

ISP and Cyber Security



SC Leung

Senior Consultant

CISSP CISA CBCP

Who am I?

- ▶ Senior Consultant
 - @HKCERT since 2001
 - International and local liaison, strategic planning, supervision of CERT operation
- ▶ Previous industrial experiences
 - ISP, Telecommunication
 - Multinational Banking
 - Outsourcing Consultancy
 - Software distributor



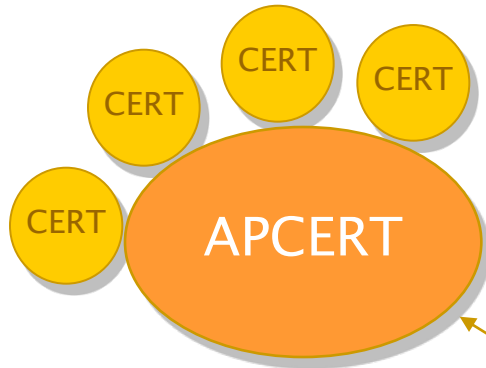
SC Leung

Agenda

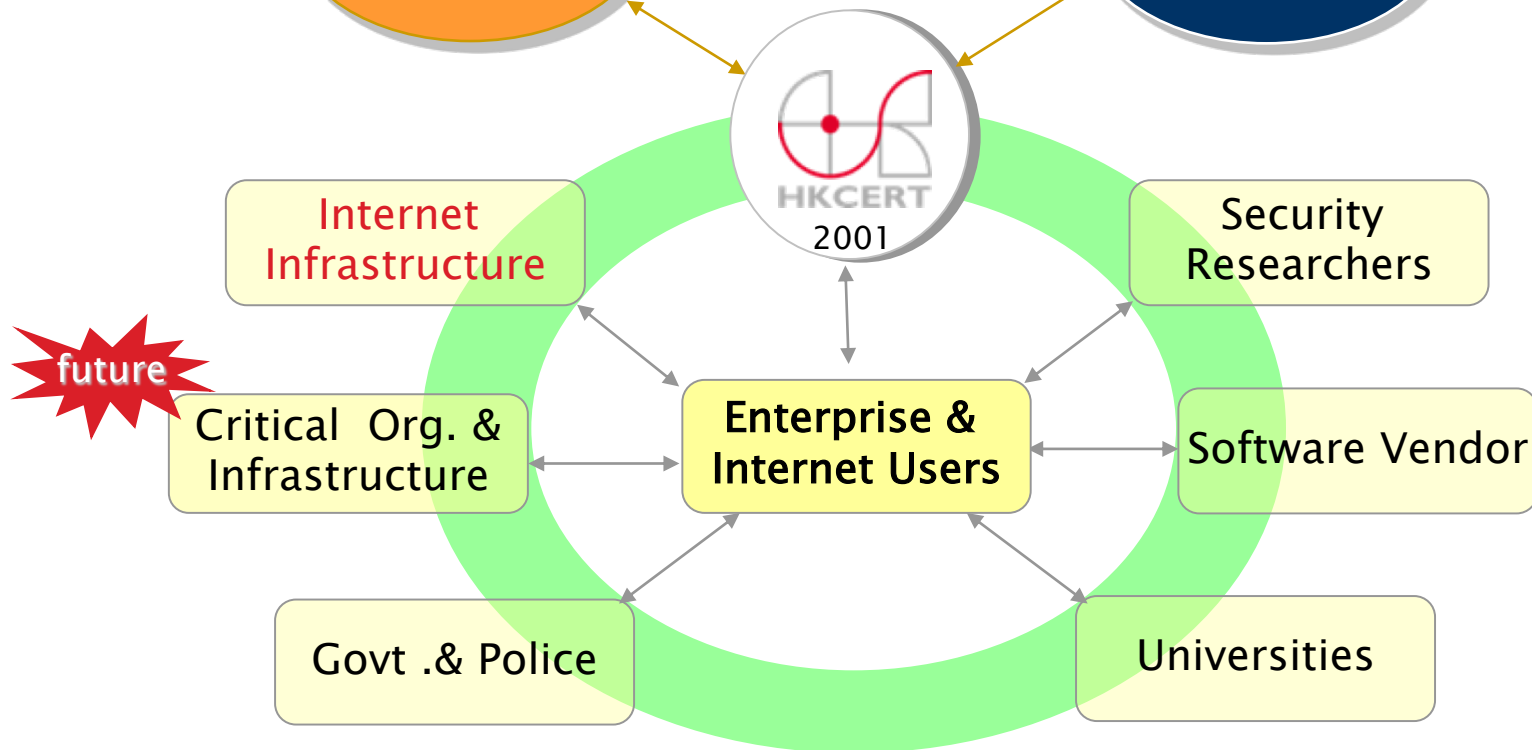
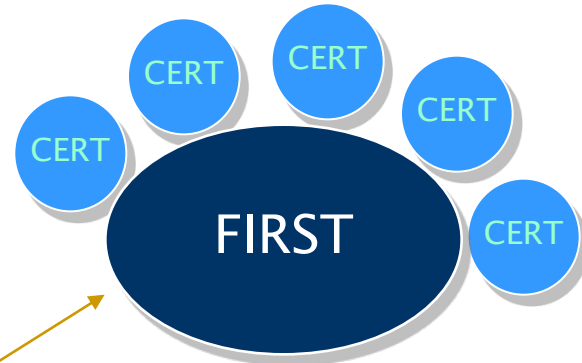
- ▶ Major threats & problems we face today
- ▶ How these problems affect you?
- ▶ What HKCERT is doing to solve them?
- ▶ How you can get involved in solving the problems?

HKCERT as a Coordination Centre

CERT Teams in Asia Pacific



CERT Teams around the World



Services



- ▶ Incident Response
24-hour Hotline: 8105-6060



- ▶ Cross Border Coordination



- ▶ Early Warning and Advices



- ▶ Awareness Education

Security Status of Hong Kong

HKCERT Statistics

Incentive for hackers to pick on Hong Kong

- ▶ Economy with Fastest Average Internet Speed

Country/Region		Q2 '13 Peak Mbps	QoQ Change	YoY Change
1	Hong Kong	65.1	-0.9%	32%
2	South Korea	53.3	19%	14%
3	Japan	48.8	3.1%	21%
4	Romania	47.5	-0.6%	23%
5	Singapore	45.6	4.1%	61%
6	Latvia	44.6	5.4%	33%
7	Switzerland	41.4	3.9%	38%
8	Israel	40.1	6.4%	53%
9	Belgium	39.9	8.1%	35%
10	Taiwan	39.5	22%	61%

Source: Akamai Report (2013-Aug)

Incentive for hackers to pick on Hong Kong

► Highest Attack Traffic

- In 2013 Q1, Hong Kong was at 10th position (1.6%)

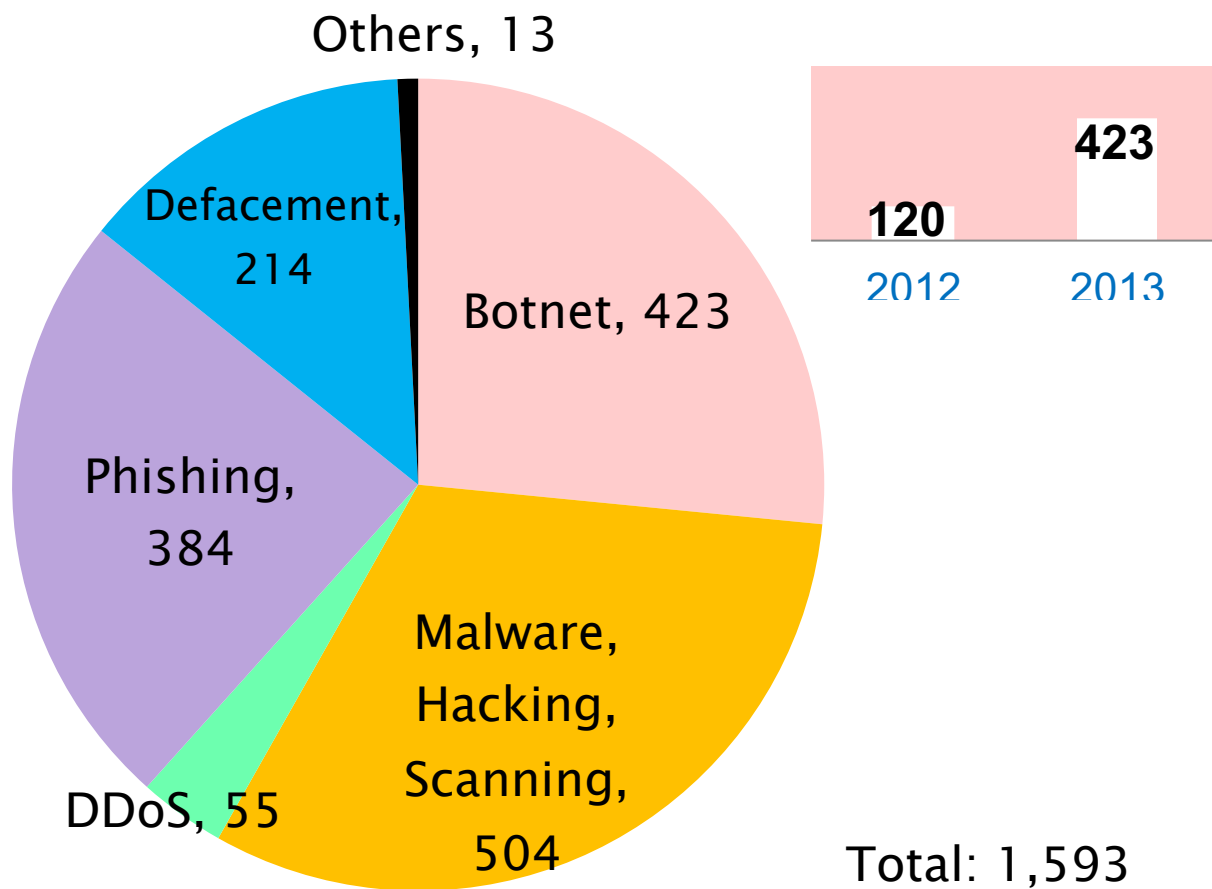
	Country	Q2 '13 % Traffic	Q1 '13 %
1	Indonesia	38%	21%
2	China	33%	34%
3	United States	6.9%	8.3%
4	Taiwan	2.5%	2.5%
5	Turkey	2.4%	4.5%
6	India	2.0%	2.6%
7	Russia	1.7%	2.7%
8	Brazil	1.4%	2.2%
9	Romania	1.0%	2.0%
10	South Korea	0.9%	1.4%
—	Other	11%	18%

Source: Akamai Report (2013–Aug)

Security Incident Reports Handled



Distribution of Security Incident Reports Handled



Invisible Bots 隱形殭屍

(Unreported compromised computers)

未被報告的被入侵電腦

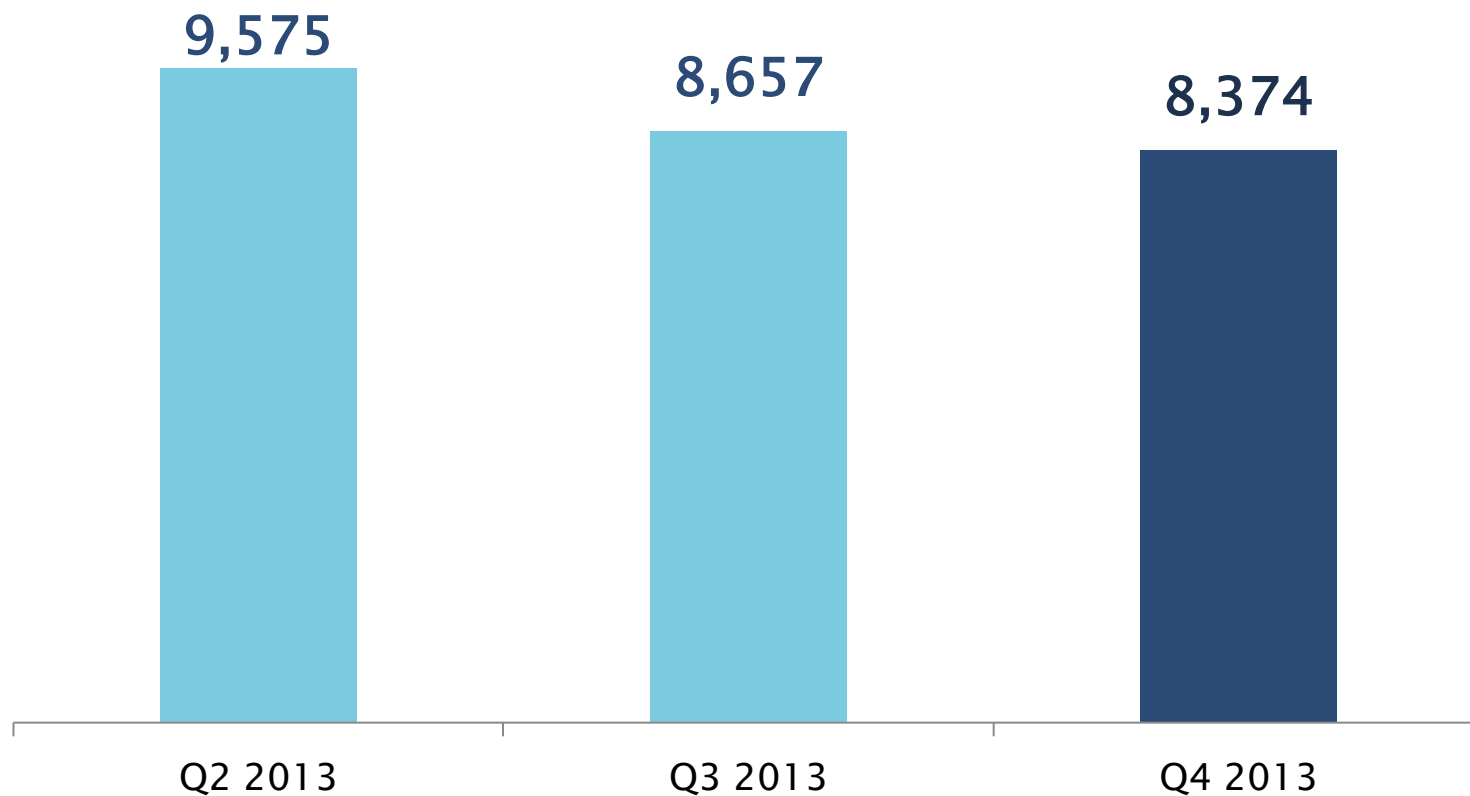


(image created by Tom-b: <http://commons.wikimedia.org/wiki/File:Botnet.svg>)

