Yui Kee Computing Ltd.

Newsletter

June 2008

Contents

Lies, Damn Lies and the Mean Cyber-Streets of Hong Kong

<web-link for this article>

McAfee's second annual report of malicious websites worldwide, "Mapping the Mal Web, Revisited" finds that the .hk top-level domain (TLD) has become the "most dangerous" place to web surf, jumping from 28th place last year. Predictably, this result has attracted some attention in the local press, and anger among legitimate .hk webmasters who feel their sites are being unjustly maligned. What is the reality behind the report?

Obviously, and this is mentioned explicitly in the 2007 report, .hk does not equal Hong Kong:

Individual domains can be owned by persons from any nationality. For example, .com's are registered to people of almost every nationality. This data should not be used to infer riskiness of nationality.

Many of Hong Kong's best-known, and perhaps, highest traffic, websites, such as netvigator.com and scmp.com, are not in the .hk TLD.

Unfortunately, the published report omits some key information that makes it difficult to understand what is going on:

- **What is being measured?** The report is based on "9.9 million site reports" of "the most trafficked web sites", accounting for over 95% of web traffic. However, the precise meanings of these are not explained and the detail could introduce subtle biases. Is that 95% of page views, or bytes? How was it measured? If it is by software installed on users' computers, like the Alexa toolbar, then the sample population is "people that do not mind being monitored", and the monitoring software might be more heavily installed by some language groups than others, particularly if it is only available in a few languages. This will create a bias in the choice of "popular" sites for a TLD - the sites that are really most popular will probably be in the local language, but the sites most visited by outsiders are likely to be the dodgy, spamvertised sites. On the other hand, if traffic was measured directly, where were the monitoring stations established? All methods of measurement will introduce some bias, why has McAfee omitted to explain their methods so that we can understand the potential bias ourselves?

- **How many sites were measured in each TLD?** We know 9.9 million sites were measured in total, and the report states that the rankings were restricted to TLDs with at least 2000 tested sites, but exactly how many sites were tested in each TLD? Two thousand is not a large sample, this suggests that, for the "smaller" TLDs, the ranking could be easily skewed by a small number of dodgy sites. The "change in risk" statistic shown is a large positive spike for .hk, and a large negative spike for .tk, last years' "most risky" TLD, this is a classic warning sign that the statistic reflects random variations of a small sample rather than an underlying trend in the data.
- **When was the data collected?** The report does not specify whether the data was collected over the whole year preceding its release, or a limited testing period, or some other time period. The Web is not a static entity, and the exact time period could make a huge difference to the results, particularly in the light of events in Hong Kong over the last year described below.

In addition, in the discussion the report refers to reports by Sophos and Sunbelt as confirming the dramatic increase in the risk of .hk during the last year. This is a gross mis-representation of those reports. The Sophos report was published January 2007, and related to data from 2006, covering some of the same period as McAfee's March 2007 report, so, if anything, it merely confirms that Hong Kong was "dangerous" before the sudden rise claimed by McAfee. Secondly, the Sophos report (which is about spam relay locations) aggregates Hong Kong with China, so little or nothing can be inferred about the specific situation in Hong Kong. The Sunbelt report related to one specific case of one .hk domain, endeny.hk that was used by the Storm worm. While that was a significant case, it does not reflect the general riskiness of the TLD, indeed, it is an example of an incident that could skew the statistics for a small TLD. The domain no longer exists, and can be registered with HKDNR.

A significant event during the last year that impacts on this report is the delisting of over 8000 .hk domain names by HKDNR, as previously reported in this newsletter and at the AVAR Conference. The delisting was a result of cooperation between OFTA and the HKDNR on combating spamvertised domains reported to OFTA following the introduction of the Unsolicited Electronic Messages Ordinance (UEMO). This event links directly to the three significant ommissions in McAfee's report, listed above: The sites were heavily spamvertised to victims outside of Hong Kong, and could therefore be over-represented in geographically-biased traffic statistics. The number of delisted sites was over 8000, a lot more than the 2000 cut-off point for TLDs to be ranked, so their inclusion or exclusion would have a large effect on the results. The sites were delisted around June to September 2007, so McAfee's data collection dates are highly significant for .hk in particular.

