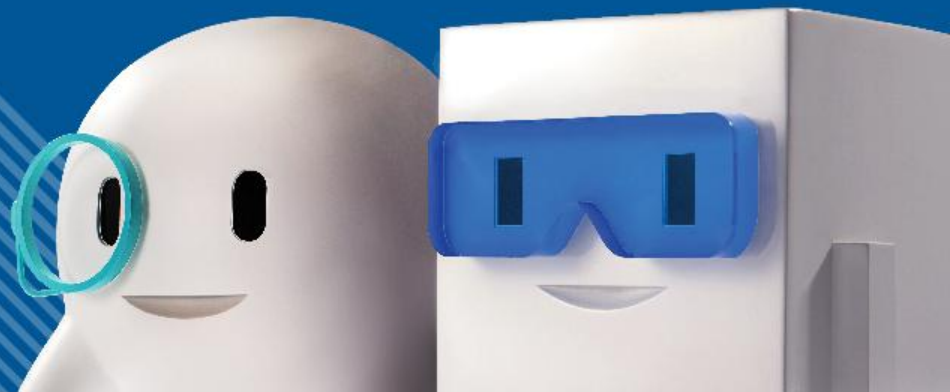




Cyber Security Risks and Mitigation for SME



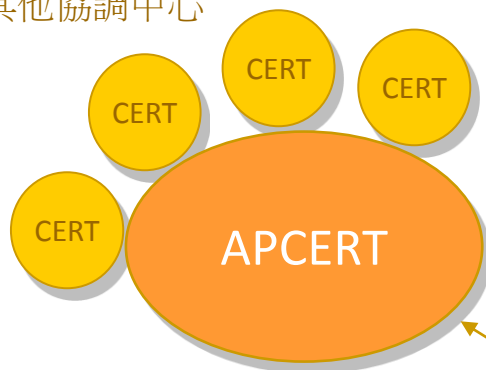
Agenda

- Introduction of HKCERT
- Security Challenges to SMEs
- How do hackers attack you?
- Security Mitigation Measures and Tips
- Q & A

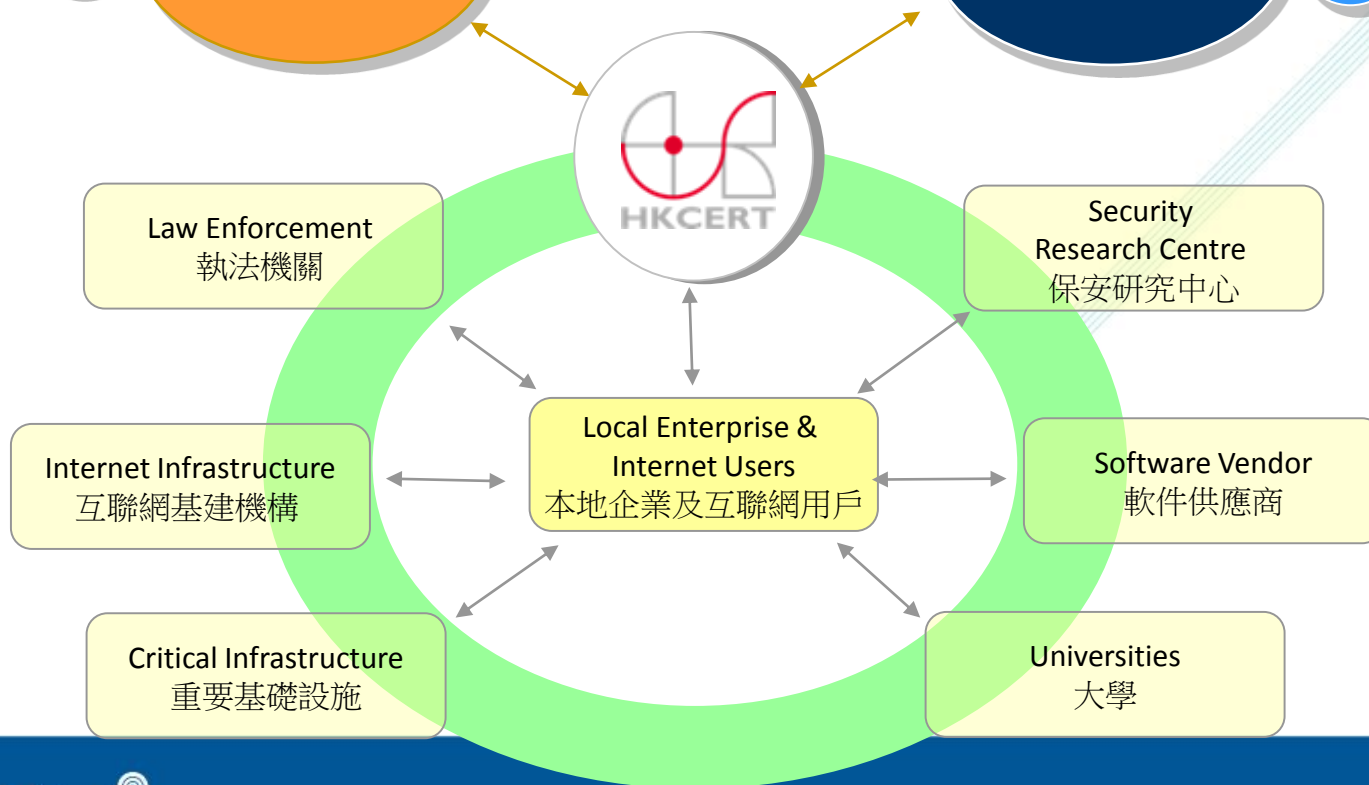
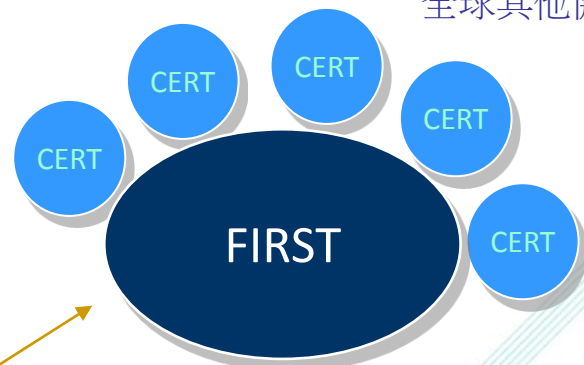
Introduction of HKCERT

- HKCERT
 - Established in 2001. Operated by HK Productivity Council
 - Provide Free-of-charge service to Public
 - Scope of services
 - Incident Handling, Response and Coordination
 - Dissemination of Alerts, Warnings and Security-related Information
 - Security Awareness Education
 - Coordination and Collaboration with Relevant parties on Security Preventive Measures
 - 24 hrs hotline: 8105-6060

CERT Teams in Asia Pacific
亞太區其他協調中心

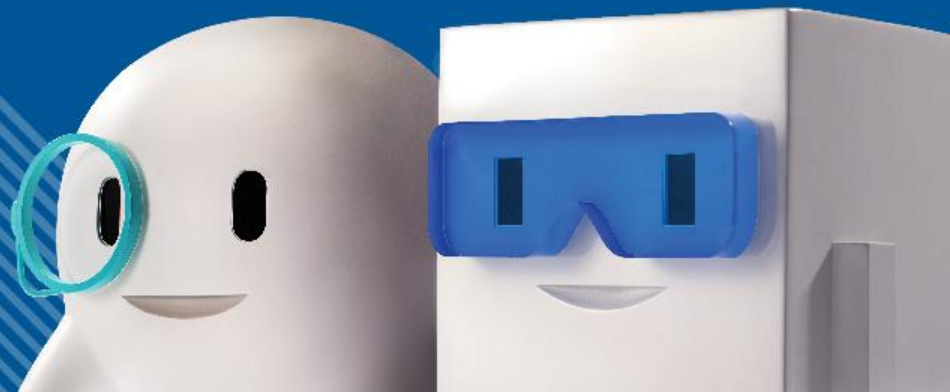


CERT Teams around the World
全球其他協調中心





Security Challenges to SMEs

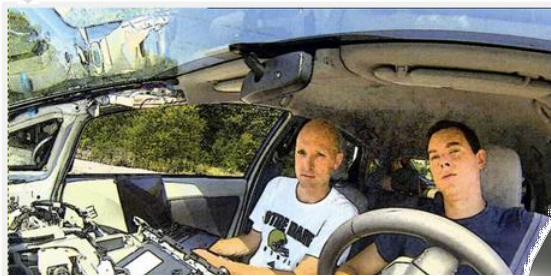


Nothing cannot be hacked

Hackers Reveal Nasty New Car Attacks--With Me Behind The Wheel (Video)

This story appears in the August 12, 2013 issue of Forbes.