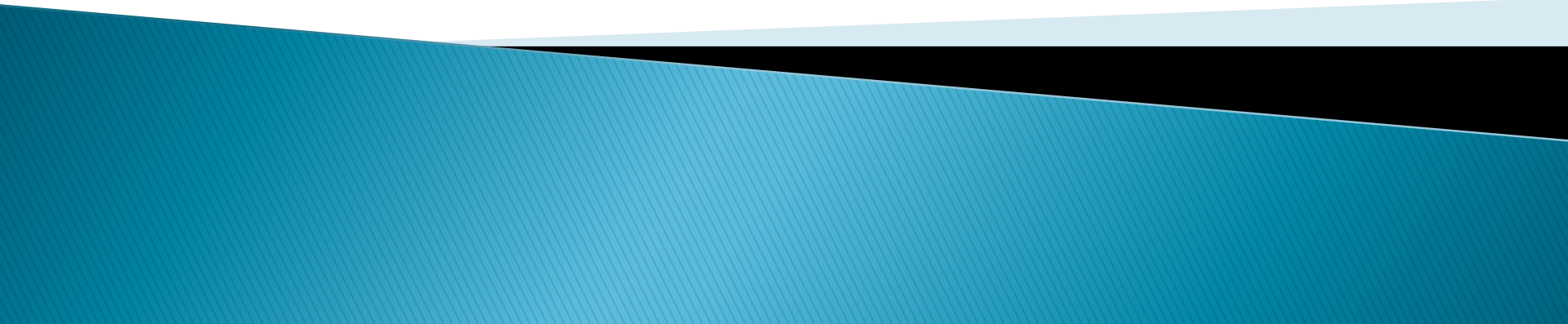
Invisible Bots 隱形殭屍

Source: data collected from global security researchers

** Events not reported to HKCERT



Hacktivist and Nation State attacks



Modern Hackers

Cyber
Criminal



Hacktivist



Nation
State



Image credits: Infographics of WatchGuard

Modern Hackers

Cyber
Criminal



- ▶ Motive: \$\$\$
 - Underground economy
 - Crime-as-a-Service
- ▶ Botnet infrastructure
- ▶ Advanced (banking) Trojan
- ▶ Moving to mobile and cloud

Image credits: Infographics of WatchGuard

Modern Hackers

Hacktivist



- ▶ Motive: Ideological
- ▶ High profile
- ▶ Crowdsourcing
- ▶ Data leakage → DDoS

Image credits: Infographics of WatchGuard

Modern Hackers

- ▶ Motive: Political/Military
- ▶ Target critical infrastructure
- ▶ Advanced malware / attacks
- ▶ Low profile
- ▶ Espionage

Nation
State



Image credits: Infographics of WatchGuard

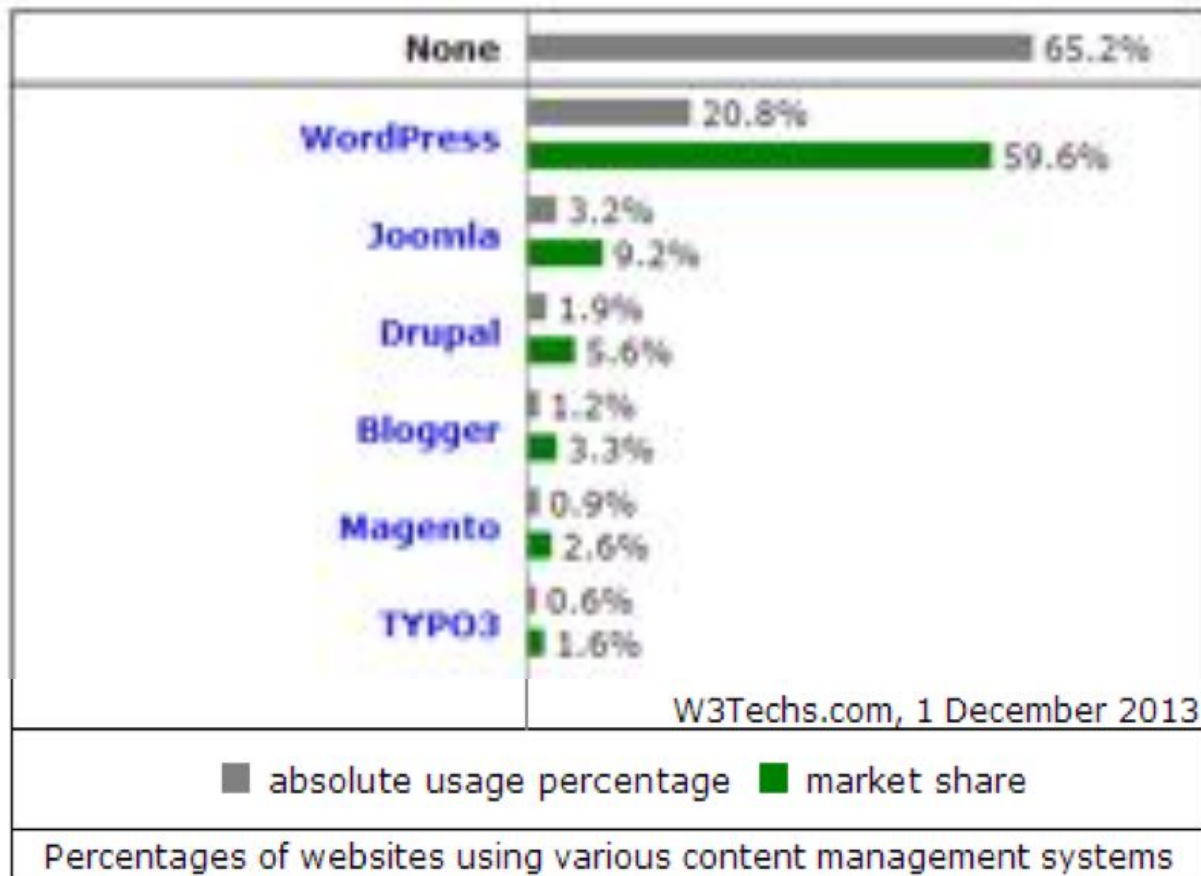
Largest DDoS attack on **US Banks**

since 2012-Sep

- ▶ "Operation Ababil" by Islam hacktivist group
- ▶ Attack sources: **hundreds of hijacked web servers**
 - Hacked web CMS servers with higher bandwidth (100Mbps)
- ▶ Attack traffic volume: 60–150 Gbps
 - As a reference: HKIX average throughput in 2012 = 150Gbps)