What is the final conclusion? Without the missing methodology details, McAfee's report is questionable and almost useless. The biases cannot be understood, and the web changes quickly. It is doubtful that choosing sites by their TLD will significantly alter the riskiness of your surfing. If users want to make their surfing safer, they should stop following links in dodgy, unsoliticted emails.

OFTA and HKDNR should be praised for their actions in shutting down many spamvertised domains, but it should also be remembered that HKDNR's efforts to increase the number of .hk registrations attracted the spammers and malware distributors in the first place. The .hk TLD is a valuable resource for Hong Kong, and HKDNR should remember that it needs to protect that value for all of us. On a related point, a puzzling omission from the factors constituting a "Hong Kong Link" for the purposes of the UEMO was the involvement of a .hk domain name. Although the idea was proposed during the consultation period, it was left out of the Bill because .hk domain names could be registered by non-Hong Kong entities. It is clear that, if an entity chooses to register a .hk domain, it is claiming an association with Hong Kong, so it is entirely reasonable to require compliance with Hong Kong laws. Amending the UEMO to

make a .hk domain constitute a Hong Kong Link would put the delisting of abused domains on a stronger legal footing.

More Information

Mapping the Mal Web, Revisited
Mapping the Mal Web (2007 report)
.hk - World's most dodgy domain
Weekend run of fake greetings loads malware
Sophos Security Report 2007 reveals United States is worst for malware hosting and spam-relaying
Combating Phishing and Spamming Sites by HKDNR
Is Hong Kong's new Anti-Spam Law Effective?
Hong Kong, China Web domains cited as 'most dangerous'
Abuse of .hk Domain Names Falls
Pindar Wong on CNN
.hk the "Most Unsafe" Domains?

MessageLabs lists Hong Kong as the "most spammed country"

<web-link for this article>

MessageLabs' May 2008 report lists Hong Kong as the "most spammed country", with 85.9% of email processed by the company for Hong Kong being spam. Globally, spam is still rising, with 76.8% of all emails being spam, an increase of 3.3% over April.

More Information

MessageLabs Intelligence: May 2008

Immigration Department Learns Information Security Management Basics

<web-link for this article>

The Immigration Department, following a recent personal data leak, has pledged to comply with 10 recommendations made by the Privacy Commissioner. These include categorising according to their sensitivity, ranging from "absolute prohibition of photocopying or storage" to "data that can be taken or copied for use outside the office". Anyone who has looked at information security best practices or standards, such as ISO 27001, will know that this type of categorisation is a basic step in the security process. The Immigration Department should be encouraged in their efforts, but why weren't the basics already in place?

More Information

Immigration moves to stem tide of alarming data leaks
Immigration to use data-privacy plan
Data Leak Disease
Data Leak Disease Spreads to Police?

Fighting Fire with Fire: HKDNR's Flawed Response

<web-link for this article>

The Hong Kong Domain Name Registration Company (HKDNR) has reacted to McAfee's damning and flawed report (discussed in this newsletter) with a hastily-prepared press release that is also stuffed with dubious claims and unverifiable statistics. Chief among these is the claim that there was a daily average of 38 cases of spamvertised and phishing .hk domains

during 2007, and that this dropped to 3 cases (presumably per day, the wording is a little unclear on this) for January to May 2007. Therefore, there were about 456 cases in the first five months of this year, however, later in the release it states,"more than 14,000 '.hk' domain names were suspended by HKDNR this year by the end of May" for spamvertising or phishing activities. Why did only 456 cases result in 14,000 suspensions?

Of course, it must be considered that a reduction in the number of cases does not, necessarily, indicate a reduction in the size of the problem. HKDNR's recent efforts, with OFTA, the Police and HKCERT, in clearing up the problem date from the implementation of the Unsolicitied Electronic Messages Ordinance, when OFTA started accepting spam reports. OFTA soon found they were receiving many reports of phishing and spamvertising, which, strictly speaking, did not fall under their powers under the UEMO. Laudably, they decided to do something about it anyway, resulting in the cooperation, and the domain suspensions. So, before there was a contact point for reports, there were no reports and, therefore, no cases. Does this mean that there was a precipitous increase in the problem when the UEMO came into force? Of course not. The headline, "Drastic Decline Proves Stringent Measures Taking Effect" is wrong, the figures prove nothing of the sort.