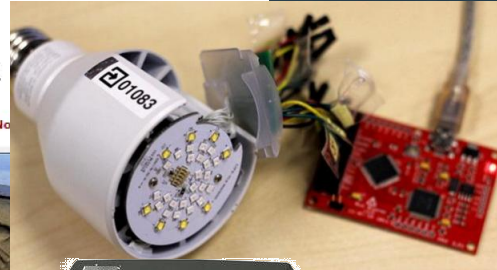
136 comments, 43 called-out + Comment No



Philips Smart TVs vulnerable to Screen Hijack
Cookie Theft

Saturday, March 29, 2014 Wang Wei

344 Like 579 Share 98 Tweet 159 Reddit 3 share 20 ShareThis



Students Fake GPS Signals to 'Hijack'
\$80 Million Yacht - Networkworld July
29, 2013



Trustwave SpiderLabs Security Advisory
TWSL2013-020:

SME

- SMEs are facing the same threat as large enterprise.
 - Data Leakage. (sensitive data such as staff, customer, business proprietary info.)
 - Down time (web and email)
 - Reputation loss (turn away new and existing customers)
- Security Challenge of SME
 - Lack of resources (budgets and manpower)
 - Lack of IT and information security expertise
 - Lack of security awareness

Attackers and Motives

- Unfriendly Parties: Damage Reputation and Business Interests
 - Disgruntled employees, business competitors..
- Cybercriminals: Money
 - Extortion (Ransomware, DDoS...)
 - Theft of information for \$\$\$
 - Control machine for other purposes

Cybercrime-as-a-Service

Russian Cybercriminal Underground Market Product Offerings

Product	2011 Price	2012 Price	2013 Price
---------	------------	------------	------------

Russian Cybercriminal Underground Service Offerings

Service	2011 Price	2012 Price	2013 Price
Dedicated-/Bulletproof-server hosting <ul style="list-style-type: none"> • Low-end • High-end • Virtual private server (VPS) 	US\$160 US\$450 US\$70	US\$100 US\$160 US\$40	US\$50 US\$190 US\$12+
Proxy-server hosting (per day): <ul style="list-style-type: none"> • HTTP/S • SOCKS 	US\$2 US\$2	US\$1 US\$2	US\$1 US\$2
VPN-server hosting: <ul style="list-style-type: none"> • With one exit point • With an unlimited number of exit points and traffic • Average price 	US\$8–12 US\$40 US\$22	No data US\$38 US\$20	No data US\$24 US\$15
Traffic-to-download conversion (PPI per 1,000 installations): <ul style="list-style-type: none"> • Australia traffic • U.K. traffic • U.S. traffic • Europe traffic • Mixed global traffic • Russia traffic 	US\$300–500 US\$220–300 US\$100–150 US\$90–250 US\$12–15 US\$100–500	US\$200–500 No data US\$100–250 US\$75–90 US\$10–17 US\$100–190	US\$120–600 US\$150–400 US\$120–200 US\$50–110 US\$10–12 US\$140–400

(Source from TrendMicro)

Email Password Cracking made easy..!!

Request an E-mail Password :-

Fill in the below form to the best of your knowledge. Make sure that the email addresses are entered correctly. Once submitted, check your email for a confirmation mail. Add our email address(es) in your address-book, to prevent our emails and the proofs landing in bulk folder. Once you verify the order by clicking on the confirmation link sent to you, we will process your order.

Your Name

Your Email Address

Confirm your Email Address

Your Country

☐ Most Urgent
 ☐ Urgent
 ☐ Just do it whenever you can

Victim Name

Victim Email Address

Confirm Victim Email Address

Victim Victim Country

Victim Language

Optional Information :-

How you know us

Your Yahoo! Chat ID

Your MSN Chat ID

Preferred Mode of Payment

Bonus offered (if any)

Any Instructions ?

(Source from McAfee)

Cybercrime-as-a-Service

Distributed Denial-of-Service Service Prices

Offering	Price
1-day DDoS service	US\$30-70
1-hour DDoS service	US\$10
1-week DDoS service	US\$150
1-month DDoS service	US\$1,200

(Source from TrendMicro)

Prices for stolen credit card numbers.

Dumps	Estimate of Prices (without PIN, with PIN, PIN and good balance)									
	US		EU			CA, AU		Asia		
Visa Classic	\$15	\$80	\$40	\$150		\$25	\$150	\$50	\$150	
Master Card Standard		\$90		\$140			\$150		\$140	
Visa Gold/Premier	\$25	\$100	\$200	\$45	\$160	\$250	\$30	\$160	\$55	\$150
Visa Platinum	\$30	\$110		\$50	\$170		\$35	\$170	\$60	\$170
Business/Corporate	\$40	\$130		\$60	\$170		\$45	\$175	\$70	\$170
Purchasing/Signature	\$50	\$120		\$70			\$55		\$80	
Infinite				\$130	\$190		\$60	\$200		\$190
Master Card World		\$140								
AMEX	\$40			\$60			\$45		\$70	
AMEX Gold	\$70			\$90			\$75		\$100	
AMEX Platinum	\$50									

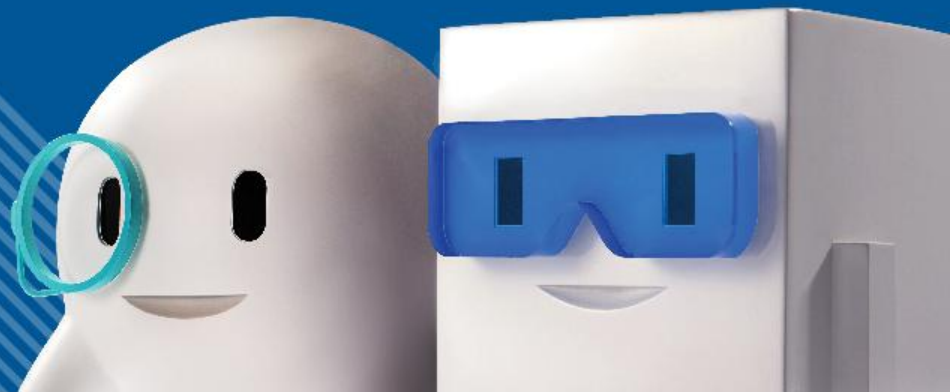
(Source from McAfee)

Prices for zero-day vulnerabilities.

Adobe Reader	\$5,000–\$30,000
Mac OS X	\$20,000–\$50,000
Android	\$30,000–\$60,000
Flash or Java Browser Plug-ins	\$40,000–\$100,000
Microsoft Word	\$50,000–\$100,000
Windows	\$60,000–\$120,000
Firefox or Safari	\$60,000–\$150,000
Chrome or Internet Explorer	\$80,000–\$200,000
iOS	\$100,000–\$250,000



How do hackers attack you?



Attacks tactics

- Social Engineering (use human vulnerabilities)
 - Phishing website and email – Spoofed identity
- Malware & Botnet
 - Steals confidential information, damage system data and software on the computer
 - Malware causes victim PC and becoming part of Botnet
- Network Attack
 - Eg. DDoS, No data is stolen or compromised, but the interruption to the service can be costly for a company.
 - Eg. Server Hacking, may have data loss or compromised for malicious activity, such hosting phishing , malware file etc.

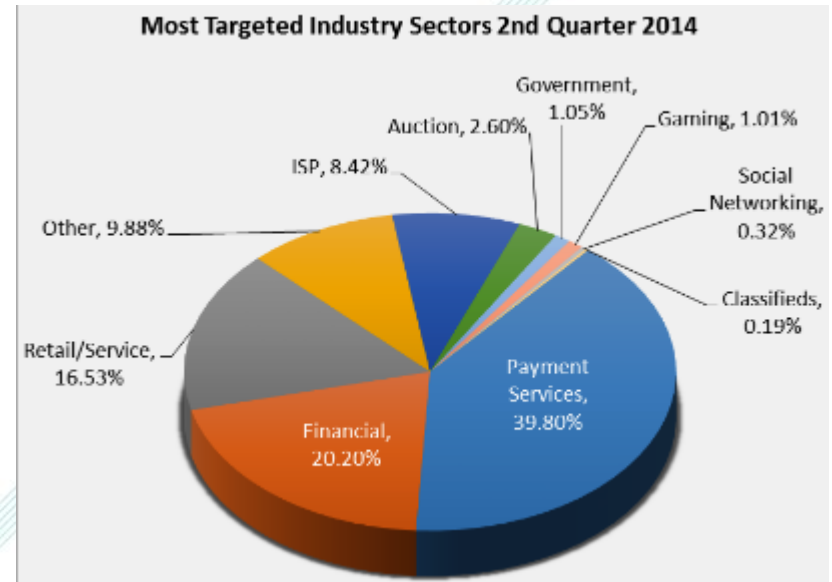
Phishing

APWG Phishing Attack Trends Reports 2Q2014 (Released Aug 29, 2014)