Market Share of CMS

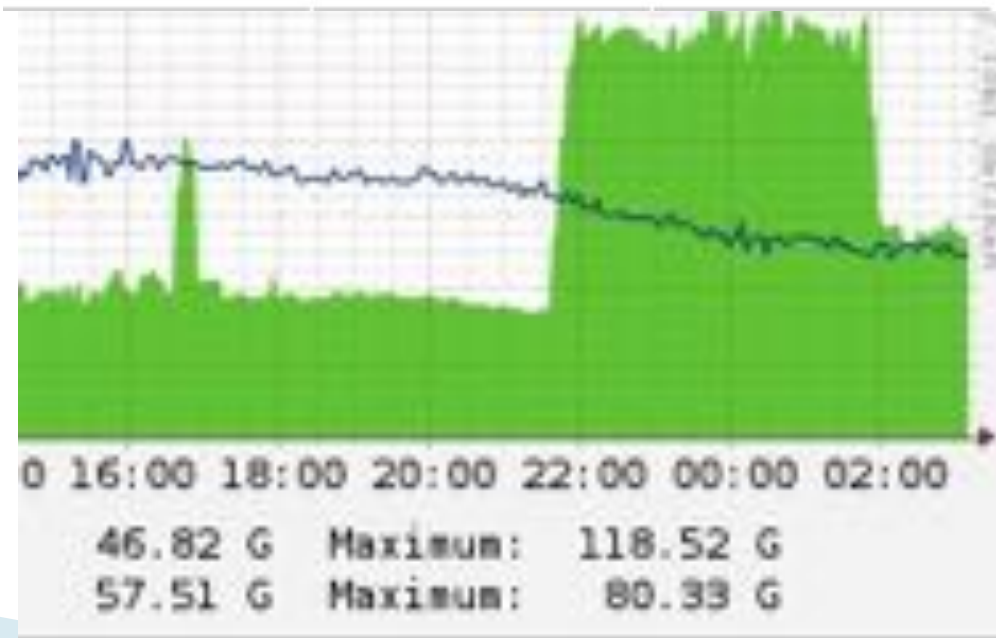


source: W3Techs

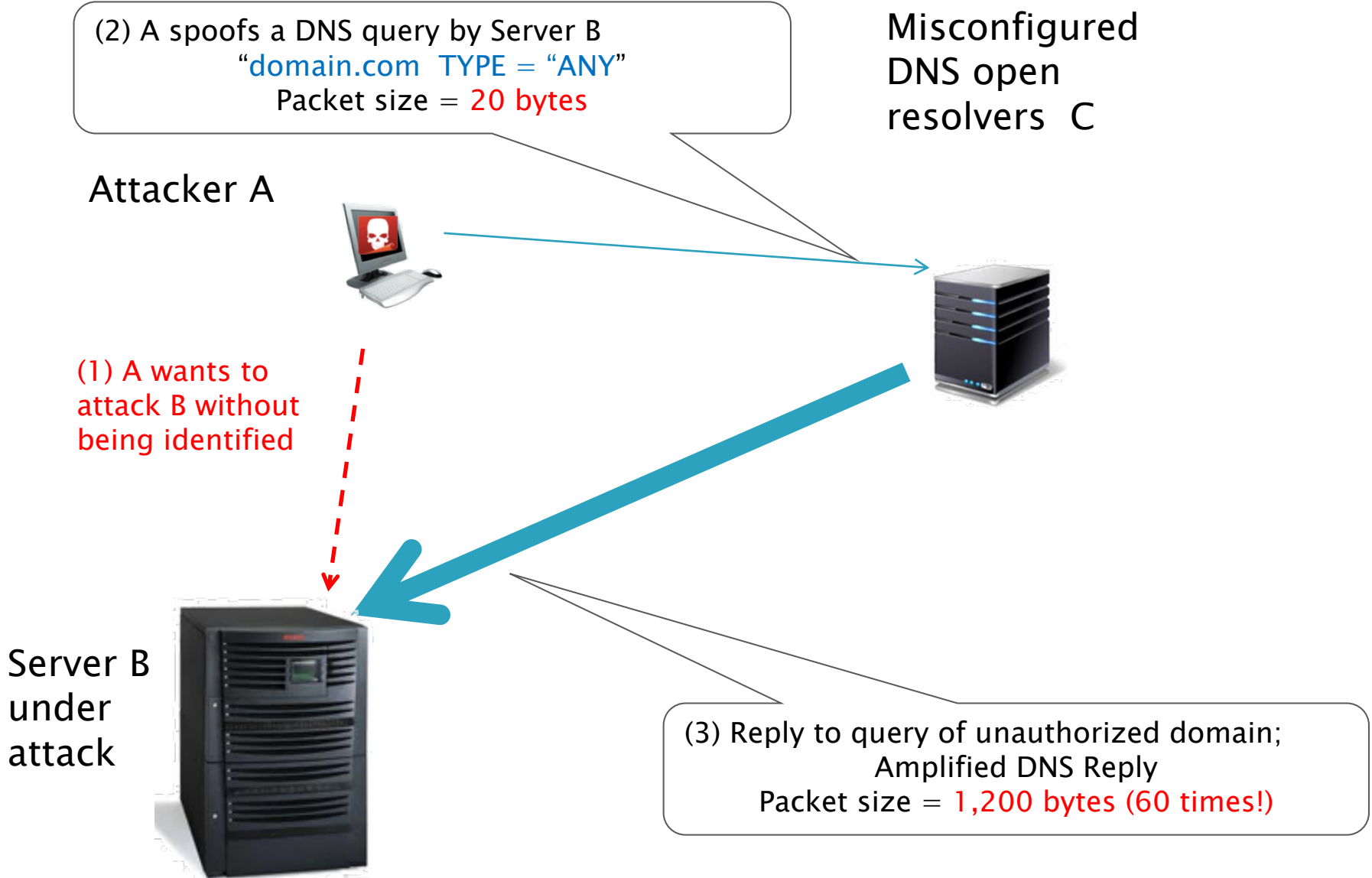
DDoS attack on Spamhaus

2013-Mar

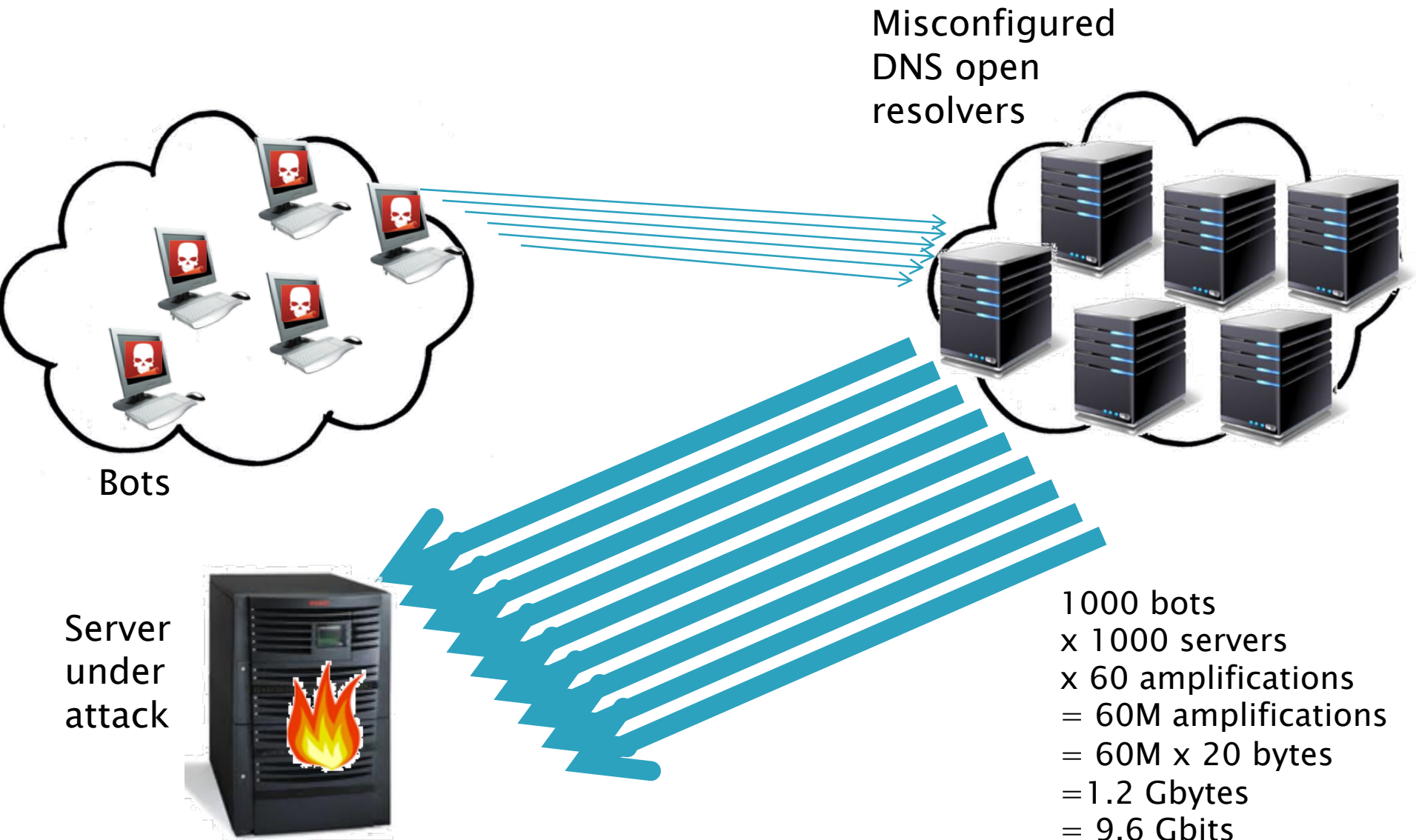
- ▶ Attack against Spamhaus which fights spam
- ▶ Reflective amplification attack from open DNS recursive resolvers
- ▶ Traffic: 30–120Gbps



Attack arsenal – Open DNS resolvers



Attack arsenal - Open DNS resolvers



Nominum Study: Home routers open to exploitation

- ▶ > 24M routers have **open DNS proxies** exposed ISPs to DrDoS
- ▶ > 70% of total DNS traffic on a provider's network was associated with DNS amplification (2014-Jan)
- ▶ 5.3M routers used in DrDoS (2014-Feb) clogged ISP networks
- ▶ Reference:
 - <http://nominum.com/news-post/24m-home-routers-expose-ddos/>

DDoS attack on CloudFlare

2014-Feb

- ▶ Traffic: > 350Gbps
- ▶ Attacker sources: **Misconfigured NTP servers**
- ▶ NTP (Network Time Protocol)
 - ntpd prior to version 4.2.7p26 that use the default unrestricted query configuration; other proprietary NTP implementations too

Nature of DrDoS

- ▶ Distributed **Reflective** DoS attack
- ▶ Spoofed IP addresses
- ▶ Bandwidth Amplification Factor
 - DNS (UDP/57) : 20X – 100X
 - NTP (UDP/123) : 20X – 200X
 - SNMP (UDP/161,162) : 3X – 10X
 - Chargen (UDP/19) : 10X – 20X

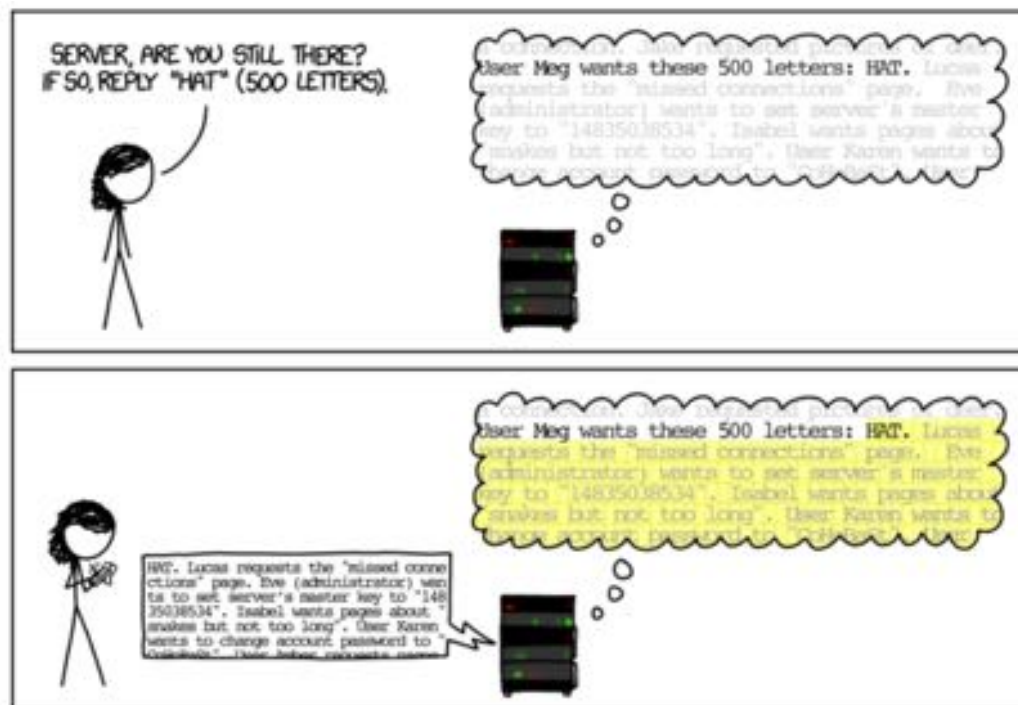
Routers, Set-top boxes, Webcams



- ▶ Internet exposed – weak password, default config. & vulnerability
- ▶ Lists of compromised CPE are traded in the underground
- ▶ Symantec: linux worm targeting hidden devices (2013–Nov)
 - Exploits a PHP vulnerability (CVE-2012-1823) to propagate itself
 - <http://www.symantec.com/connect/blogs/linux-worm-targeting-hidden-devices>

Vulnerable web servers

- ▶ OpenSSL Heartbleed vulnerability → leakage of private keys, credentials ...



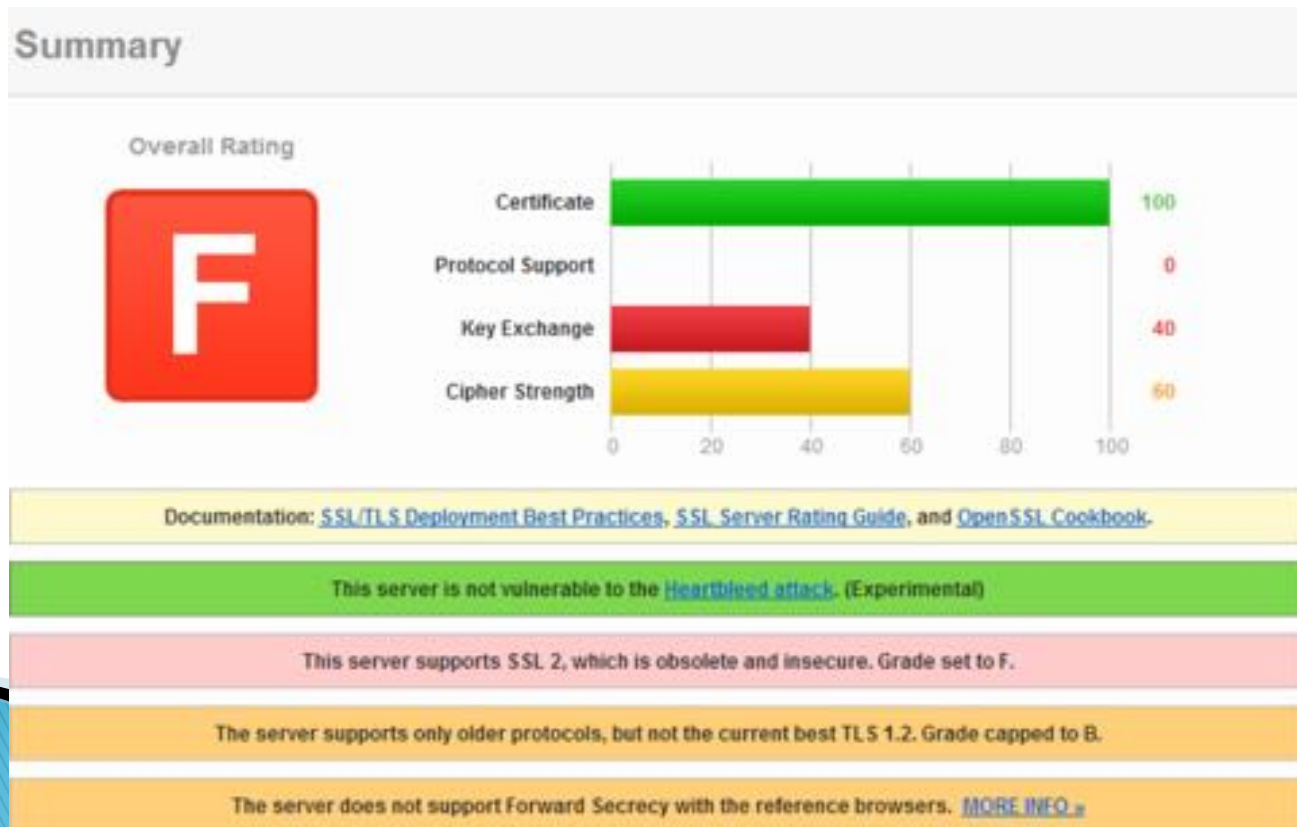
More info: https://www.hkcert.org/my_url/en/alert/14040802

Source: <http://www.xkcd.com/1354/>

Good Guy using Bad Crypto

▶ SSL Server Test

- <https://www.ssllabs.com/ssltest/analyze.html>
- Many organizations use old SSL protocol versions, weak cryptographic algorithms and 1024-bit SSL digital certificates



Challenges

- ▶ **Cross border / jurisdiction** attacks by organized groups
- ▶ **Critical infra, critical biz and mass media** are targets
- ▶ **DDoS: huge international traffic** → \$\$\$
- ▶ **Undetected malware** infiltrated to internal network
- ▶ **Hacked computers** (botnets) being used in attacks with their owners unaware → **ISP blacklisted**
- ▶ **Vulnerable / misconfigured systems** may become bots

Mitigation Measures

Adopt ISP Best Security Practices

- ▶ RFC3013 Recommended ISP Security (Nov 2000)
 - Computer Security Incident Response Team (CSIRT)
 - Notification of vulnerabilities & Reported Incidents
 - User Policy
 - Ban IP spoofing traffic via Ingress filtering from customers; Egress filtering to customers (RFC1918, RFC2827)
 - Ban open mail relay (RFC2505)
 - ...

