

Contents

Contents.....	1
Clueless Attackers Deface Hong Kong Websites.....	1
Five Arrested for Attacks on HK Government Websites.....	2
Hong Kong CPA Website Hosts Phishing Redirection Page.....	3
HKMA warns about fake Nanyang Commercial Bank Webpage.....	3
Washington Security Company Reports Compromise of Hong Kong Democracy Websites....	4
HKMA warns about fake Bank of China and Wells Fargo Websites.....	5
Security Down Under: AVAR 2014, Sydney Conference Preview.....	5

Clueless Attackers Deface Hong Kong Websites

[<web-link for this article>](#)

Attackers claiming to be the Anonymous group of hackers defaced some Hong Kong websites and attempted DDoS attacks starting on Thursday 2 October, supposedly in support of the Occupy Central campaign for democracy in Hong Kong.

Their aim has been erratic, a few (some reports say eleven) websites belonging to small businesses with .hk domain names were defaced, including the site of Autism Partnership Hong Kong. Denial of Services attacks on the websites of Occupy Central civil disobedience movement, the Silent Majority for Hong Kong, and the Democratic Alliance for the Betterment and Progress of Hong Kong (DAB) took the sites offline for parts of Friday. While the Silent Majority for Hong Kong and the DAB strongly oppose the civil disobedience, Occupy Central is the organisation that the attackers were claiming they supported.

HKCERT is working closely with the Office of Government Chief Information Officer and Hong Kong Police to tackle the attacks.

Allan Dyer, chief consultant of Yui Kee, commented, "The Anonymous group of hackers is, by its nature, anarchic and loose-knit. Anyone who wants to stir up trouble around the latest *cause célèbre* can hide behind the label and incite the uninformed to target innocent victims. This is in contrast to the Occupy Central protesters, who, over the past week, have earned themselves the reputation as the world's politest protesters, carefully cleaning up after themselves."

More Information

[Beware of Web defacement attacks targeting Hong Kong](#)

[HKCERT warns of Web Defacement Attacks Targeting Hong Kong](#)

[Hong Kong Protesters Clash With Rivals as Tensions Rise](#)

["Anonymous" Facebook Event for the Attacks](#)

['Anonymous' hacker group declares cyber war on Hong Kong government, police](#)

['Anonymous' hacker group brings down DAB, Occupy Central websites](#)
[Occupy Central with Love and Peace](#)

Five Arrested for Attacks on HK Government Websites

[<web-link for this article>](#)

Five people who allegedly attacked government websites, including the Hong Kong Police Force website and the online government telephone directory, using online tools were arrested on 7th October. The attacks have been linked with the ["Anonymous" group's threats to attack government websites](#) in "support" of the Occupy Central movement.

The suspects include a 13 year-old, an 18 year-old student and a 39 year-old car repairer. The student and car-repairer have been charged with "Access to computer with criminal or dishonest intent". The student allegedly attacked the Police website 11,552 time in less than an hour on 4th October. According to Mingpao News, the Office of the Government Chief Information officer noticed the attacks on the Police website early on 4th October and traced the IP address.

The car repairer suspect claimed that his computer was not switched on at the time of the attacks, and suggested that it might be the the action of a trojan.

Following the arrests, HKCERT released a statement [urging the public not to participate in cyber attacks](#), pointing out that participants that download automated tools or applications that require no technical know-how to launch attacks are not aware that the attack tools and applications normally use their IP addresses for the attacks and consume their network and computing resources.

Yui Kee's Chief Consultant, Allan Dyer, commented, "the difficulty with this type of case is ensuring there is a strong evidential link between the attacks and the IP address, the IP address and the suspect computer, and the actions of the computer and the intention of the user."

Updated: 24th October 2014

On 22 October, Secretary for Commerce & Economic Development Gregory So reported to the Legislative Council about the recent DoS attacks on Government websites, saying that they have not caused a significant impact on e-Government services and Government network systems and websites have not been compromised or defaced. The Office of the Government Chief Information Officer blocked the DoS and got the websites to run normally again.