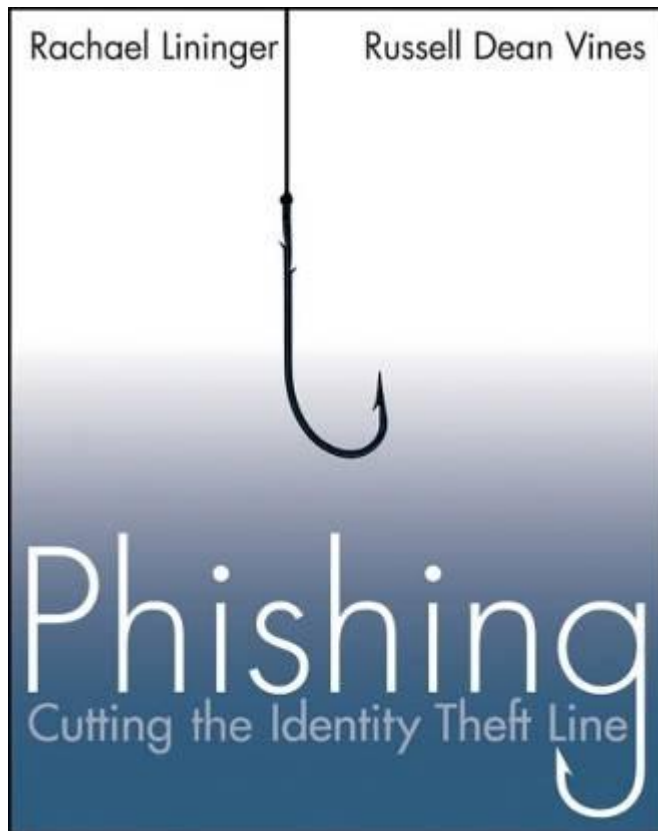
- Average detected ~42K Phishing websites
- Most-Targeted Industry Sectors
 - ✓ Payment Services – 39.8%
 - ✓ Financial – 20.20%
 - ✓ Retail/Service – 16.53%

<http://www.apwg.org/resources/apwg-reports>



Phishing Website

Spoofer website → lure user to input username, password, credential



 HONG KONG MONETARY AUTHORITY
香港金融管理局

RSS | 我的自訂色彩

關於金管局 | 主要職能 | 刊物與研究資料 | 市場數據與統計資料

主頁 / 主要資訊 / 新聞稿類別

新聞稿

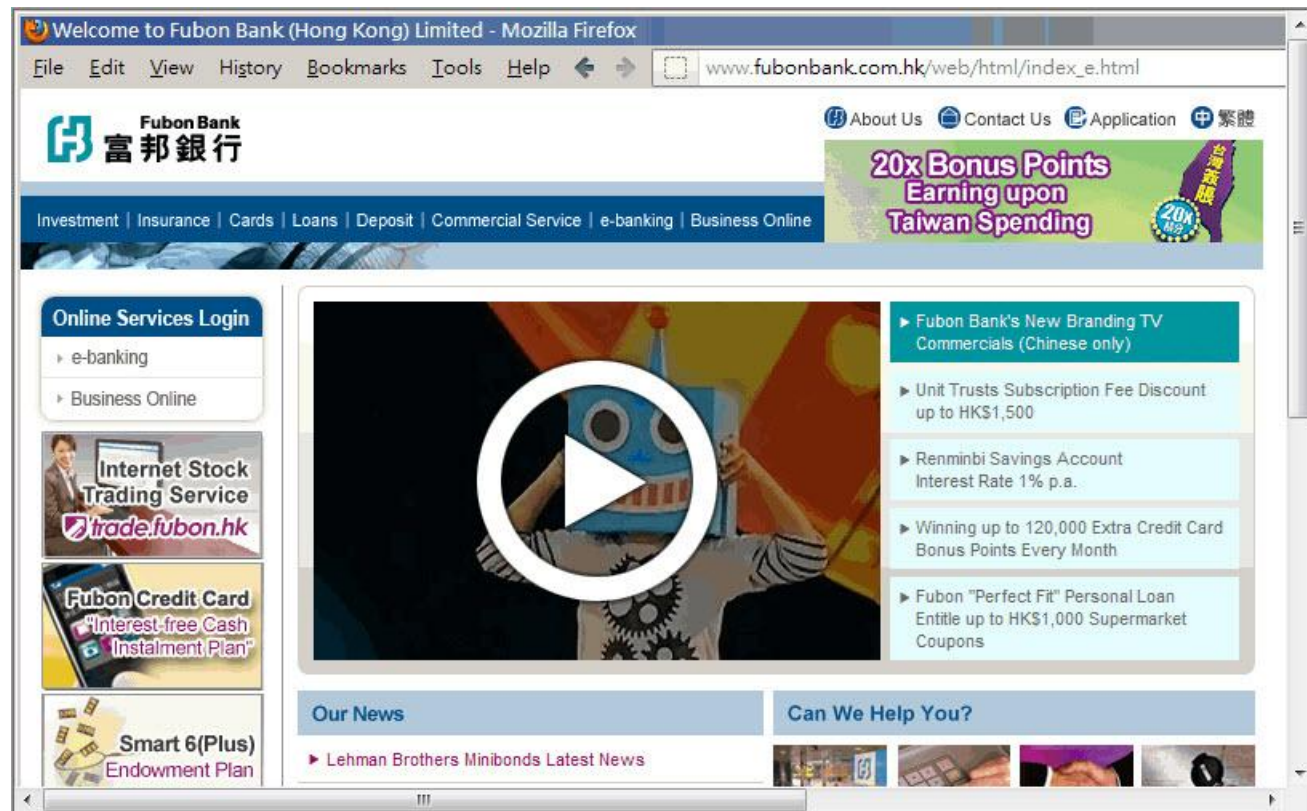
年份 -- | 類別

欺詐網站、電郵、電話系統及其他騙案

2015年1月9日	欺詐網站「 http://hsplbk.com/bank.hangseng.com/1/2/personal/private-banking/private-banking.html 」
2014年12月15日	欺詐網站「 http://www.wlpbhk.com/ 」
2014年11月28日	欺詐網站「 http://bank.cncbnkintl.com 」
2014年11月25日	欺詐網站「 http://cccmkc.hk/templates/rhuk_milkyway/index.htm 」
2014年11月21日	欺詐網站「 http://www.standardcharteredv.com/hk 」
2014年11月4日	欺詐網站「 http://www.maydanhgiay.org/ibank/schk/login/index.html 」
2014年10月31日	聲稱與花旗銀行(香港)有限公司有關的欺詐電郵