Harden your network

- ▶ Physical security (site and racks)
- ▶ Close all unnecessary services
- ▶ Secure network management (syslog, snmp, tftp)
- ▶ Secure remote access (ssh, vpn)
- ▶ Strong authentication
- ▶ Prevent route poisoning
 - Accepts only customer prefixes which have been assigned or allocated to their downstream customers



Coordinated Botnet Takedown

Collaborate to take down Botnets

Citadel take down (2013–Jun – now)

C&C investigation and takedown

Reverse engineer botnet communication	Security Researchers
Apply court order	FBI & Microsoft
Seize C&C data and evidence in USA	FBI
C&C takedown outside USA	Microsoft, CERT, ISPs

Bot Cleanup

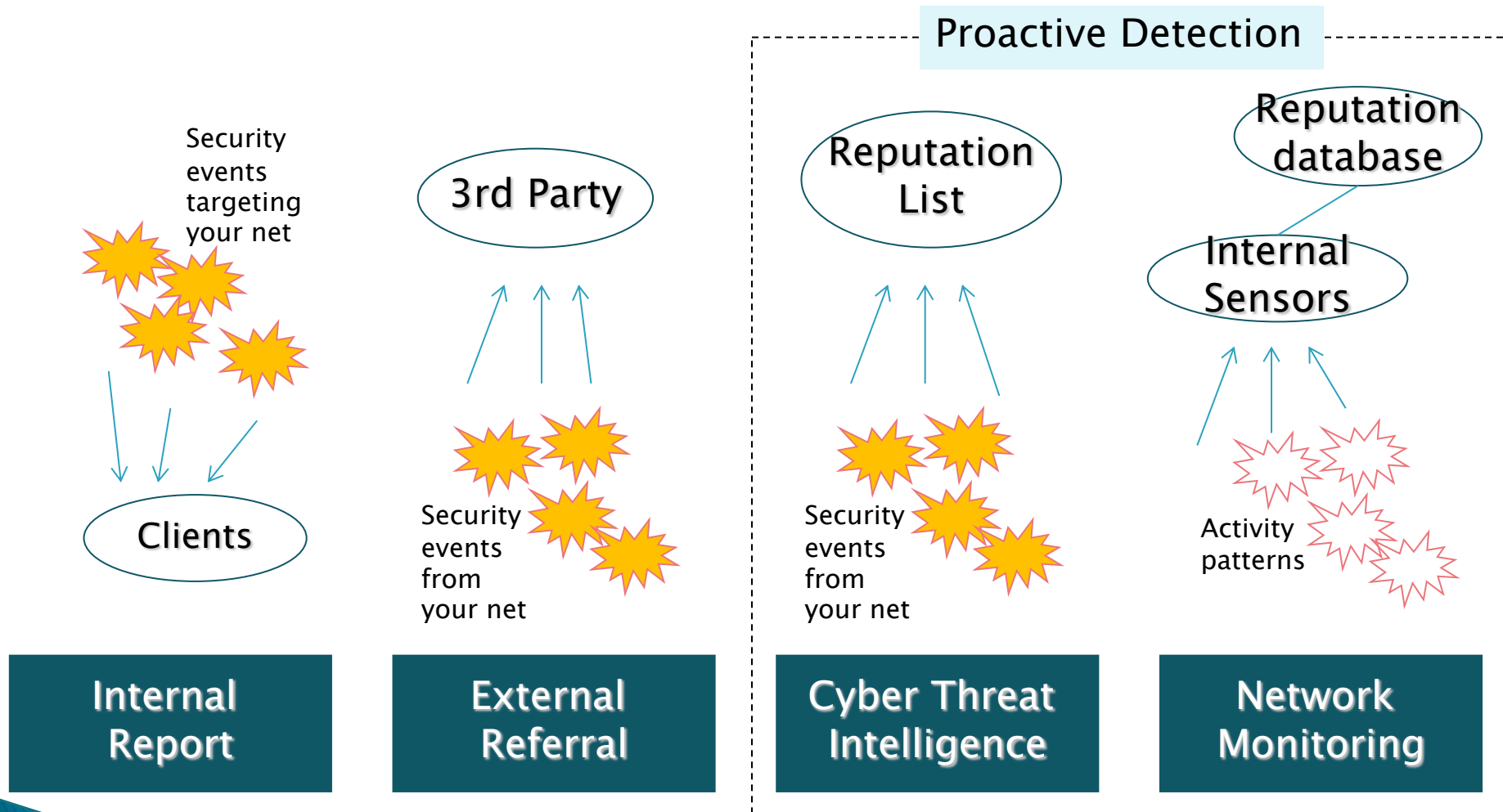
Sinkhole (fake C&C trap bot IP addresses)	Microsoft, DNR
Clean up local bots	Microsoft, CERT, ISPs
Provide tools to detect and clean up bot	Microsoft, security vendors

Clean up Botnets in Hong Kong

- ▶ Works with HKCERT in joint operation with security researchers, law enforcement to take down botnet C&C and bots
- ▶ Botnet Detection and Cleanup Guideline | HKCERT
 - <https://www.hkcert.org/botnet>

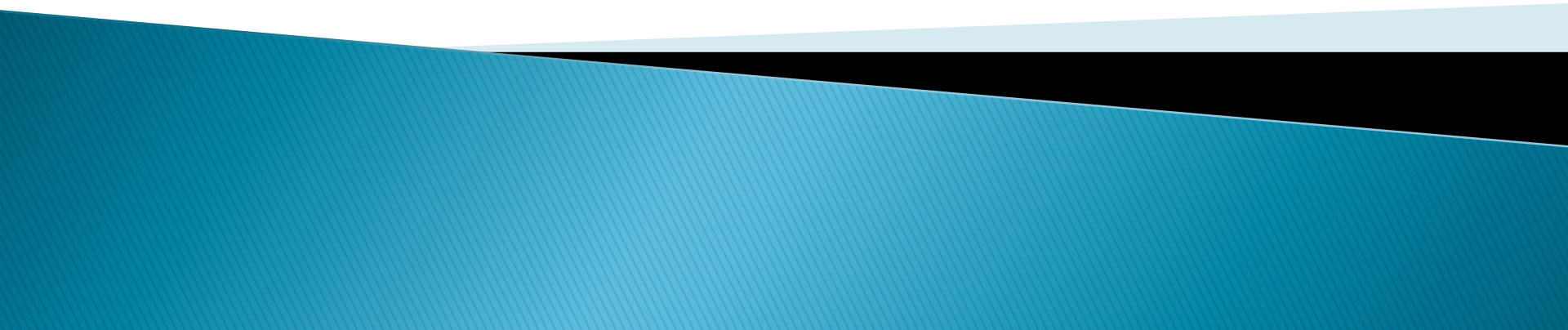
Botnet	1st Operation	Max no. of IP addr detected (approx) by operation
ZeroAccess	2013-12	3,700
Pushdo	2013-08	490
Citadel	2013-06	720
brobot	2012-11	25
Flashback	2012-04	320
DNSChanger	2012-03	3,500
Conficker	2009-02	4,000

Incident Responses

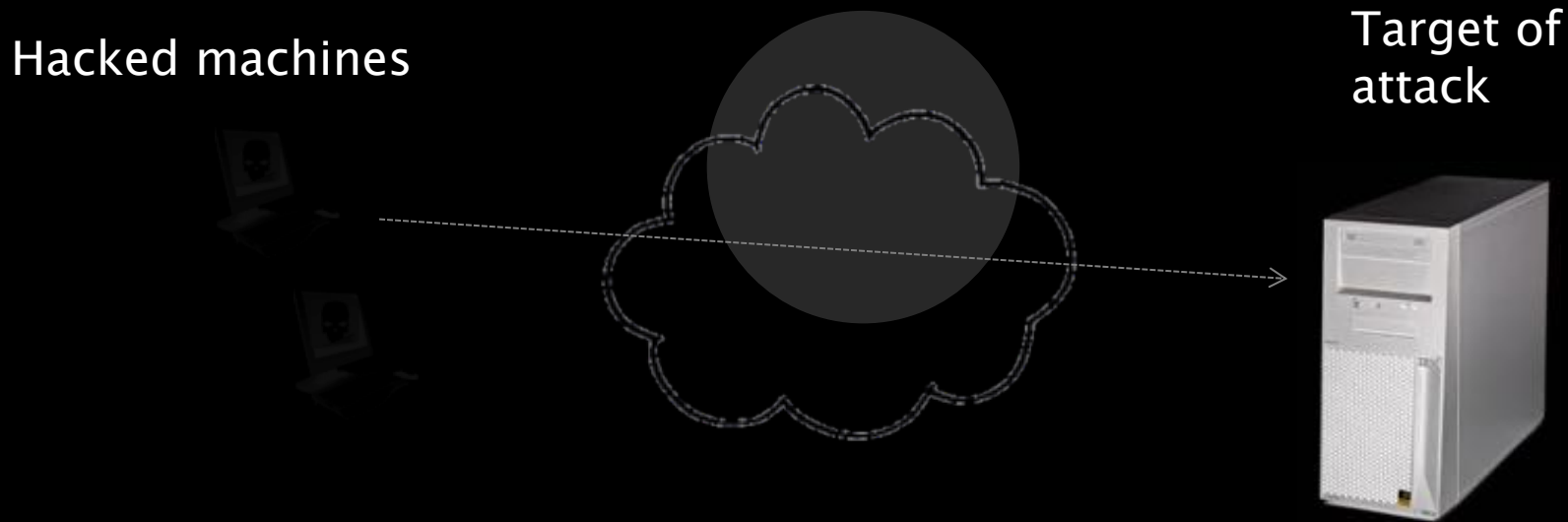


Proactive Detection of bots in your network

Leverage on Global Security Intelligence



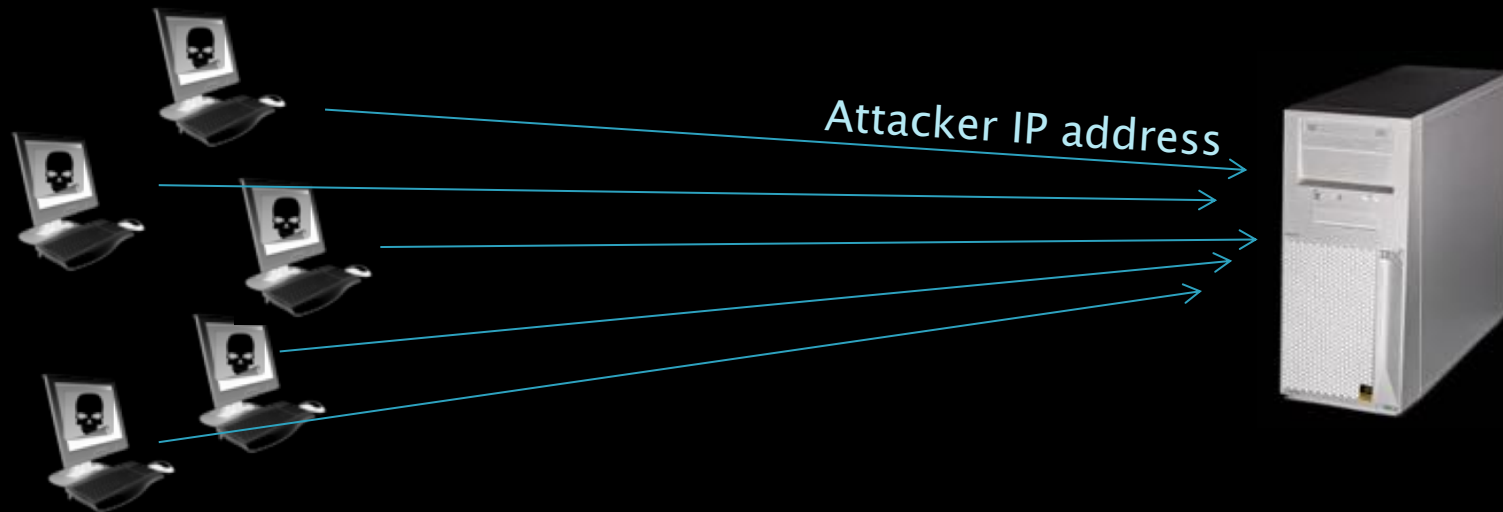
Global Intelligence, Local Footprints



- Attackers control hacked computers via stealthy malware.
- Owners of the hacked computers not aware of the compromise.
- But when a hacked computer launches an attack to a global target, it leaves footprints.

