Yui Kee Computing Ltd.

Newsletter

February 2009

Contents

Security Threats are Greek to Hong Kong Users

<web-link for this article>

In a survey commissioned by F-Secure and carried out by independent third party Zoomerang in December 2008, Hong Kong users were just as likely to classify "Spartans" and "Trojans" as not a threat to their internet security.

The annual Online Wellbeing survey also shows that over 90% of people have security software installed on their computers. However, the knowledge of online threats is not as high: 71% may have a false sense of security and it is a trojan not a 'Spartan' which presents a threat to your online security. For the first time, the survey was also conducted in India, Hong Kong and Italy, as well as the United States, Canada, France and Germany that have been surveyed in previous years.

The majority of respondents across the countries - 92% - said they have security software installed on their computers. At the same time only 21% of all the respondents knew that antivirus definitions need to be updated many times a day. This indicates that a large population of users may have a false sense of security if their security software is expired or does not update automatically often enough. However, 67% were also aware that they need more than antivirus to keep them safe and almost 90% knew that they can get infected by visiting a malicious website, even if they don't download anything.

Sean Sullivan, Security Advisor and blogger form F-Secure Security Labs in Helsinki says: "The fact that millions of PC's keep getting infected shows that people do not always understand the way their security software works. The software they have chosen may be manual and curative, rather than automatic and preventative. This is often the difference between free and trial software and a paid security service, which is automatically updated."

The results show that people rely on their security software for online safety and secure websites to ensure the safety of their online shopping and banking. Just over 20% realise that appropriate online behavior on their own part also plays a big role. Respondents in Hong Kong and Germany were most aware of this. Respondents in the UK were least likely to pay attention to their own online habits to keep them safe.

Respondents in India and Hong Kong relied on the security software they had purchased or the security service from their Internet Service Provider (70% India, 50% Hong Kong). Those surveyed in the US had the least confidence in purchased software but rather relied on secure websites. In France, respondents relied more on the security of their online shopping and banking websites than their software.

When asked which concept in a list (worms, phishers, Trojans, Spartans, bots) did not refer to an Internet security threat, 40% answered that they didn't know. Germany had the highest percentage of respondents (54%) who answered correctly that 'Spartans' are not concept in any way related to online security. The second savviest respondents were from Canada (38%). Only 4% of respondents in Hong Kong knew that 'Spartans' are not threatening.

The Internet Explorer vulnerability in December 2008 and the Downadup/Conficker worm which spread widely in corporate networks in January 2009 highlighted once again the need for users to update their applications with the latest patches and updates.

F-Secure's Online Wellbeing survey showed that only 17% of respondents were absolutely sure that they had the latest patches and updates. 40% of respondents were less sure but agreed with the statement. Canadians were the most sure (22%) that their applications were patched, with Germans coming in second (21%).

The survey was carried out across 2019 Internet users aged 20-40 in the United States, Canada, France, Germany, UK, Italy, India and Hong Kong. There were approximately 200 persons surveyed per country. F-Secure asked respondents a series of basic online security questions and, using a Likert scale, asked them to rate the extent to which they were confident in the security of given online activities.

More Information

F-Secure survey: Are Spartans a threat to your online security?

Facebook Privacy

<web-link for this article>

Do you use Facebook? Then you need to understand Facebook's privacy settings - take a look at this guide.

More Information

10 Privacy Settings Every Facebook User Should Know

Incompetent Phishers

<web-link for this article>

Hong Kong based security commentator Richard Stagg asks why phishing gangs are so dumb. One possible reason for the convincing website, but stupid emails is that the "gangs" are very loosely knit, joined only by the money trail. In this scenario, the webmasters outsource the promotion to spammers on a "pay per download" basis. Spammers that are better at drafting and delivering their message will get a better catch, and the ones that mess up the message and repeat-deliver will get laughed at by commentators. Either way, the webmasters still gut the catch.

P. T. Barnum's famous misquote, "there's a sucker born every minute", isn't limited to honest suckers.

More Information

Plenty more phish in the sea
Phishing emails target HSBC customers in Hong Kong

Annelid Affects Availability

<web-link for this article>

Yeovil, UK resident Mark Taylor suffered a laptop failure when an earthworm crawled in through a vent and jammed the cooling fan. Computer technician Sam Robinson was able to repair the problem, reporting that the worm was, "burned to a frazzle". Mr. Taylor blamed his cats for the incident, suspecting that the earthworm may have been brought into his house by one of them, and then crawled into the laptop in an attempt to escape.