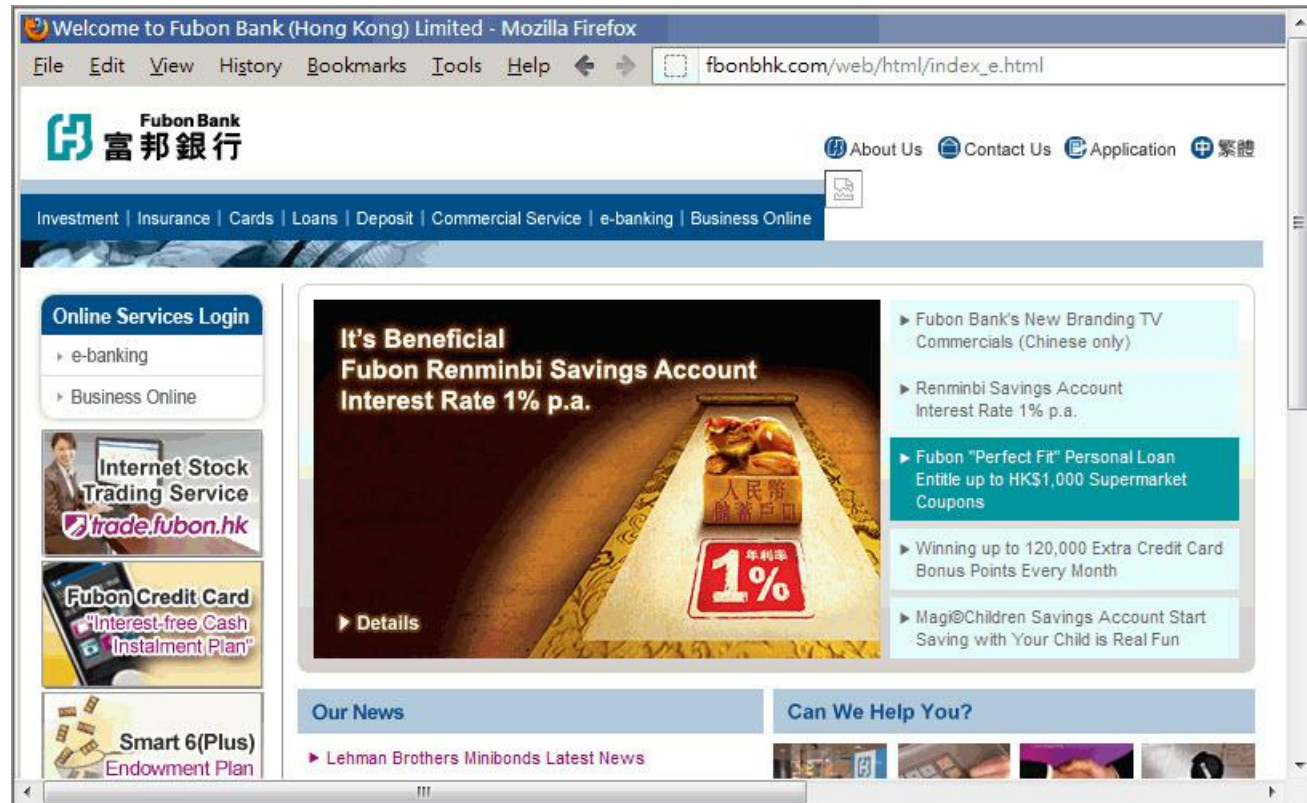
Which one is Phishing Website (釣魚網站) ??

A.



Which one is Phishing Website (釣魚網站) ??

B.



Which one is Phishing Website (釣魚網站) ??

C.



Which one is Phishing Website (釣魚網站) ??



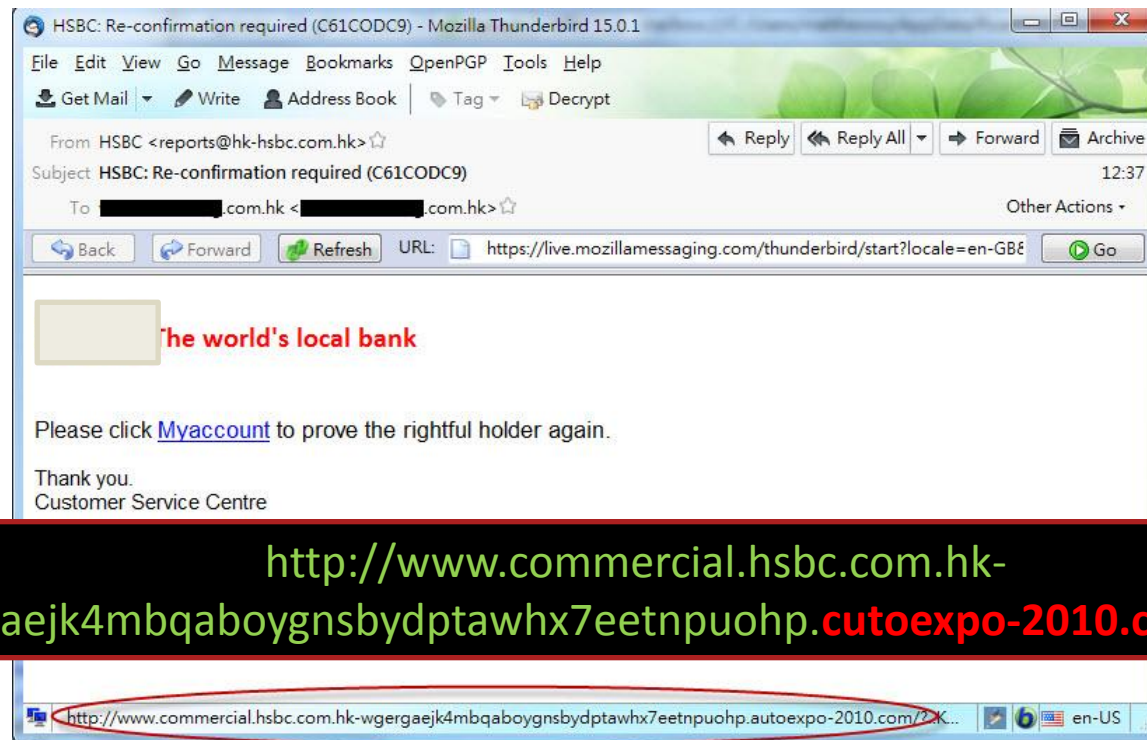
Which one is Phishing Website (釣魚網站) ??



Phishing Website (釣魚網站)



Phishing Email (釣魚電郵)



Spoof email sender → lure to install Malware or visit a Phishing website
→ user get infected.

Malware Propagation channels

Executables

Document
Malware

Website

- Fake security software
- Fake video player codec
- Social network website redirect



Malware Propagation channels

Executables

Document
Malware



Website



Malware Propagation channels

Executables

Document
Malware

Website



- **Legitimate and trusted websites compromised**
- **Web admin incapable to detect and mitigate the risks**

BotNet targeting Banks and e-Commerce

- Zeus, SpyEye, Citadel Botnets
 - Steals online banking information by Key logging and Form Grabbing
 - Features:
 - Take screenshot (save to html without image)
 - Redirect to a prepared fake bank webpage
 - Hijack login session and modify web page
 - **Log the visiting information of e-banking site**, record the input string (text or post URL)

Ransomware

- Encryption Ransomware
 - 2013 > CryptoLocker (PC)
 - 2014 > BitCrypt (PC)
 - 2014 > CyptoDefense (PC)
 - 2014 > Synolocker (NAS)
 - 2014 > Simplocker (Mobile)
 - 2014 > CryptoGraphic Locker (New*)



Beware of Encryption Ransomware, Do data protection now
https://www.hkcert.org/my_url/en/blog/14041401

Ransomware

Your files are encrypted.

To get the key to decrypt files you have to pay **500 USD/EUR**. If payment is not made before **02/04/14 - 09:03** the cost of decrypting files will increase 2 times and will be **1000 USD/EUR**.

Your system: Windows XP (x32) First connect IP: [REDACTED]

[Refresh](#) [Payment](#) [FAQ](#) [My screen](#) [Test decrypt](#)

We present a special software - CryptoDefense Decrypter - which is allow to decrypt
How to buy CryptoDefense decrypter?

SynoLocker™

Automated Decryption Service

All important files on this NAS have been encrypted using strong cryptography



1. You should register Bitcoin wallet ([click here for more information](#) with

2. Purchasing Bitcoins - Although it's not yet easy to buy bitcoins, it's getting easier. Here are our recommendations:

- [LocalBitcoins.com](#) - This fantastic service allows you to search for people in your area who are willing to sell bitcoins to you directly.
- [How To Buy Bitcoins](#) - An international directory of bitcoin exchanges.
- [Cash Into Coins](#) - Recommended for fast, simple service.
- [Coinbase](#) - Bitcoin exchange based in the United States. (Highly rated).
- [BitStamp](#) - A multi currency bitcoin exchange based in Slovenia. (Highly rated).
- [CoinJar](#) - CoinJar allows direct bitcoin purchases on their site. They're based in the UK and have a large international clientele.

3. Send 1.09 BTC to Bitcoin address: **1EmLLj8peW292zR2VvnnYPPa9wL**

4. Enter the Transaction ID and select amount:

Note: Transaction ID - you can find in detailed info about transaction you made.
(example 44214efca56ef039386ddb929c40bf34f19a27c42f07f5cf3e2aa08114c4d)

5. Please check the payment information and click "PAY".

PAY

List of encrypted files available [here](#).

Follow these simple steps if files recovery is needed:

1. Download and install [Tor Browser](#).
2. Open Tor Browser and visit <http://cypherxfttr7hho.onion>. This link works **only** with the [Tor Browser](#).
3. Login with your identification code to get further instructions on how to get a decryption key.
4. Your identification code is [REDACTED] (also visible [here](#)).
5. Follow the instructions on the [decryption page](#) once a valid decryption key has been acquired.