Global Intelligence, Local Footprints

Hacked machines



The footprints made by a local hacked machine

- IP addresses (logs of honeypot, firewall, ids/ips)
- Malware hosting URLs (reported)
- Phishing emails (reported)

Phishing intelligence



The screenshot shows the PhishTank website with a blue header and a dark blue navigation bar. The main content area displays a table of phishing intelligence data.

PhishTank® Out of the Net, into the Tank.		
Home Add A Phish Verify A Phish Phish Search Stats FAQ Developers Mailing Lists My Account		
ID	URL	Submitted by
1964345	http://https-www.paypal.com.update-cgi.bin-webscr....	PhishReporter
1964344	http://32575743.help-vision.org/parko/?logon=mypos...	mariocarelli
1964343	http://brinker-fetten.de/frgrg/ser/mac/a90.php	mariocarelli

<https://www.phishtank.com/>

- ▶ by country
- ▶ by asn
- ▶ by target

Zeus, SpyEye botnet tracker












Zeus Tracker :: Hong Kong (HK)

The list below shows all Zeus C&Cs and FakeURLs which are hosted in **Hong Kong (HK)**.

Set a filter for the list below: [online Zeus hosts](#) | [offline Zeus hosts](#) | [Zeus hosts unknown status](#) | [Zeus hosts with files online](#) | [all](#)

 [Subscribe this list via RSS feed](#)

Dateadded	CC	FU	Host	IP address	Level	Status	Files Online	SBL	Registrar	AS number
2013-06-13			www.wxwsteel.com	59.188.241.136	2	online	0	Not listed	BIZCN.COM, INC.	AS17444
2013-05-22			103.31.186.240	103.31.186.240	4	unknown	0	Not listed	n/a	AS39743

 							
Dateadded	SpyEye BinaryURL	Status	MD5 Hash	Filesize	Virustotal	Anubis	File download
2011-10-12	gogofuck.eu/bh/w.php?f=16&e=6	offline	665c5383160fd98f63fe7e4edbe67dcc	431'104	 17/43 (39.50%)	 report	 download
2011-10-11	wavone.us/w.php?f=16&e=6	offline	1b18b0f15960b38023d8c8a7cfd72e5d	130'960	 13/43 (30.20%)	 report	 download
2011-09-15	31.31.203.123/e-cards.exe	offline	22b6a5069366f9c0fd8be82aaf653b27	207'360	 35/44 (79.50%)	 report	 download

<http://zeustracker.abuse.ch>

<http://spyeyetracker.abuse.ch>

- ▶ by country

Malware intelligence

CLEAN MX realtime database 

public access query for virus URL 

Totally watched: 1207722 As of 2013-08-04 18:05:19 CEST

[Subscribe to the VirusWatch Mailing list, updated hourly](#)

This database consists of Virus URI, collected and verified since Feb 2006

Line	id	Date	Closed	hours	contributor	virusname	URL	ip state	response	ip initia
1	11359843	2013-05-23 13:00:54	OVERDUE!	1757.6	sub16		http://popskin.hk/load.exe			undef
2	449433	2010-03-02 09:16:00	2010-03-02 11:07:16	1.9	sub4	mdl_zeus/wsrpocm v2 drop zone	http://popskin.hk/index1.php	vp	dead	91.
3	446831	2010-02-28 16:26:00	2010-02-28 18:18:16	1.9	sub4	mdl_zeus/wsrpocm v2 config file	http://popskin.hk/ribkn.tar	vp	dead	89.

<http://support.clean-mx.de/clean-mx/viruses>

M A L W A R E D O M A I N L I S T						
Homepage Forums Recent Updates RSS update feed Contact us						
Date (UTC)	Domain	IP	Reverse Lookup	Description	Registrant	ASN
↑ ↓	↑ ↓	↑ ↓	↑ ↓	↑ ↓	↑ ↓	↑ ↓
2013/08/04_05:14	zxkewwcow.biz	199.79.63.83	md-47.webhostbox.net	Trojan	contact@privacyprote ct.org	40034
2013/08/04_05:01	safwdxc23e.biz	199.79.63.83	md-47.webhostbox.net	Trojan	contact@privacyprote ct.org	40034
2013/08/04_05:01	qwlpxcq2f.biz	199.79.63.83	md-47.webhostbox.net	Trojan	contact@privacyprote ct.org	40034

<http://www.malwaredomainlist.com>

Defacement intelligence



The screenshot shows the zone-h website interface. At the top is a red header with the 'zone-h' logo and the tagline 'unrestricted information'. Below the header is a navigation bar with links: Home, News, Events, Archive, Archive (with a star icon), Onhold, Notify, Stats, Register, and Login. The main content area features a search filter section with input fields for 'NOTIFIER' and 'DOMAIN' (set to 'hk'), checkboxes for 'Special defacements only', 'Fulltext/Wildcard', and 'Onhold (unpublished) only', and a 'Date' dropdown set to 'ALL' with an 'Apply filter' button. Below the filters, it states 'Total notifications: 9,143 of which 2,345 single ip and 6,398 mass defacements'. A legend explains the symbols: 'H' for Homepage defacement, 'M' for Mass defacement, 'E' for Redefacement, 'L' for IP address location, and a star for Special defacement. A table displays recent defacement records with columns for Date, Notifier, H, M, E, L, Domain, and OS.

Date	Notifier	H	M	E	L	Domain	OS
2013/08/04	dh-Class					www.eas.cuhk.edu.hk/cuhk/news/...	Win 2008
2013/08/02	Mr.Expired008	H				www.inksupply.com.hk	Linux
2013/08/02	hasnain hasar		M			asadigital.com.hk/v00t.html	Linux
2013/08/02	EC GREY HAT HACKERS		M			killer.hk/as.htm	Windows

<http://www.zone-h.org>

- ▶ by country
- ▶ by domain

TorExit List

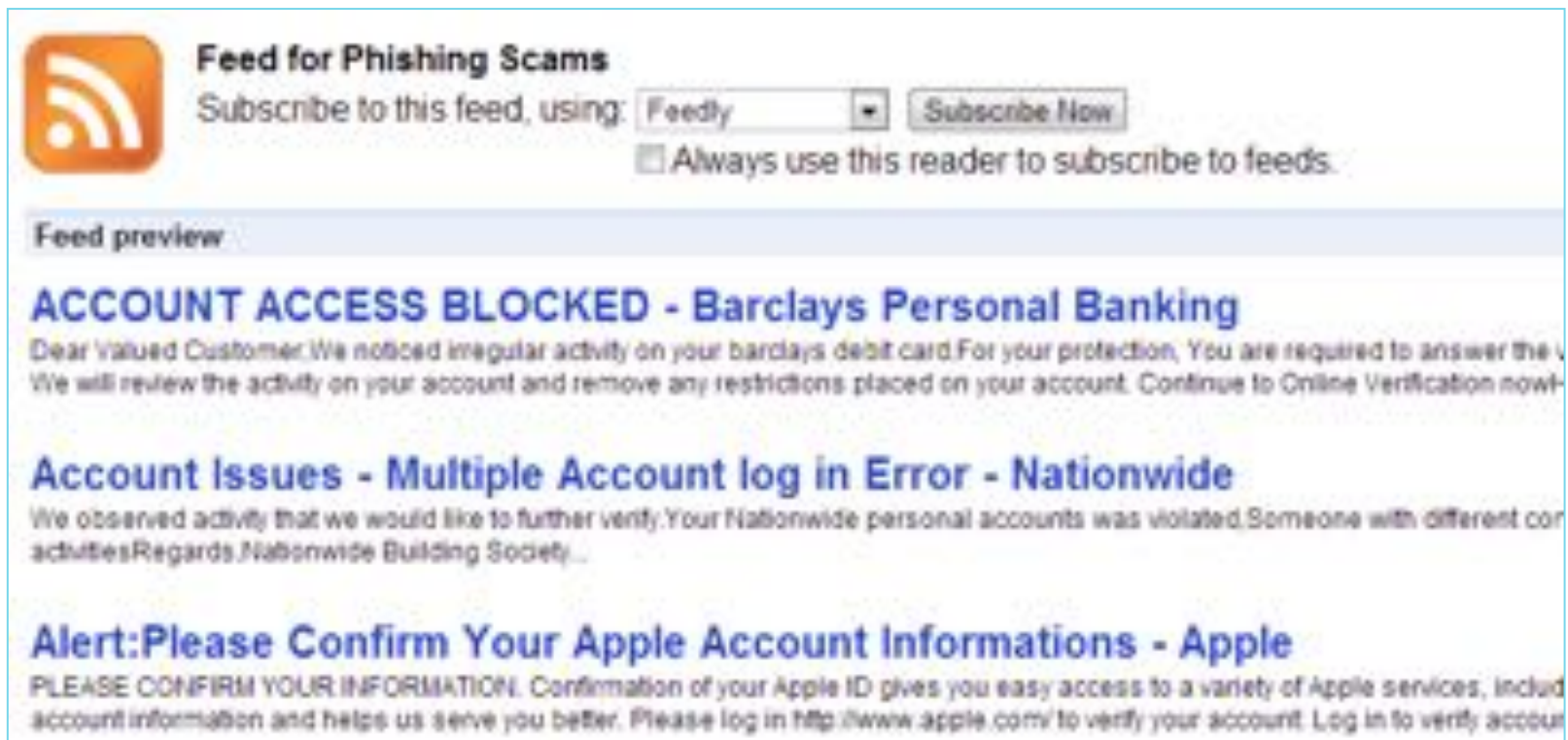
- ▶ Traffic originated from Tor Exit Node is suspicious

 HKRealDemocracy		100	0 d	n11649205030.netvigator.com [116.49.205.30]
 HKRelay		6	8 d	223.16.44.193 [223.16.44.193]
 HKT01		9	75 d	117.18.118.136 [117.18.118.136]
 HKT02		113	75 d	117.18.118.137 [117.18.118.137]
 HongTor		6	0 d	119247089219.ctinets.com [119.247.89.219]

- ▶ <http://torstatus.blutmagie.de>
 - (note this site is blocked by some web security tools)

Automated collection of intelligence

- ▶ Some provide API or structured format, e.g. XML



Feed for Phishing Scams
Subscribe to this feed, using:
☐ Always use this reader to subscribe to feeds.

Feed preview

ACCOUNT ACCESS BLOCKED - Barclays Personal Banking
Dear Valued Customer, We noticed irregular activity on your Barclays debit card. For your protection, You are required to answer the v...
We will review the activity on your account and remove any restrictions placed on your account. Continue to Online Verification now...

Account Issues - Multiple Account log in Error - Nationwide
We observed activity that we would like to further verify. Your Nationwide personal accounts was violated. Someone with different con...
activities. Regards, Nationwide Building Society...

Alert: Please Confirm Your Apple Account Informations - Apple
PLEASE CONFIRM YOUR INFORMATION. Confirmation of your Apple ID gives you easy access to a variety of Apple services, includ...
account information and helps us serve you better. Please log in <http://www.apple.com/> to verify your account. Log in to verify account...

Google Safe Browsing Alerts

for network admin

► <http://www.google.com/safebrowsing/alerts/>

安全瀏覽

AS13354 (ASN-EBLGLOBAL) 的診斷網頁

公告發佈者：Google

Google 造訪此聯播網上的網站時有什麼發現？

我們在過去 90 天內測試了此聯播網上的 6593 個網站，當中有 sirkenayo.net/、ewallpops.com/、sanghparivar.org/ 等 70 個網站的內容會擅自將惡意軟體下載及安裝至使用者的電腦。

Google 上次針對此聯播網上的網站進行測試的日期是 2014-04-13，而上次發現可疑內容的日期則是 2014-04-13。

此聯播網中是否有任何網站成為進一步散佈惡意軟體的媒介？

在過去 90 天內，我們發現惡意軟體透過此聯播網上的 cornerstoneethics.org/、sirkenayo.net/、club-vw.cl/ 等 12 個網站，向其他 141 個網站進行散佈，受害網站包括：dhr.it/、google.com/、sexxdoll.com/。

此聯播網中是否有任何網站曾散佈惡意軟體？

是，此聯播網中有 15 個網站曾在過去 90 天內散佈惡意軟體，這些網站包括：tbclassifieds.com/、topfreeproxy.com/、kicksdrinks.com/。受害網站有 199 個，其中包括：proxysite.org/、aplusproxy.com/、dom-arquitectura.com/。

後續步驟：

- [返回上一頁。](#)

上次更新時間：7 小時前

Google Safe Browsing Alerts

for network admin

- ▶ <http://www.google.com/safebrowsing/alerts/>

Google Safe Browsing Alerts for Network Administrators

[Home](#)
[Messages](#)


Safe Browsing Alerts for Network Administrators allows autonomous system (AS) administrators to register to receive Google Safe Browsing notifications. The goal is to provide network administrators with information of malicious content that is being hosted on their networks.