Proof would require an independent measure of the size of the problem to start with, and further evidence to demonstrate a causal relationship.

All this is a criticism of the press release: an ill-advised, knee-jerk reaction to a dubious research report published by McAfee. The cooperation between the relevant authorities: HKDNR, OFTA, HKCERT, the Police, and their overseas counterparts, has had positive results in cleaning up many dodgy sites, and should be encouraged and further developed.

One area for further improvement is touched upon in the press release: "document verification for suspicious applications of second-level '.hk' domain names". This is covered by changes to paragraph 2.4 of the HKDNR's Rules, made February 2008:

All interested individuals and entities are eligible to register a Second Level Domain Name, except during the Soft Launch Period where the criteria set out in the Soft Launch Period Rules apply. We may, however, request the submission of any documentary evidence that we consider necessary to verifiy(sic) your identify in determining whether to accept your application for the registration of a Second Level Domain Name.

According to HKDNR's Customer Service Department, this involves a human vetting applications for suspicious features (including, but not limited to, the domain name using words like 'bank', '銀行', 'banco', 'banque', 'banca', 'b-a-n-k', etc.), and asking the applicant for additional documentation when suspicions are raised. Failure to produce the documentation would result in rejection of the application, before payment was made. Improvements to this would include:

- **Receive the payment before the vetting is performed, no refund for rejected applications.** This is reasonable because the fee covers processing the application, so processing should only start after the fee is paid, and it severely discourages cyber-criminals trying repeated applications until one gets through.
- **Demand an explanation and documentation for ALL applications** This avoids the possibility of the vetting staff missing brand names or words in an unfamiliar language. Ordinary applicants will have no trouble explaining their chosen name ("yuikee is our company name") and, in most cases, documentation will be available (birth certificate, business or trademark registration etc.). The rest can be scrutinised more closely ("I'm an individual, my nickname is Banco").

Those interested in discussing this topic further should note a public forum being held on Saturday, 14th June. As this is a topic that affects the trust and confidence in Hong Kong as an

international business hub and financial centre, the organisers have wisely chosen to avoid using the most common language of international business, and one of Hong Kong's official languages: English, instead choosing to hold the forum in another of Hong Kong's official languages, Cantonese. This will, naturally, maximise the coverage in the international media that the fair and reasoned arguments presented during the forum receive. The forum details are:

Organisers	Internet Society Hong Kong Chapter (ISO-HK) Office of Sin Chung-kai, Legislative Councilor Professional Information Security Association (PISA) Hong Kong Internet Service Providers Association (HKISPA)
Date	14 June 2008 (Sat)
Time	2:15pm – 5:00pm (2:15pm-2:30pm Registration)
Venue	Room 202, Duke of Windsor Social Service Building, 15 Hennessy Road, Wanchai, Hong Kong
Language	Cantonese
Participants	Members of the organizers and supporting organizations First-come-first-served and Free-of-charge
Moderator	Charles Mok (ISOC-HK)
Panelists:	Mr. Leo Chan (information security industry), Mr. Jonathan Shea (HKDNR), Mr. Roy Ko (HKCERT), Mr. York Mok (HKISPA), Mr. Bernard Kan (PISA), Mr. SC Leung (IT Voice)
Registration & Enquiry	Email to rsvp@isoc.hk with the following information: Name, Organisation, Company Name, Contact Email, Contact Phone #

More Information

‘.hk’ Domain Name Spamvertising & Phishing Cases Record Average Daily Drop of 92% from Last Year
Mapping the Mal Web, Revisited
Lies, Damn Lies and the Mean Cyber-Streets of Hong Kong
HKDNR Rules for .hk Domain and Sub-domains Version 5.0 Effective 25 February 2008
.hk spamvertising and phishing cases record 92% daily drop, says HKDNR

"Mapping the Mal Web" is the New "Virus Calendar"

<web-link for this article>

Allan Dyer

Marketing is NOT Education!

Last Friday was the 13th June, Black Friday! Days like that used to trigger a peak of interest in viruses: for a few days before, reporters would call up for predictions and advice to prevent disaster, and for a few days after, reporters would call for damage estimates and advice on recovery. Oh, and some users would call with problems. The more the damage, predicted or reported, then the better the headlines, so reporters tended to focus on the more exaggerated predictions and estimates. Less responsible marketing droids would take advantage of this, and more responsible predictions and advice would be overshadowed and overlooked.