Technical details about the encryption process:

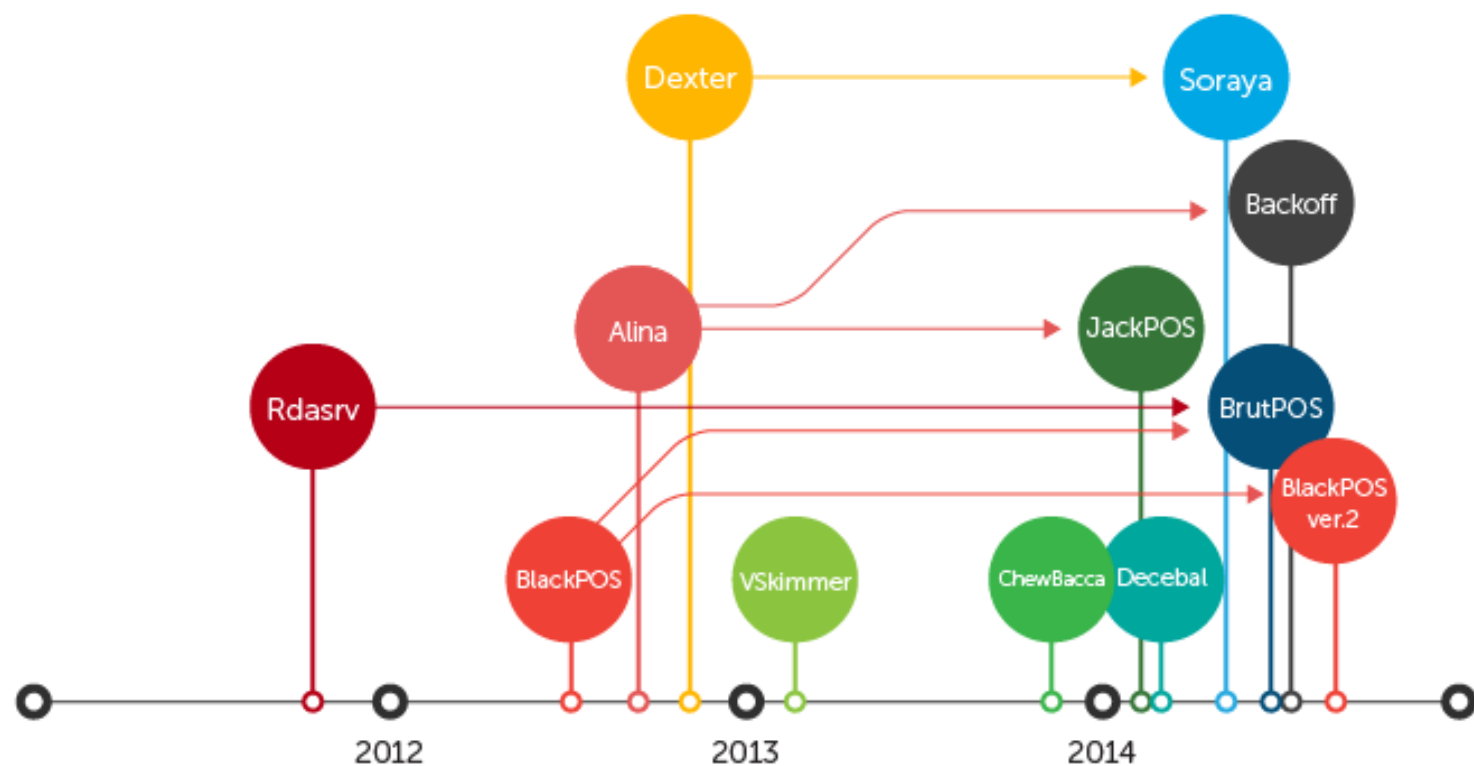
- A unique RSA-2048 keypair is generated on a remote server and linked to this system.
- The RSA-2048 public key is sent to this system while the private key stays in the remote server database.
- A random 256-bit key is generated on this system when a new file needs to be encrypted.
- This 256-bit key is then used to encrypt the file with AES-256 CBC symmetric cipher.
- The 256-bit key is then encrypted with the RSA-2048 public key.
- The resulting encrypted 256-bit key is then stored in the encrypted file and purged from system memory.
- The original unencrypted file is then overwritten with random bits before being deleted from the hard drive.
- The encrypted file is renamed to the original filename.
- To decrypt the file, the software needs the RSA-2048 private key attributed to this system from the remote server.

Point of Sales (POS) Malware

- Support various payment methods and increase attack surfaces
- Support various business needs and not only store financial data but also personal data
- Connected to corporate network through the Internet
- RAM (memory) scraping malware



Retail POS Malware



Source: TrendMicro

Website defacement (網頁塗改)

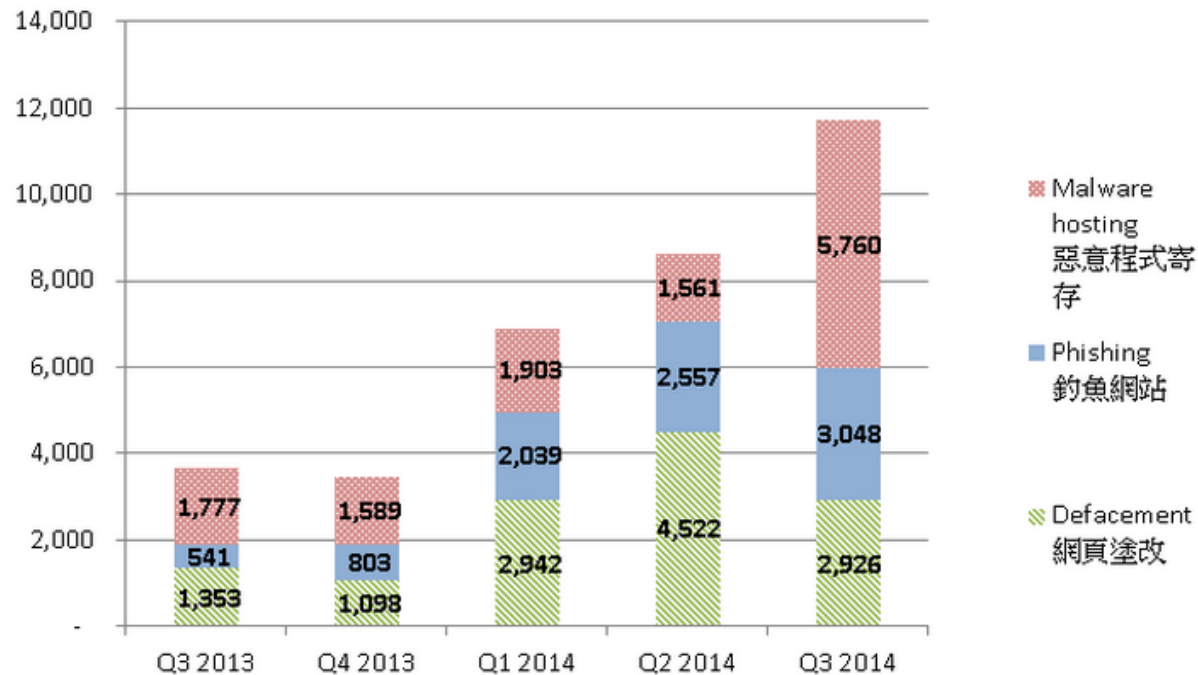
An attack on a website that changes the visual appearance of the site or a webpage