[Malware Forum](#)

AS Registration

In order to register to receive notifications for an ASN, you need to be verified by an AS contact. After completing the registration form, we will send a verification email to the contact you selected. Once the contact completes the verification step by clicking on the link provided in the email, you will see the ASN listed as verified on the welcome page.

Number	13354
Name	ASN-EBLGLOBAL
Contact	<input type="text" value="ipeng@coreexchange.com"/>
Source	ARIN
Notification Emails	<input type="text" value="ipeng@coreexchange.com, admin@coreexchange.com"/> (comma separated list)



HKCERT IFAS Project

– an automated global intelligence collection system

Visualize **Internet Security Status**

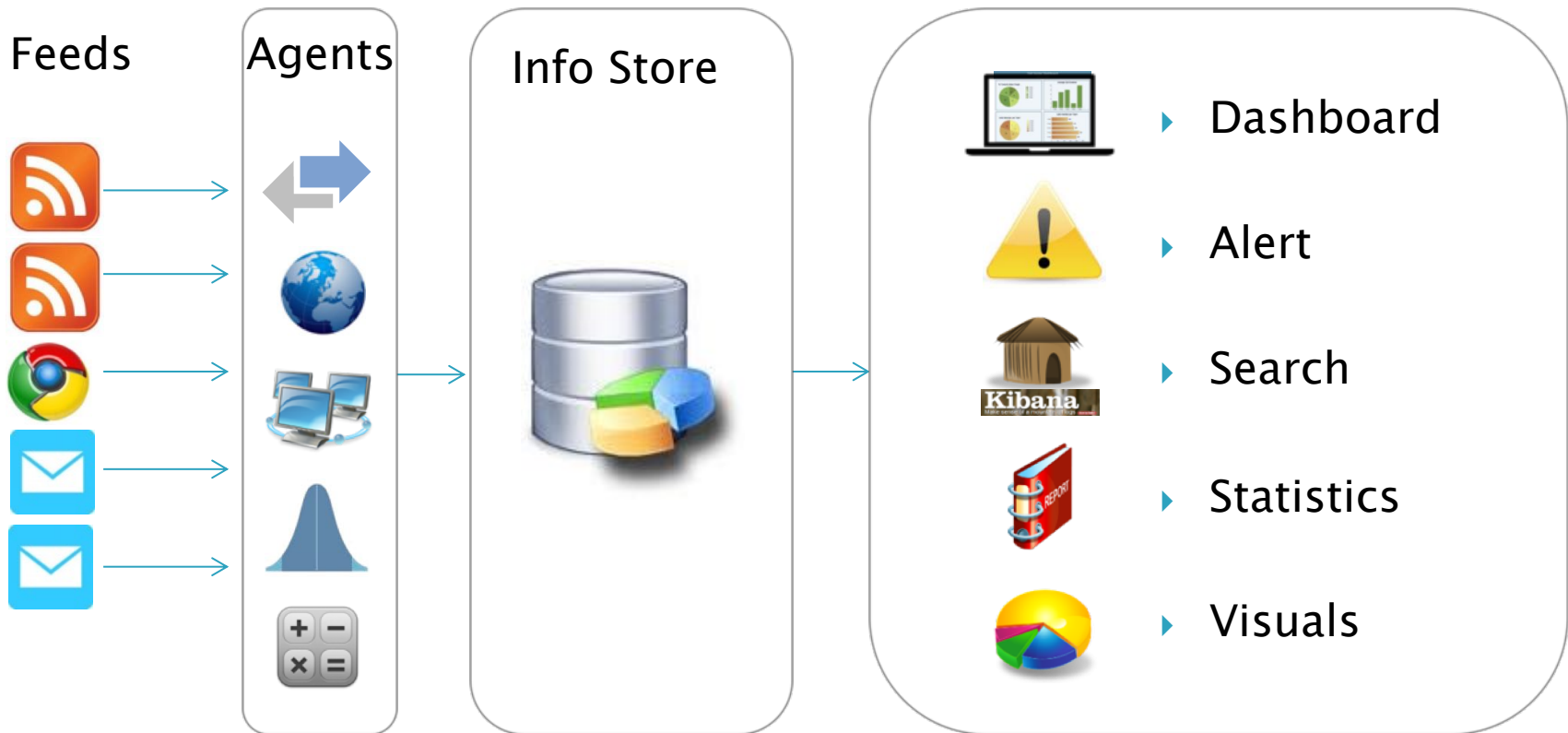
Situational Awareness

Track **Trends**

Generate **Alerts**

IFAS

– an automated global intelligence collection system



– feed collection, geolocation tag, ASN tag, normalization and calculation

IFAS Information Sources

Current plug-ins for ...

- ◉ Abuse.ch
- ◉ Arbor SRF
- ◉ CleanMX
- ◉ Malc0de
- ◉ MaliciousDomainList
- ◉ Millersmiles
- ◉ Phishtank
- ◉ Shadowserver
- ◉ Zone-H

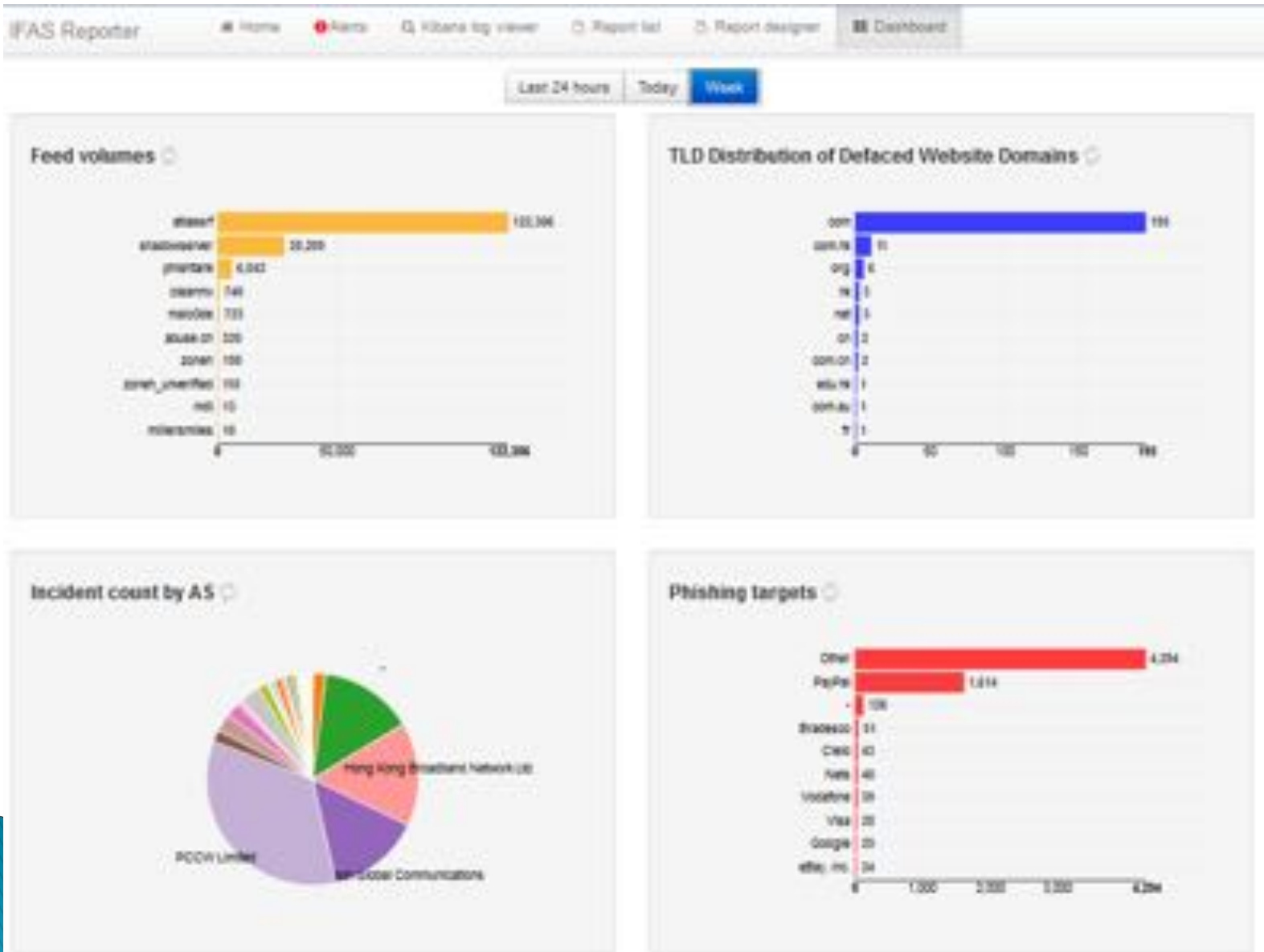
Plug-ins to be developed

- ◉ Google Safe Browsing
 - ◉ Microsoft
 - ◉ Scumware
- ... more

Dashboard

Real-time situational awareness
for CERT management

Real-time situational awareness for CERT management



Give a sense of Today's Events

IFAS Reporter

Home

Alerts

Kibana log viewer

Report list

Report designer

Dashboard



Last 7d



Search

Search

Reset

157,916 hits



ns in export stream



Older

0 TO 50

Time @message

08/05 11:02:48 %[event_type]: %[host]. %[cc]

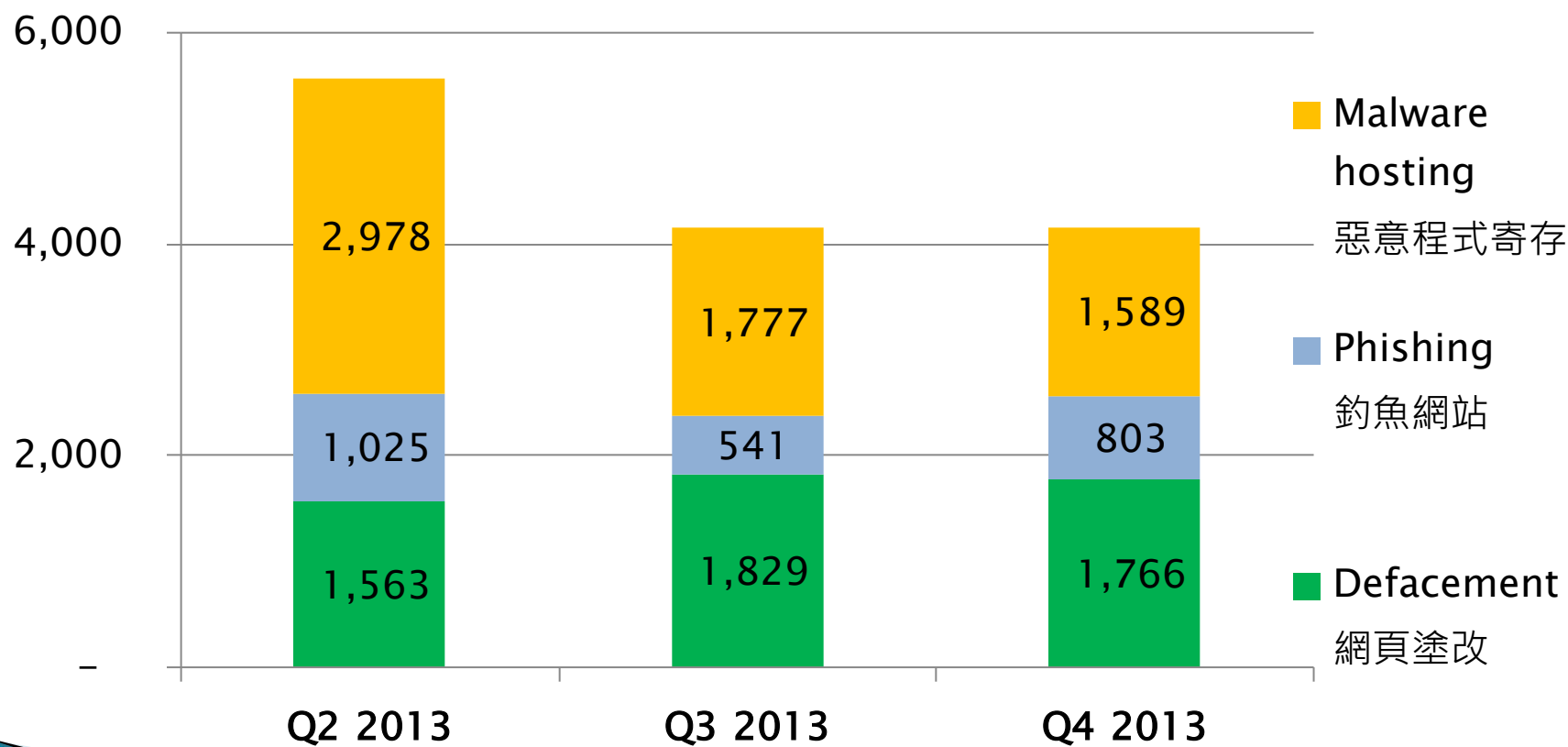
08/05 11:02:48 phishing: %[url]. %[cc]