Then a brilliant marketing driod came up with the "Virus Calendar" - print the virus activation dates for the year on a nice big poster, with your company name on it, of course. This is presented as an "educational" tool - raising awareness about the virus problem, and helping people deal with it. It does nothing of the sort. It raises fear and anxiety about the problem, and focuses attention on one, relatively insignificant detail: the activation date. Activation dates are probably the second easiest feature of a virus to change, after the text messages - on an old, non-polymorphic DOS virus, just search for the date check OS call, and change the values in the conditional test just afterwards. Trivial to do without access to the source code. In any case, many viruses don't have a calendar date trigger for their payload. The calendar does have a small, diagnostic utility: it is the morning of March 6th, and someone calls up saying their PC won't boot. The technician considers that it might be a Michelangelo activation; but a good technician also considers it might be a disk crash, power supply failure, other software failure, etc... an investigation is still needed. In the end, it doesn't matter if the data was lost to a virus or a disk crash, what matters is whether adequate protection was in place - where are your backups? The calendar doesn't tell you. I don't think any IT department used those calendars for their planning, either; "OK, we have to complete the preventive sweep of all PCs by 18:00 on 5th March. Remember, we're looking for Michelangelo. In two months, we have another sweep to prepare for, that time for Friday 13th". A sane IT department works to prevent infection in the first place.

So why do I say that McAfee's "Mapping the Mal Web" is the new Virus Calendar? It presents itself as a tool to help users, saying, "For the first time, *Mapping the Mal Web* offered a comprehensive guidebook for web tourists - where it was safe to surf and where surfers should avoid." As an annual *report*, it can (possibly) reveal what the situation *was*, but not what it *will be*. This year's report, the second, compared to last year's demonstrates the danger. Assuming, for the moment, that both were accurate, then, the attentive "web tourist" would, after reading the first report, carefully avoid visiting .tk (Tokelau) domains, and view .hk (Hong Kong) domains as only one eighth of the risk. The first report directs surfers to the domains that are identified as high risk in the second report!

In addition, apart from the specific advice being damaging, the general message focuses attention on an unimportant detail, distracting from truly useful advice. For the Virus Calendar, the detail is the date, the evil meme is, "you can avoid viruses by watching a calendar". For "Mapping the Mal Web" the detail is the TLD, the evil meme is, "you can avoid malware by avoiding certain TLD's". I visit .hk websites every day, according to McAfee's report, about one in five of those should be malicious - why haven't I encountered hundreds of malicious .hk sites in the past year? There must be a difference between my surfing behaviour and the surfing behaviour of the users studied by McAfee. Most of the .hk sites I visit are related to a company or organisation I know. Most I have visited before. Others have been linked from a site I know, or a friend or business contact provides the link. This does not guarantee that the sites are safe, maybe the linking site was hacked, or the person I knew fooled, but it makes it less likely. It might account for the difference between my experience, and that of the users McAfee studied. Unfortunately, we don't know because McAfee did not provide sufficient detail about those users. Were they users who, in general, had no interest in Hong Kong people and events, but who would click on any link arriving in spam? If they were, we could expect a very low number of legitimate .hk sites and a very high incidence of malicious .hk sites in their surfing. The lesson to learn, and the lesson that McAfee's report distracts from, is to be cautious about the links you follow - especially those arriving in unexpected emails.

McAfee's first two "Mapping the Mal Web" reports have been misleading, and they encourage unsafe user behaviour. I ask McAfee to apologise and to present a plan for making their third annual report truly useful.

More Information

Latest Symbian OS Vulnerability

<web-link for this article>

A recently–discovered privilege escalation hack allows mobile phone hackers to bypass the security system of the Symbian OS 9 based S60 3rd Edition phones with a mobile application. Symbian OS 9 based S60 3rd Edition is a market-leading open operating system for mobile phones.

The vulnerability allows hackers to get unauthorised access to the phone's normally protected file system, and thus make system modifications.

Hacks directed towards the S60 3rd Edition have been evolving for some time. What makes this case different is that the new hack can be carried out without external devices or system knowledge by installing just one mobile application that could be downloaded from the web.

Because the application can be considered as a hacking application, it is classified by F-Secure as riskware. F-Secure Mobile Security software identifies this application and removes it.

