/genbl.df155696!olympus , Worm.Win32.Hamweq.ly , ,)

One of these files has been in the Wildlist.

Note:

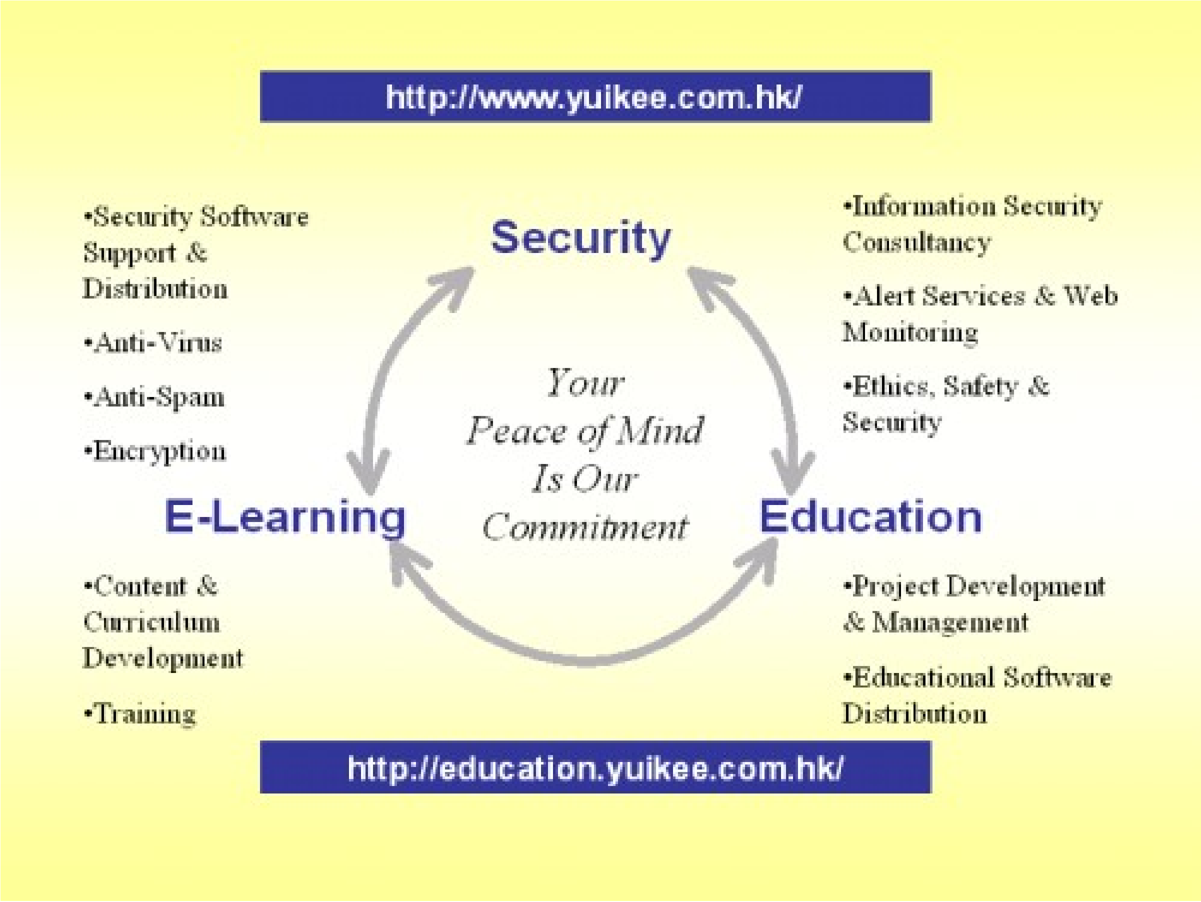
The parameter 'Detection' here relates to whether one or more scanners was able to associate a name with this checksum.

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/