08/05 09:59:01 phishing: http://beyazdanişmanlik.org/temQ/1e0370fc990575c97447a0189737488c20337353b7962f533d78c762373b3318/index/138ea7b50dc03dd9a78569659dd9421f

08/05 09:59:01 phishing: http://el-lodefimg.com
/vuxtruoant0ummip_ut3urtfurnn0v1v%TE50mzx_t00xpnyprvwm_t0vor_u0qtdyumosnoplmtocx_st7ur_mro_ufdw3yutyrutxveumpolte3ult0x0ut0out7eum_thy1
US

Compromised Servers in HK

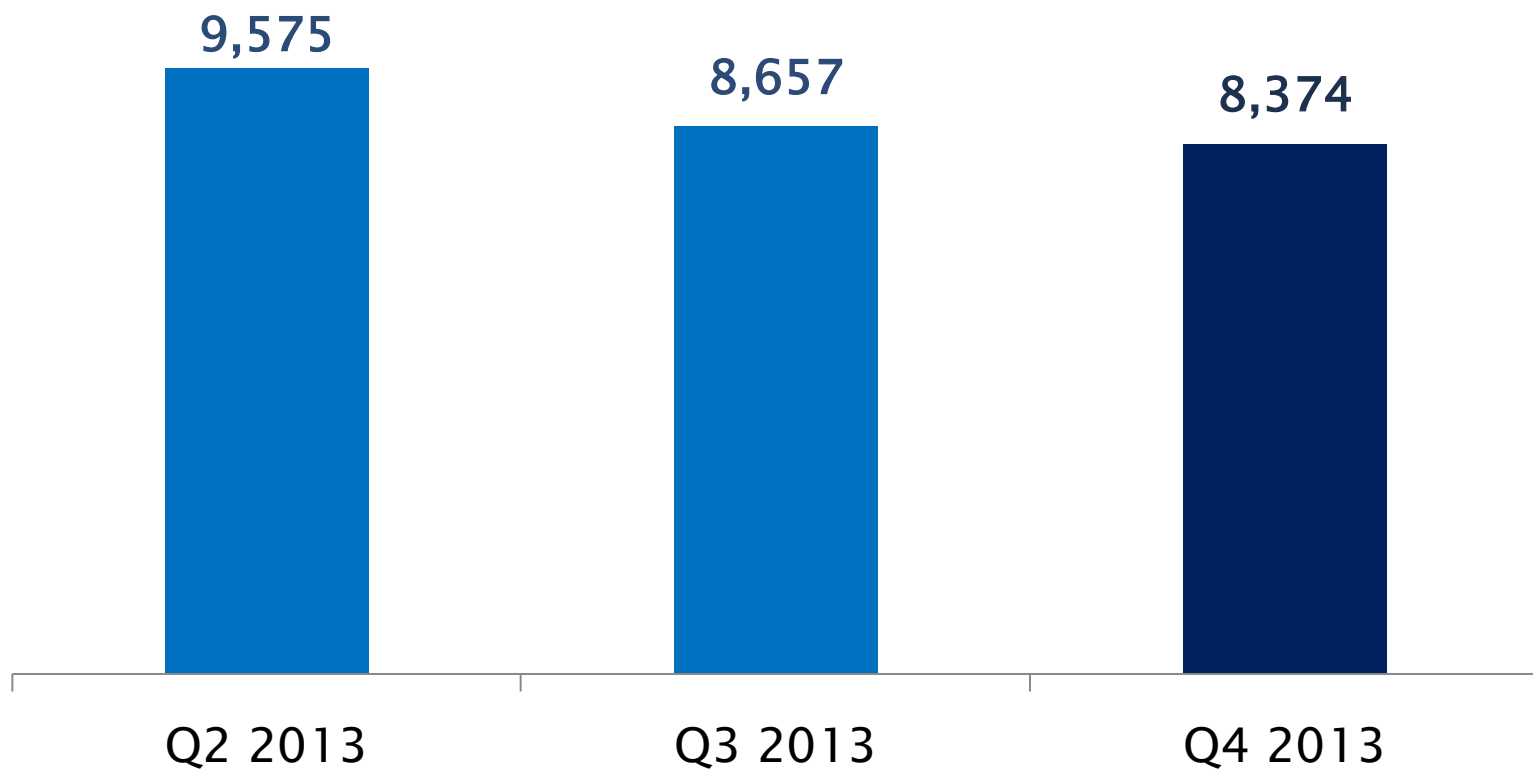
> 4,000 compromised servers



Source: HK Security Watch Report 2013 Q4

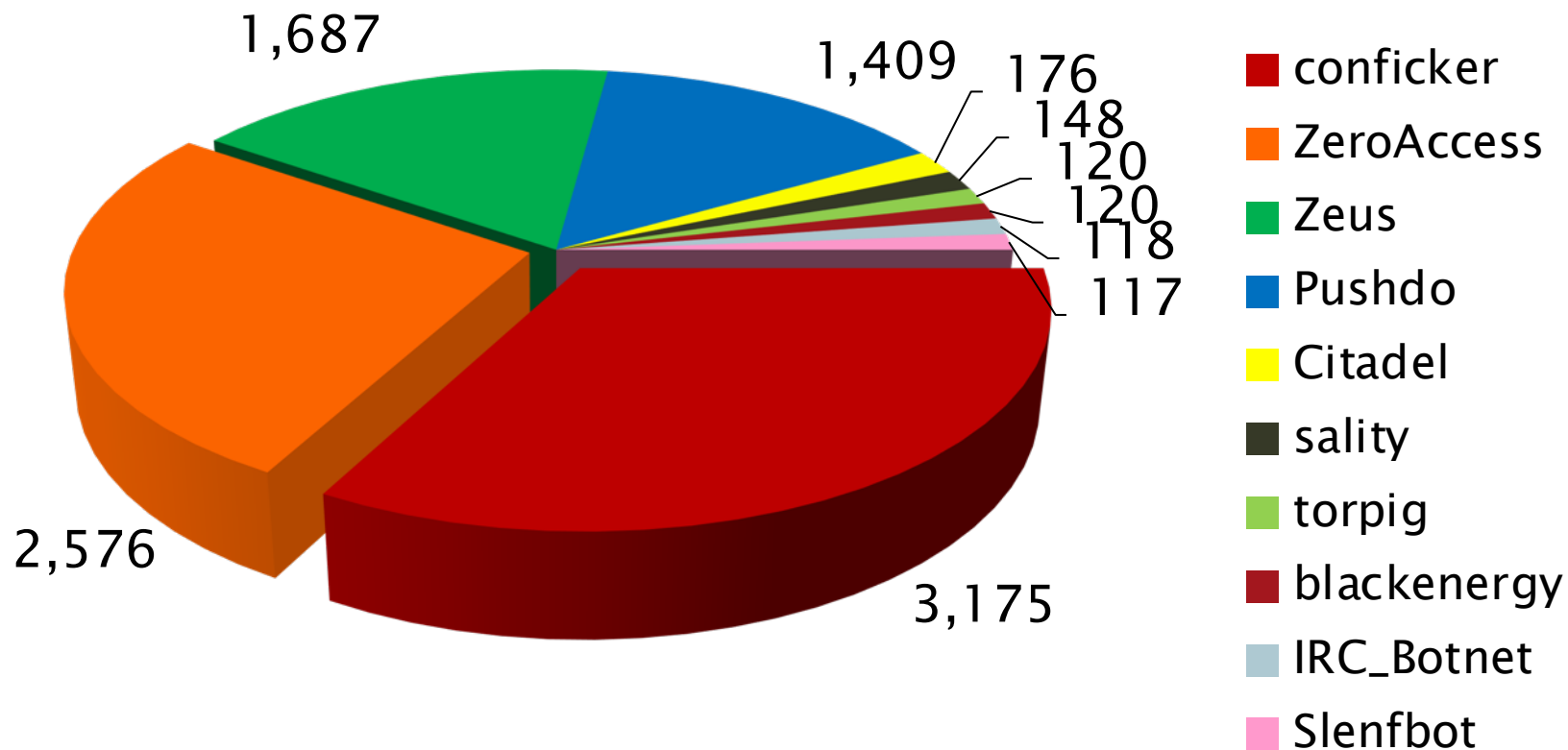
Invisible Bots 隱形殭屍

> 8,000 compromised PCs



Source: HK Security Watch Report 2013 Q4

Major Botnet Families in Hong Kong



Source: HK Security Watch Report 2013 Q4

Analysis of Trend with Events

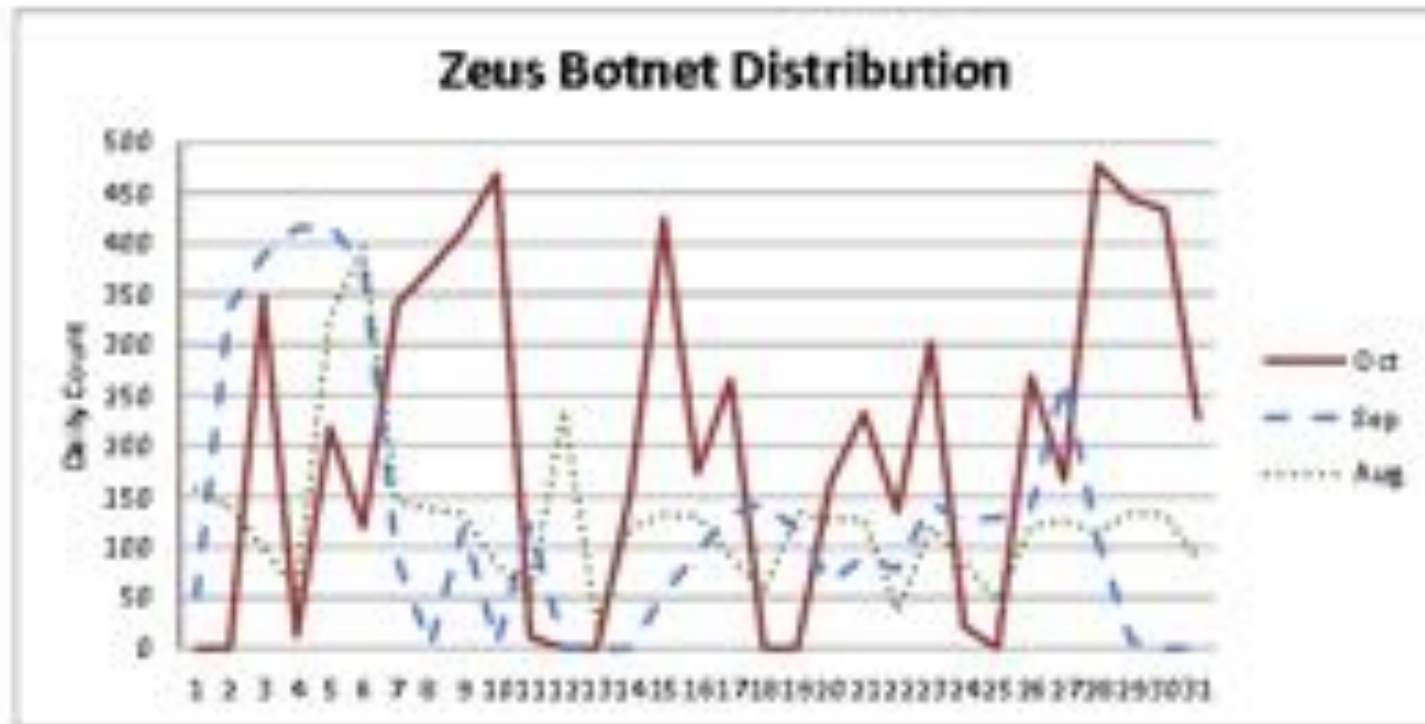


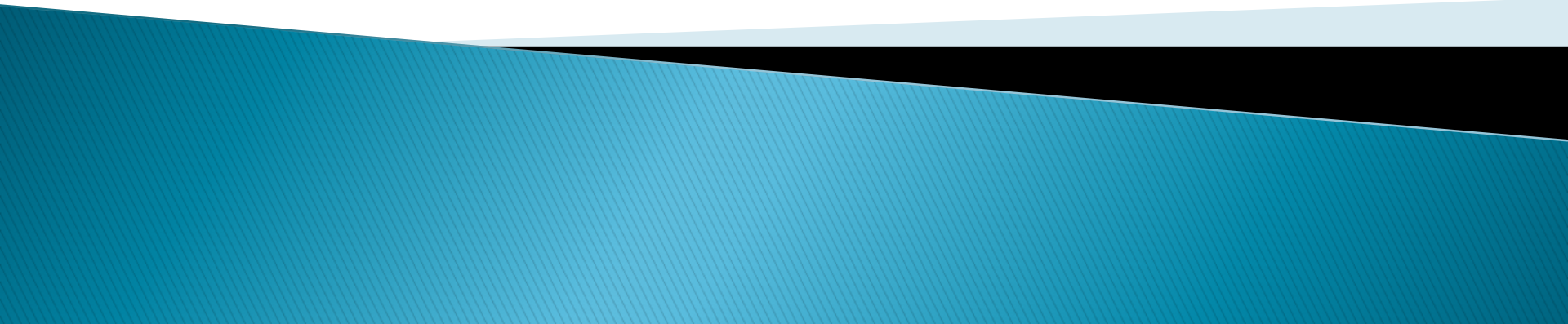
Figure 4- Zeus Botnet Distribution

- ▶ Correlate Cryptolocker 2013-Oct with Zeus

Network Monitoring

- ▶ Closer watch on the critical network segments
- ▶ Detect anomaly outgoing traffic
 - Passive DNS
 - Netflow
- ▶ Deceptive detection
 - Honeypot – Dionaea
 - Honeydoc

Proactive Network Hygiene



Network Hygiene

Detect / Clean up weak infrastructure

- ▶ CERTs work with ISPs and service providers to address the network hygiene issue.