HKCERT Security Watch Report

Trend and Distribution of server related security events

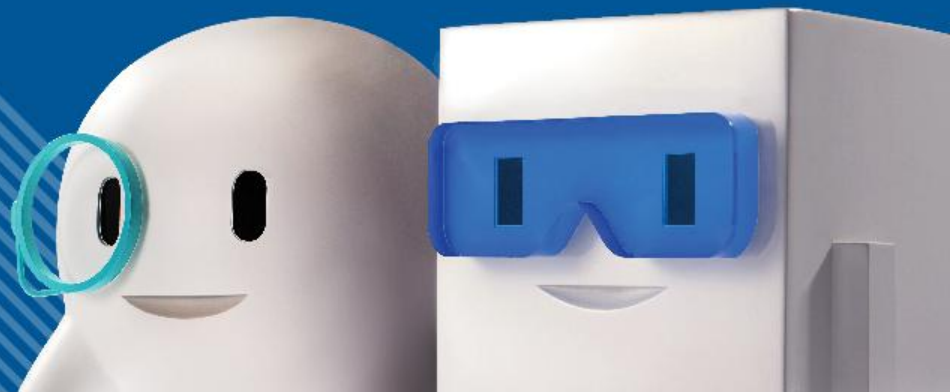
與伺服器有關的安全事件的趨勢和分佈



HKCERT – Hong Kong Security Watch Report Q3 - 2014

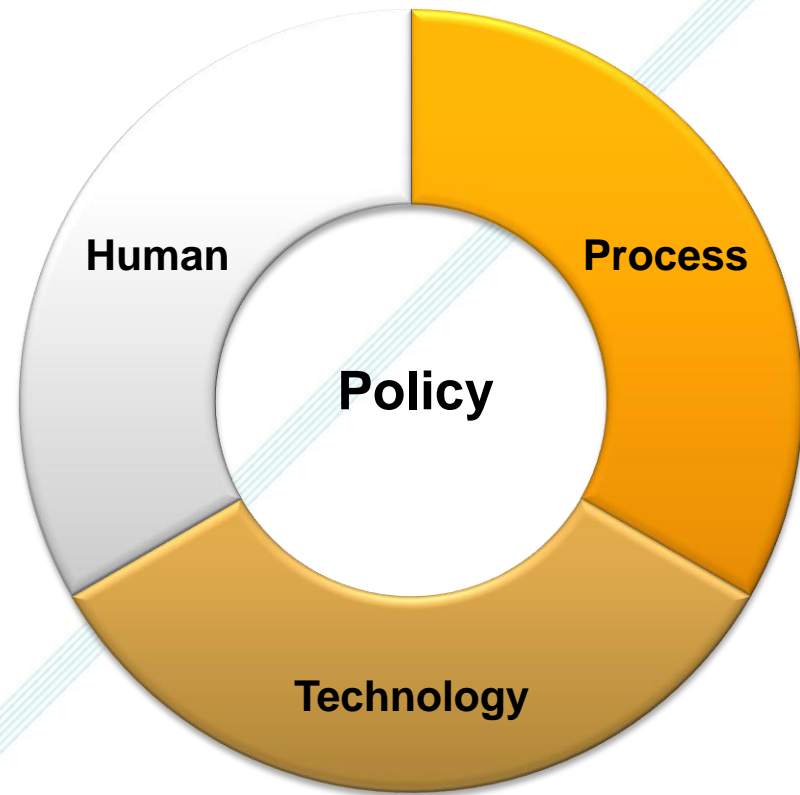


Security Mitigation Measures and Tips



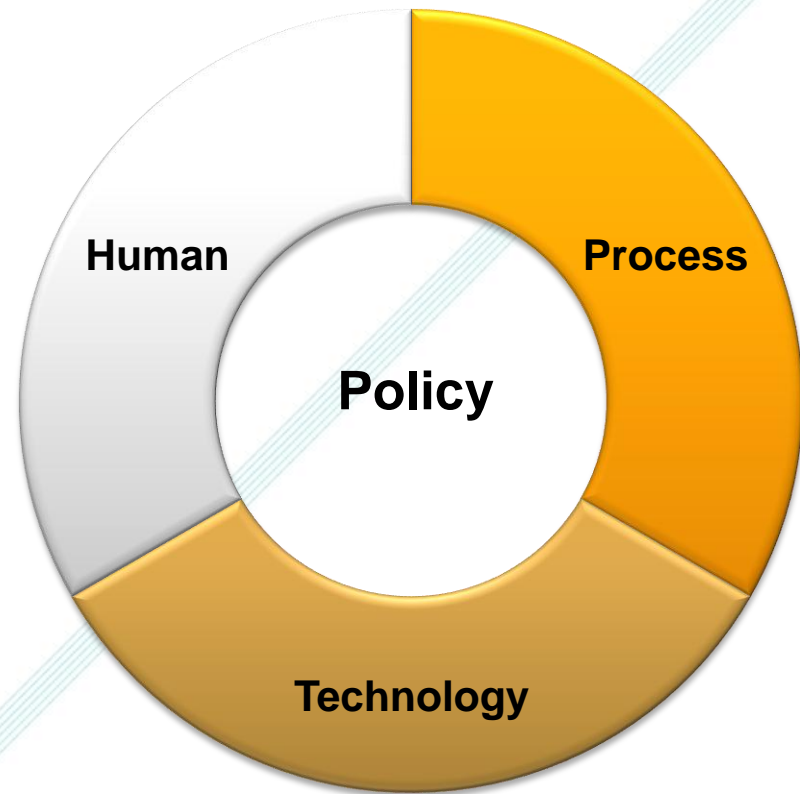
Security Practice

- **Process**
 - Download apps/software from official website
 - Password lock / screen lock
 - Patch frequently
 - No jailbreak/root mobile device
 - Close unnecessary network (Wi-Fi, Bluetooth)
- **Technology**
 - Security software
 - Found my phone
 - Encryption (File and USB storage device)



Security Practice

- Human
 - Avoid loss and theft
 - Be careful of phishing website/email
 - Stop → Think → Connect
- * Data Backup & Recovery
 - * Backup important file regularly
 - * Protection on backup (Offline backup?)
 - * Recovery test.
- * Stay Alert and Keep Updated
- Report incident and Know where to get Assistance



IT Security Assessment

- Evaluate organizations security framework against common industry standards as well as other companies of similar size, industry and geography.
- Helps organizations reduce risk exposure, protect information assets and limit the impact of security-related events on business activity.

Evaluates 14 priority information security risk areas

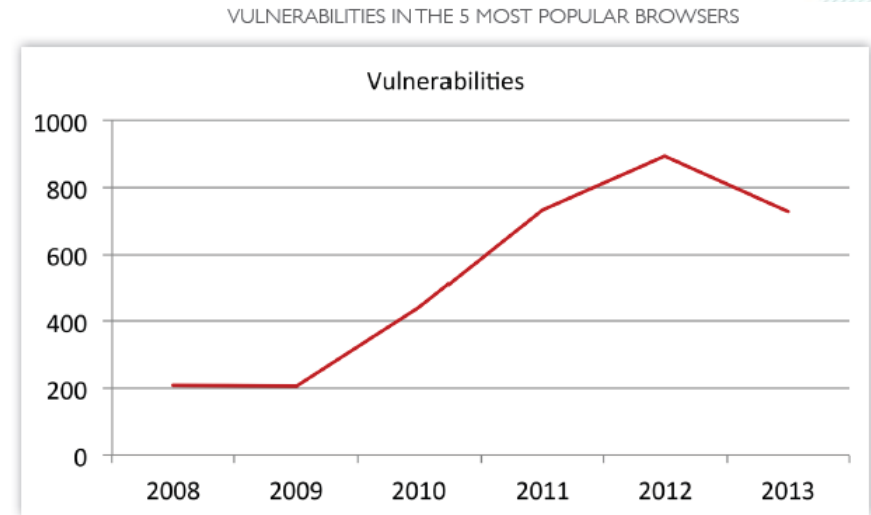
- | | |
|--|-----------------------------|
| • Physical Security | • Web Application Security |
| • Logical Security | • End Point Security |
| • Servers & PCs | • File Backup & Recovery |
| • Network Infrastructure | • Wireless Network Security |
| • Security Policies, Procedures, Practices | • AV, Spyware, Spam |
| • Internal Network Vulnerabilities | • Social Engineering |
| • External Network Vulnerabilities | • Software Security |

References

- IT Security Policy and Guidelines - OGCIO
http://www.ogcio.gov.hk/en/infrastructure/methodology/security_policy/
 - Baseline IT Security Policy (S17)
 - IT Security Guidelines (G3)
 - Internet Gateway Security Guidelines (G50)
 - Security Risk Assessment & Audit Guidelines (G51)
 - Information Security Incident Handling Guidelines (G54)

Use Browser Securely

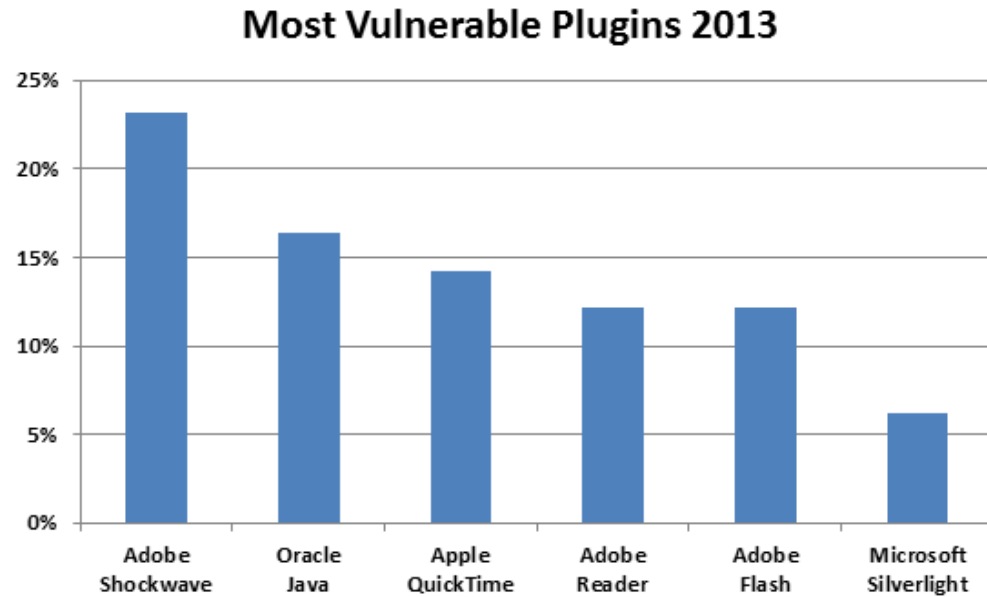
- Use newer and secure browsers
 - Security features: URL blocking, sandbox, private browsing
 - Avoid installing unknown add-ons (extension, ActiveX objects ...) on the browser