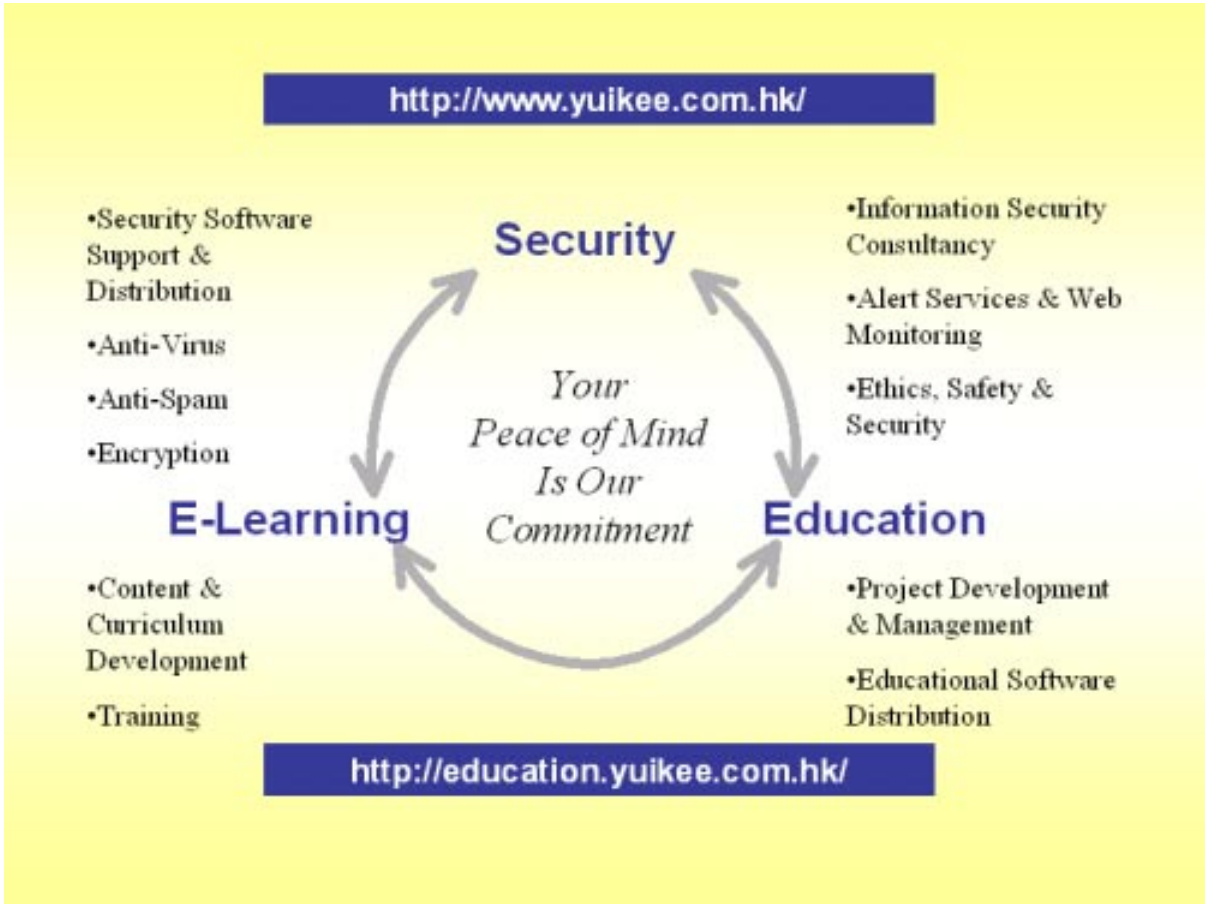
Commenting on the vulnerability, Jarno Niemelä, Senior Mobile Virus Researcher at F-Secure, said, "The application needs to be installed by the user, so this hacking tool is not a threat to the average mobile user. Because the application lets a user access the file system, we consider this as a security risk. Mobile virus source code could be updated to work on 3rd Edition phones and with the addition of this privilege escalation, hackers could do pretty much the same things as they do on 2nd Edition phones."

More Information

Symbian Jailbreak

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
Education
•Content & Curriculum Development
•Training
•Project Development & Management
•Educational Software Distribution
http://education.yuikee.com.hk/