More Information

[Gov't websites resist hackers](#)

[HK Police arrested five over govt website attacks](#)

[HKCERT Urges the Public not to Participate in Cyber Attacks](#)

[OCCUPY CENTRAL - DAY NINE: Full coverage of the day's events](#)

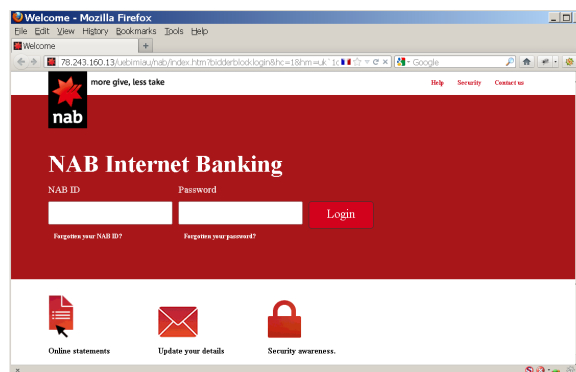
[Clueless Attackers Deface Hong Kong Websites](#)

[Do Not Participate in 「One-Click DDoS Attack」 Cyber Attacks Activity](#)

Hong Kong CPA Website Hosts Phishing Redirection Page

[<web-link for this article>](#)

The Hong Kong Monetary Authority (HKMA) has issued a warning about a page on the website of a Hong Kong CPA that redirects to a fake login page for the National Australia Bank.



The page <http://www.lamchui CPA.com.hk/uebimiau/tool/index.php> is hosted on the website of Lam & Chui CPA Limited and redirects to

<http://78.243.160.13/uebimiau/nab/index.htm?bidderblocklogin&hc=1&hm=uk%601d72f%2Bj2b2vi%3C265bidderblocklogin&hc=1&hm=uk%601d72f%2Bj2b2vi%3C265bidderblocklogin&hc=1&hm=uk%601d72f%2Bj2b2vi%3C265> - a web hosting site in France.

The Police are investigating and anyone who has provided personal information to or has conducted financial transactions through the website should contact NAB at 2826 8111 and any local Police Station or the Commercial Crime Bureau of the Hong Kong Police Force at 2860 5012.

The CPA appears to have been let down by their webmail software. The Lam & Chui front page contains only minimal contact information, but the server hosts their company webmail, run by Uebimiau, a little-known webmail reader. Public development of Uebimiau stopped in 2006, and there are 10 known vulnerabilities. Apparently, a vulnerability allowed an attacker to insert the redirection at [/uebimiau/tool/index.php](http://www.lamchui CPA.com.hk/uebimiau/tool/index.php). The French site also appears to use the same webmail reader.

More Information

[Fraudulent website: http://www.lamchui CPA.com.hk/uebimiau/tool/index.php](http://www.lamchui CPA.com.hk/uebimiau/tool/index.php)

[Uebimiau](#)

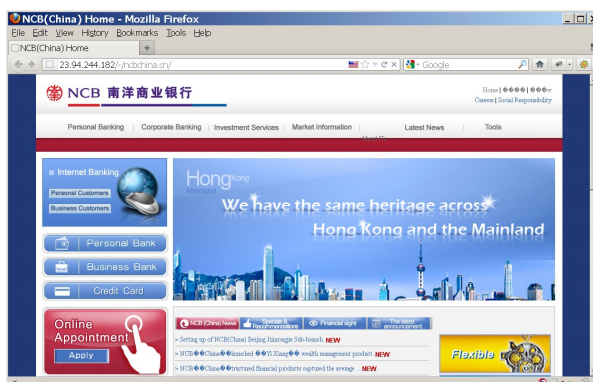
[Alert issued on bogus website](#)

HKMA warns about fake Nanyang Commercial Bank Webpage

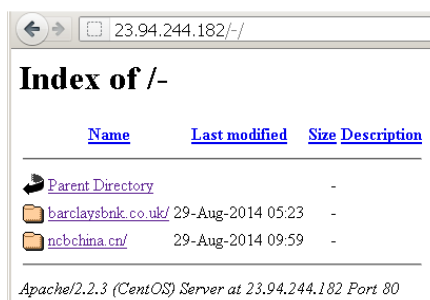
[<web-link for this article>](#)

The webpage <http://23.94.244.182/-/ncbchina.cn/> is a fraudulent copy of the official Nanyang Commercial Bank, Limited (NCB) website, according to the Hong Kong Monetary Authority (HKMA).

The police are investigating and anyone who has provided personal information to or has conducted any financial transactions through the website should contact NCB at 2622 2633 and any local Police Station or the Commercial Crime Bureau of the Hong Kong Police Force at 2860 5012.



The server at 23.94.244.18 also appears to have been involved with a similar fraud targeted at Barclays Bank customers, based on the higher level directory listing of 23.94.244.18. The directory barclaysbnk.co.uk redirects to <http://kingprivatebnk.co.uk/hm3re>, a server that no longer exists. The domain kingprivatebnk.co.uk was suspended in May 2013, which suggests that 23.94.244.18 was involved in fraud at that time.