Secunia Vulnerability Review 2014

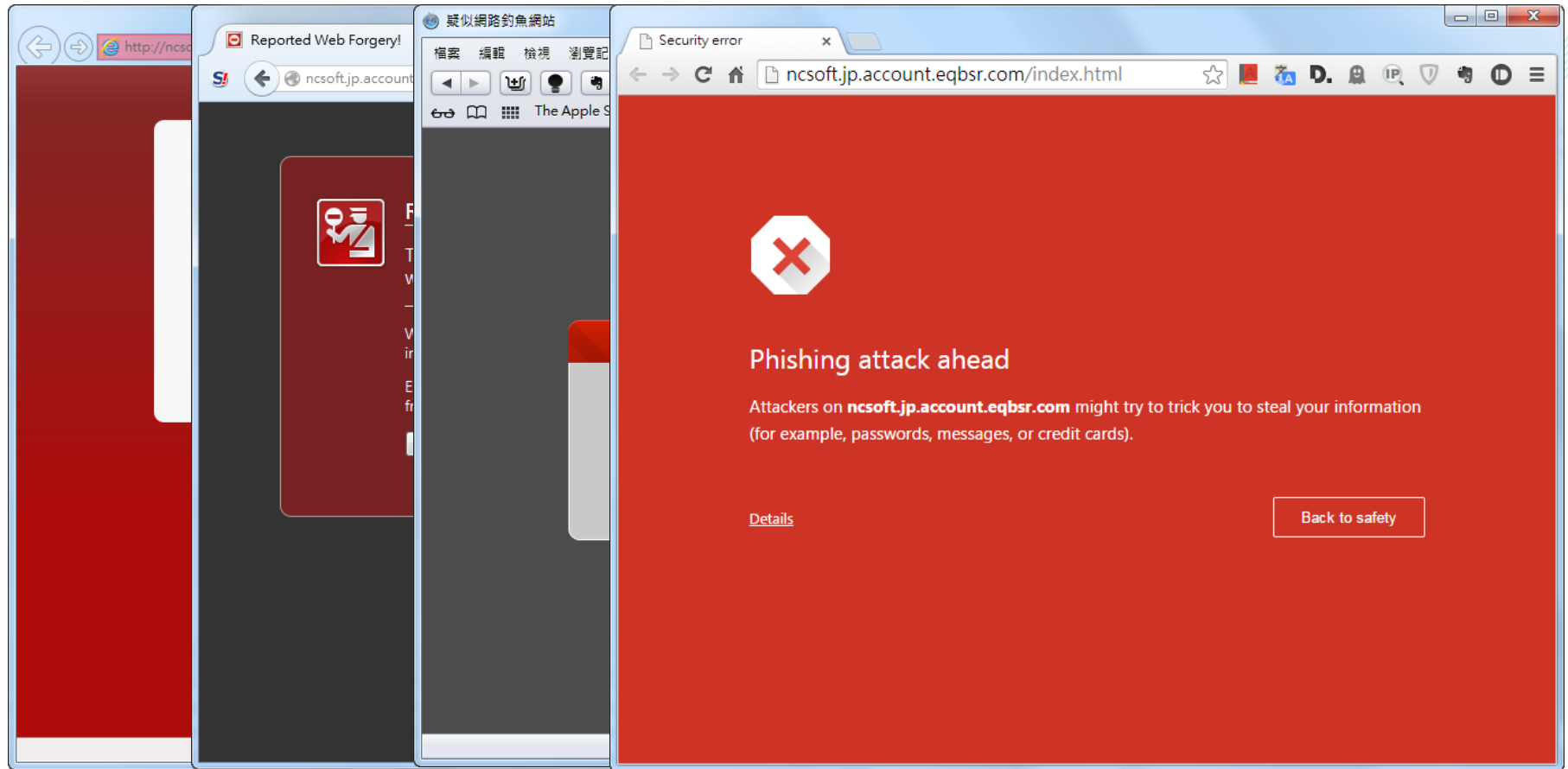
Use Browser Securely

- Use separate browsers for casual browsing and transactions
- Be aware of pop-up window
- Clear browsing history
- Use Private Browsing in public kiosk
- Logout after use

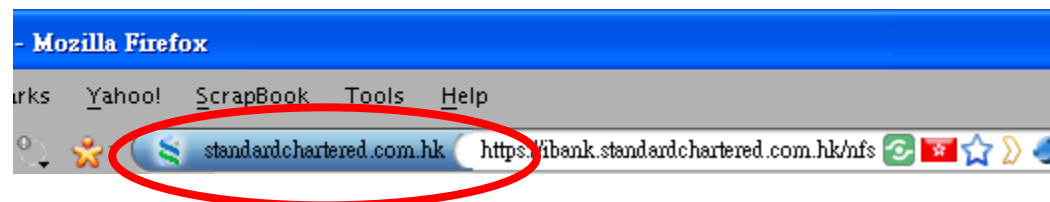


Source: Qualys

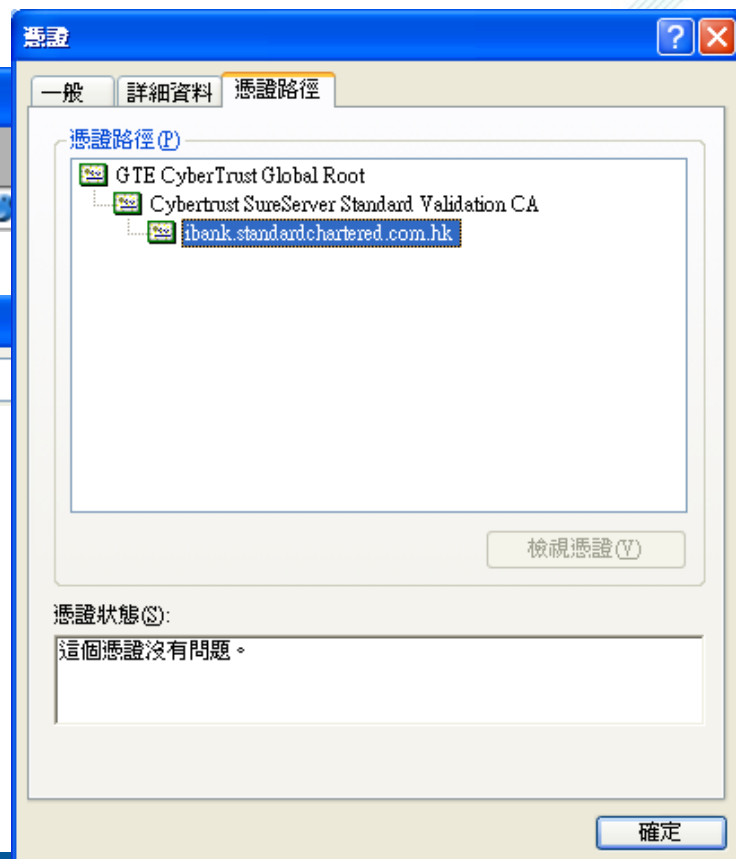
Aware of Browser Security Warnings



Verify web site identity



- SSL (HTTPS) enabled sites provides
 - Encrypted connections
 - Authenticated source
 - Remember to log out when done