More Information

Worm causes computer to crash
Earthworm blamed for laptop crash

Microsoft Issues Security Advisory about NoDriveTypeAutoRun Flaw

<web-link for this article>

Microsoft has issued Security Advisory 967940 on a new update that fixes a flaw in how AutoRun is switched off in Windows. The flaw was published in March 2008. Microsoft is, confusingly, claiming that this is not a security update, saying, "we are communicating the availability of an update that affects your ability to perform subsequent updates, including security updates. Therefore, this advisory does not address a specific security vulnerability; rather, it addresses your overall security."

According to the the original vulnerability note, the autorun feature is supposed to be disabled when the NoDriveTypeAutoRun registry value is set to 0xFF, however the operating system enables some AutoPlay features that may not have been enabled prior to setting that registry value. For example, a program specified in autorun.ini may be executed when a device icon is clicked.

The autorun feature has been criticised by security commentators since it was introduced with Windows 95, as it makes it difficult to avoid executing programs from untrusted media. The "feature" was exploited by Sony to install unauthorised software in 2005 and, more recently, used by Conficker as one of several vectors to spread.

More Information

Sony Rootkit
Microsoft Windows fails to properly handle the NoDriveTypeAutoRun registry value
Microsoft Security Bulletin MS08-038
How to correct "disable Autorun registry key" enforcement in Windows
CVE-2008-0951
Microsoft aims 'non-security' update at gaping security hole
Microsoft Security Advisory (967940) Update for Windows Autorun

Rita Lau Reports on Do Not Call Register Statistics to Legco

<web-link for this article>

Following a question by the Hon Wong Ting-kwong (Legco Member for the Import and Export Functional Constituency), Mrs Rita Lau Ng Wai-lan, Secretary for Commerce and Economic Development gave a written answer detailing operational statistics of the Do Not Call Registers (DNC)and Unsolicited Electronic Messages Ordinance (UEMO) reports.

Three DNC Registries, for faxes, SMSs and pre-recorded phone messages, have been established under the UEMO, the registrations as at January 29, 2009 are:

	Registrations	Total "relevant" numbers	% of total relevant numbers
DNC for facsimile messages	401,257	326,572 (facsimile lines in Hong Kong)	123%
DNC for short messages	393,907	11,389,185 (mobile subscribers in Hong Kong)	3.5%
DNC for pre-recorded telephone messages	747,918	15,118,194 (fixed and mobile subscribers in Hong Kong)	4.9%
Total registrations	1,543,082		

Explaining the high number of registrations on the fax register, Mrs. Lau pointed out that home phone lines can be connected to a fax machine. However, it should also be noted that some businesses may have already opted to use phone lines as fax lines as a way of reducing unwanted faxes, and some businesses decided to register all of their numbers on all three lists, regardless of whether the equipment attached was capable of receiving that type of message.

In any case, Hong Kong users appear particularly adverse to receiving unwanted faxes.

Users receiving unsolicited commercial messages on numbers in a DNC registry can complain to OFTA, who can either issue a warning letter or enforcement notice. The complaints and responses as at January 29, 2009 are:

	Valid DNC complaints	Enforcement notices issued	Warning letters issued
DNC for facsimile messages	684	1	54
DNC for short messages	4	0	1
DNC for pre-recorded telephone messages	19	0	1
Total	707	1	56

With over 1.5 million DNC registrations, and less than a thousand complaints, it appears that the registries are effective at discouraging unwanted messages - or victims are apathetic in reporting problems. Notably, the highest number of complains is for faxes, tending to confirm people's dislike of junk faxes, and the low number of UEMs for the other media.

Mrs Lau also summarised the number of all type of UEM report, up to 29th January 2009:

Reports	
Received:	9,309
Handled:	6,638
Outstanding:	2,671

Average reports per month, July - December 2008: 740

The number of UEM staff has grown form eight in December 2007 to fourteen in December 2008.

More Information

LCQ9: Unsolicited Electronic Messages Ordinance
Council Meeting (Agenda) 4 February 2009
LCQ9: Unsolicited Electronic Messages Ordinance
Response to the UEM Proposals
Is Hong Kong's new Anti-Spam Law Effective?

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/