Name	Last modified	Size	Description
Parent Directory		-	
barclaysbnk.co.uk/	29-Aug-2014 05:23	-	
ncbchina.cn/	29-Aug-2014 09:59	-	

Apache/2.2.3 (CentOS) Server at 23.94.244.182 Port 80

Washington Security Company Reports Compromise of Hong Kong Democracy Websites

[<web-link for this article>](#)

Steven Adair of Volexity, a Washington, D.C. based security firm, has reported the addition of malicious code to legitimate javascript on the websites of three Hong Kong democracy-related websites, and a malicious iframe on a fourth site.

Writing in his [security blog](#), [Steven Adai](#) reported that the Alliance for True Democracy (ATD) in Hong Kong (www.atd.hk), the Democratic Party Hong Kong (DPHK) (www.dphk.org | eng.dphk.org), People Power in Hong Kong (PPHK) (www.peoplepower.hk) and the Professional Commons (PC) (www.procommons.org.hk) websites had been compromised.

The ATD and DPHK both had additional javascript added that loaded additional javascript from java-se.com, a know-malicious site. Several pages of the PPHK website had malicious iFrames leveraging the Chinese URL shortener 985.so added. The iframes redirected to exploit pages on a Hong Kong IP address, 58.64.178.77, designed to install malware on the visitor's system. The PC website had suspicious JavaScript code that wrote an iFrame pointing back to a non-existent HTML page on a hotel website in South Korea.

Visitors to the sites when the exploits were active would have risked infection by unknown malware.

Sources in Hong Kong reported that the sites had been cleaned up and, at the time of writing, all the websites appeared clean.

More Information

[Hong Kong democracy activist websites compromised](#)

[Democracy in Hong Kong Under Attack](#)

[Alliance for True Democracy](#)

[Hong Kong's pro-democracy websites riddled with malware](#)

[Democratic Party](#)

[People Power](#)

[The Professional Commons](#)

HKMA warns about fake Bank of China and Wells Fargo Websites

[<web-link for this article>](#)

The Hong Kong Monetary Authority (HKMA) has issued warnings about two fraudulent webpages; one that mimics the official website of Bank of China (Hong Kong) Limited (BOCHK) and one that mimics the official website of Wells Fargo Bank, National Association (Wells Fargo). BOCHK and Wells Fargo have clarified that they have no connection with the fraudulent website and the police are investigating.

Anyone who has submitted personal information to or has conducted financial transactions through the websites should contact BOCHK at 3988 2388 or Wells Fargo at 2509 6036 and any local Police Station or the Commercial Crime Bureau of the Hong Kong Police Force at 2860 5012.

The [fake BOCHK site](http://ibc.bcdirecthk.com/Obs_lgn_Secure.php) was located at http://ibc.bcdirecthk.com/Obs_lgn_Secure.php and hosted in the British Virgin Islands. One interesting feature of the page was that the top item in the What's New sidebar was dated July 2014, suggesting the page had been active for some time, but not updated. The fake Wells Fargo site was on a .hk domain, and hosted at a local ISP.

Companies should remember that, even if their website is outdated and unpopular, they remain an attractive target for criminals who are looking for convenient sites to host their fraudulent pages.

More Information

Fraudulent website: http://ibc.bcdirecthk.com/Obs_lgn_Secure.php

Fraudulent website: <http://i-show.hk/arise/wellsfargo/>



Security Down Under: AVAR 2014, Sydney Conference Preview

[<web-link for this article>](#)

It is less than a fortnight to the 17th Association of anti-Virus Asia Researchers International Conference. The keynote speaker, InfoSecurity Europe Hall of Fame inductee Graham Cluley will pass on his accumulated experience of 20 years working in companies such as Sophos, McAfee and Dr. Solomon's.

Over the 13th and 14th of November, Mr. Cluley will be joined by 30 other speakers at the Sheraton on the Park in two tracks, covering all the hottest topics in security. Local speakers include Dr. Andrew Clark (CERT Australia) and Alex Tilley (Australian Federal Police). Technical presentations cover mobile platforms, zero days, APTs, botnets. The vulnerabilities of financial systems, hardware and the Internet of Things will be explained. Check the [full agenda of Day 1](#) and [Day 2](#).

If you need to keep up-to-date with the threats that affect your organisation, where better to go than a gathering of top researchers from Government, NGOs, and global and regional

companies including IBM, ESET, McAfee, K7 Computing, Sophos, Trend Micro, Symantec, Ahnlab, Quick Heal, Microsoft, Kaspersky, Intel and others?

More information

[AVAR 2014 Abstracts](#)

[AVAR 2014 Day 1 Agenda](#)

[AVAR 2014 Day 2 Agenda](#)

[AVAR 2014 Venue & Accommodation](#)



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/>