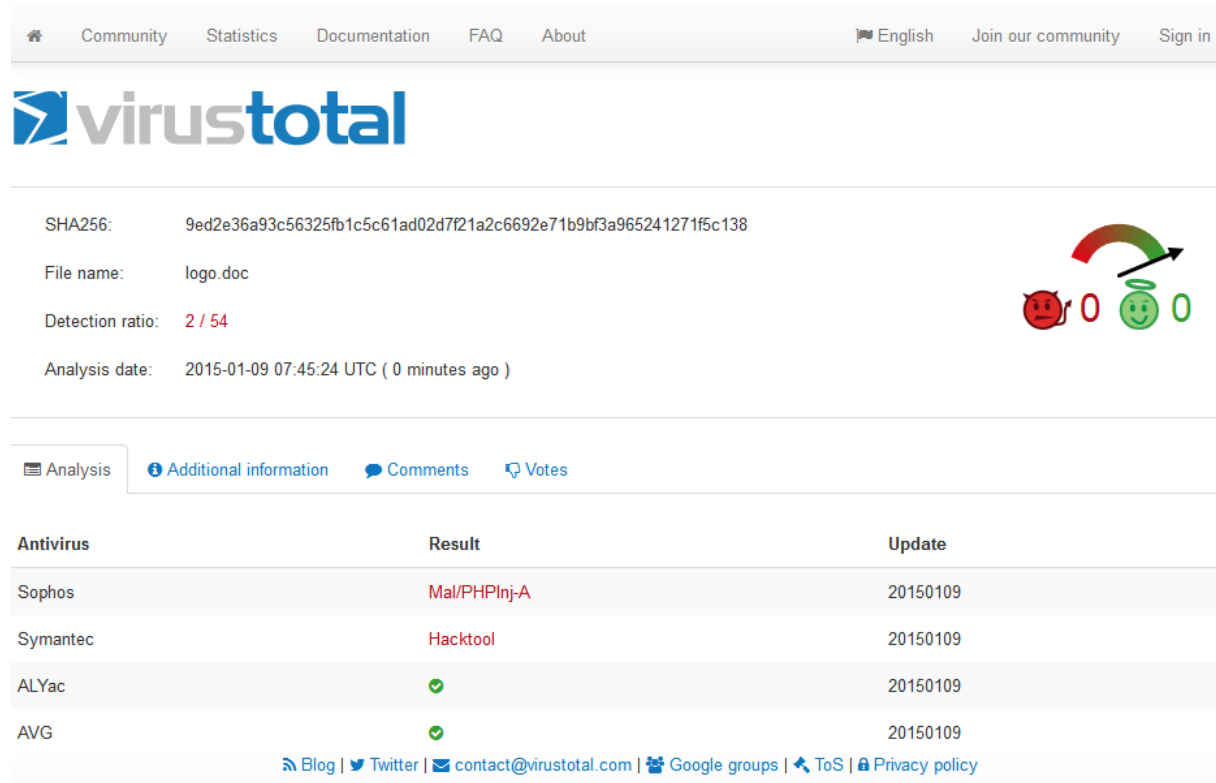


Malware Analysis Website

VirusTotal - Malware analysis website (Free)

- Analyzes suspicious files (computer file and mobile Apps) and URLs

- <https://www.virustotal.com/en/>



The screenshot displays the VirusTotal website interface. At the top, there is a navigation bar with links for Community, Statistics, Documentation, FAQ, and About, along with language and login options. The main header features the VirusTotal logo. Below this, the analysis details for a file are shown: SHA256 hash, file name 'logo.doc', a detection ratio of 2/54 (indicated by a red sad face icon and a green happy face icon), and the analysis date. A progress bar is also visible. The 'Analysis' tab is selected, showing a table of antivirus results. The table has columns for Antivirus, Result, and Update. The results show that Sophos and Symantec detected the file as malware, while ALYac and AVG did not. At the bottom, there are links to the blog, Twitter, contact email, Google groups, ToS, and Privacy policy.

Community Statistics Documentation FAQ About English Join our community Sign in

virustotal

SHA256: 9ed2e36a93c56325fb1c5c61ad02d7f21a2c6692e71b9bf3a965241271f5c138

File name: logo.doc

Detection ratio: 2 / 54

Analysis date: 2015-01-09 07:45:24 UTC (0 minutes ago)

Analysis Additional information Comments Votes

Antivirus	Result	Update
Sophos	Mal/PHPInj-A	20150109
Symantec	Hacktool	20150109
ALYac	✓	20150109
AVG	✓	20150109

Blog | Twitter | contact@virustotal.com | Google groups | ToS | Privacy policy

Website Reputation Check

URLVoid – Check website reputation (Free)

- Scan website address with multiple website reputation engines and domain blacklists

<http://www.urlvoid.com/>

Hkcert.org

No active threats were reported by the scanning engines.

[Free anonymous web proxy »](#)

Update Report

Become a fan on Facebook



Overview

IP Address







Alexa Traffic

Facebook Activity

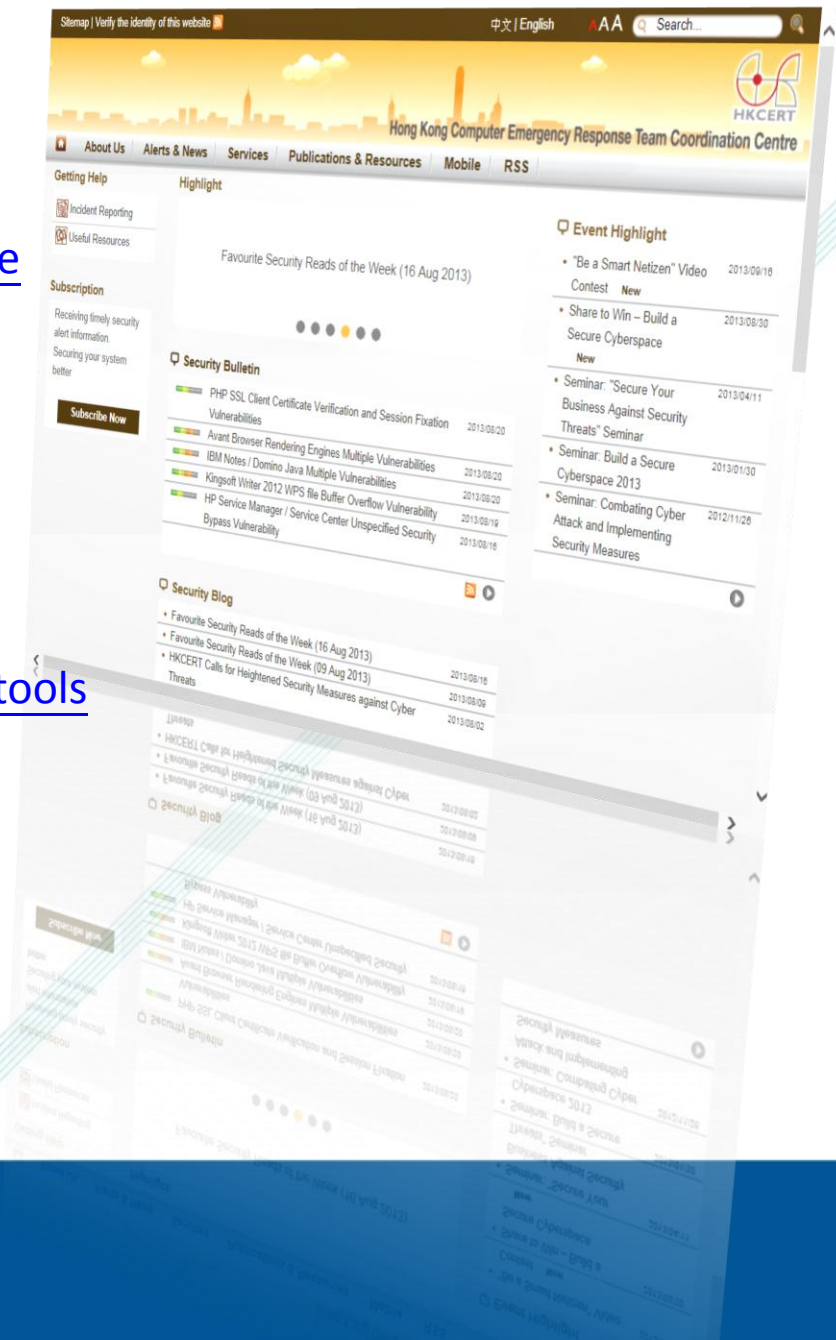
Website Information

Analysis Date	3 months ago
Safety Reputation	0/30
Domain 1st Registered	2002-01-09 (13 years ago)
Server Location	 (HK) Hong Kong
Google Page Rank	
Alexa Traffic Rank	1,466,885

Safety Scan Report

 SpamhausDBL	 View more details...
 MyWOT	 View more details...
 MalwareDomainList	 View more details...

- Security Guideline
 - <https://www.hkcert.org/security-guideline>
- Security Tools
 - <https://www.hkcert.org/security-tools>
- Mobile Security Tools
 - <https://www.hkcert.org/mobile-security-tools>
- HKCERT Mobile App
 - Search by keyword: **HKCERT**



Q & A

Website: www.hkcert.org

Hotline: 8105-6060

Email: hkcert@hkcert.org