Assess – you can do this for your network and your client

- Scan for vulnerable web servers
 - <https://www.scantosecure.com/>
- Scan for open DNS recursive resolvers
 - <http://openresolverproject.org/>
- Scan for open NTP servers
 - <http://openntpproject.org/>
- Scan for vulnerable mail servers
 - <http://mxtoolbox.com/diagnostic.aspx>

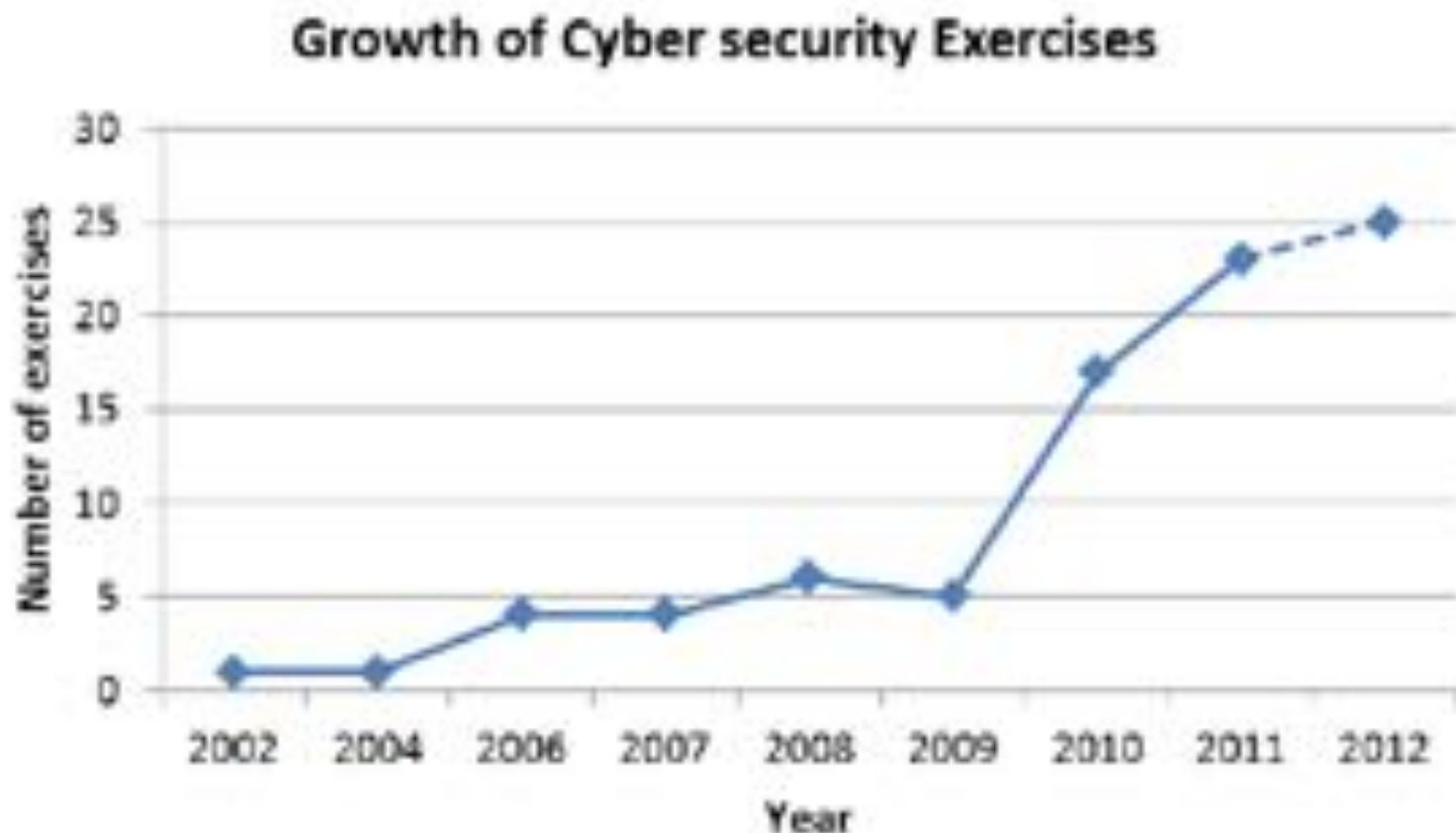
Clean up vulnerable CPE

- ▶ Find out these devices with CERTs
- ▶ Give advice to users:
 - Firewall protect the devices unless necessary to open to Internet
 - Patch the devices. Change default settings



**Preparation for
Large Scale Attacks**

ENISA – Survey of Cyber Drill Exercise 2012



ENISA – European Network and Information Security Agency

Adoption of Cyber Security Drill

▶ Hong Kong

- 2009 HKCERT

▶ Asia Pacific

- 2005 APCERT
- 2006 ASEAN
- 2006 Japan
- 2007 Taiwan
- 2008 Malaysia

...

▶ US

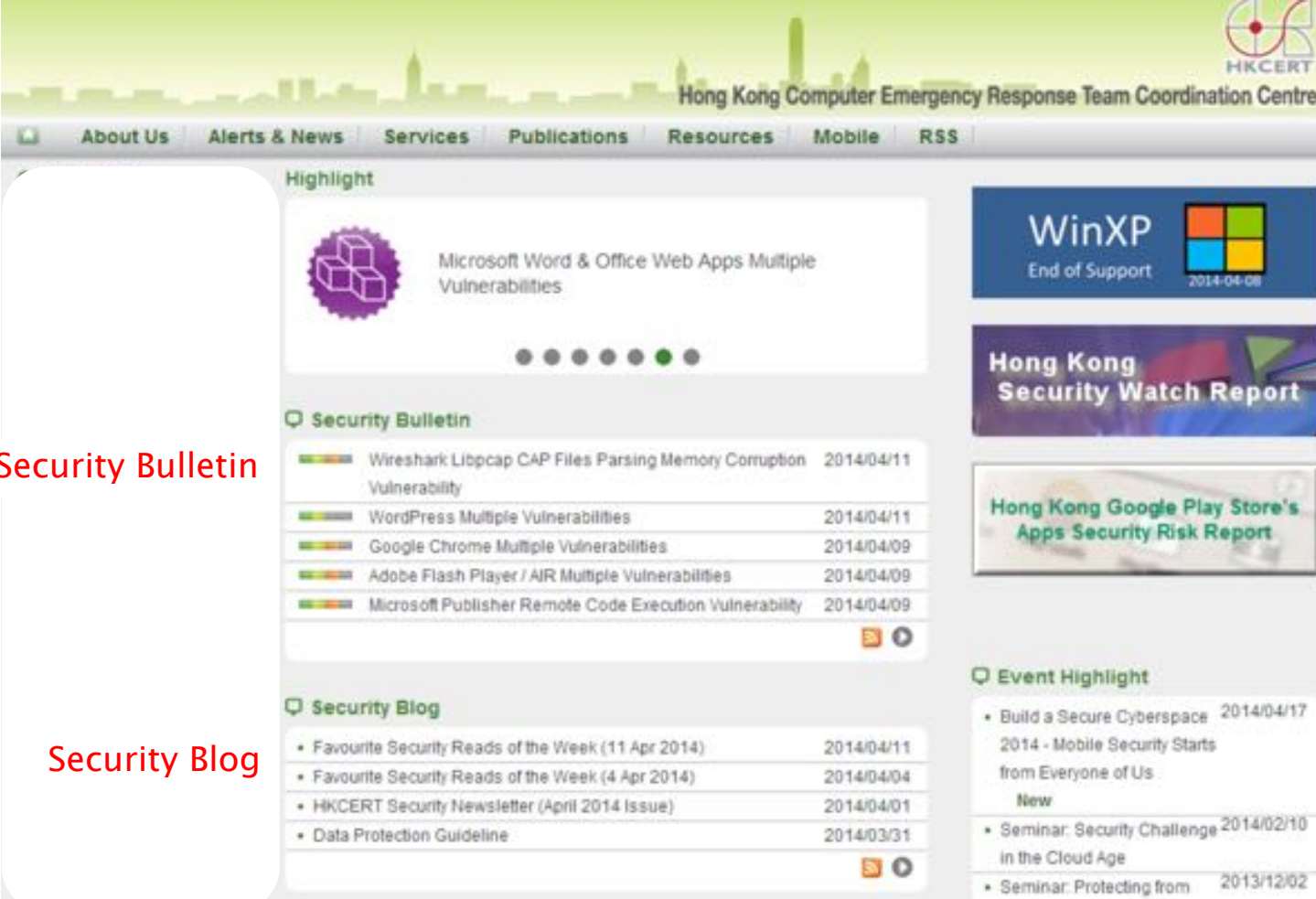
- 2006 DHS (CyberStorm bi-annually)
- 2010 FS-ISAC

▶ Europe

- 2007 Netherlands
- 2008 Finland
- 2009 Norway, UK
- 2010 Bulgaria, Estonia, France, Greece, Ireland, Spain, ENISA
- 2011 Denmark, Germany, Italy, Latvia, Slovakia
- 2012 Austria, Iceland, Poland , Switzerland

**HKCERT services
available to you**

Information @ HKCERT website



The screenshot shows the HKCERT website with a green header and a navigation bar. The main content area is divided into several sections:

- Highlight:** A section featuring a purple cube icon and the text "Microsoft Word & Office Web Apps Multiple Vulnerabilities".
- Security Bulletin:** A section with a green icon and a table of security bulletins.
- Security Blog:** A section with a green icon and a table of security blog posts.
- WinXP End of Support:** A blue banner with the Windows logo and the text "WinXP End of Support 2014-04-08".
- Hong Kong Security Watch Report:** A purple banner with the text "Hong Kong Security Watch Report".
- Hong Kong Google Play Store's Apps Security Risk Report:** A green banner with the text "Hong Kong Google Play Store's Apps Security Risk Report".
- Event Highlight:** A section with a green icon and a list of events.

Red text labels are overlaid on the image to identify specific sections:

- Security Bulletin** (pointing to the Security Bulletin section)
- Security Blog** (pointing to the Security Blog section)
- !! Hot topics** (pointing to the WinXP End of Support banner)
- Security Watch Report** (pointing to the Hong Kong Security Watch Report banner)
- Android App Risk Report** (pointing to the Hong Kong Google Play Store's Apps Security Risk Report banner)

HKCERT information

▶ RSS



HKCERT App



GovHK App



RSS Feed on Mail Client

1 @ ★ ↺ ↻ 從	主旨	日期	✕
☆ + + <香港電腦保安事...	SA13112001 Mozilla Firefox / Seamonkey 多個漏洞	20/11/2013 9:30	-
☆ + + <香港電腦保安事...	SA13112002 nginx UI 斷新漏洞	20/11/2013 9:47	
☆ + + <香港電腦保安事...	SA13112201 Drupal 多個漏洞	22/11/2013 8:41	
☆ + + <香港電腦保安事...	SA13112202 JPEGView 遠端區滿溢漏洞	22/11/2013 8:52	
☆ + + <香港電腦保安事...	[保安博錄] 每週通美保安簡訊 (2013年11月22日)	22/11/2013 15:22	
☆ + + <香港電腦保安事...	[保安博錄] 小心來歷不明的簡訊通知電郵	22/11/2013 16:16	
☆ + + <香港電腦保安事...	SA13112501 Ruby 浮點分析遠端區滿溢漏洞	25/11/2013 9:17	
☆ + + <香港電腦保安事...	SA13112601 IBM WebSphere Application Server 多個漏洞	26/11/2013 9:11	
☆ + + <香港電腦保安事...	SA13112602 思科 IOS IPSec ICMP 漏洞	26/11/2013 9:23	
☆ + + <香港電腦保安事...	[保安博錄] 香港地區 Google Play 商店應用程式保安風險報告	28/11/2013 11:11	
☆ + + <香港電腦保安事...	SA13112901 微軟視窗 NDProxy.sys 權限提升漏洞	29/11/2013 9:52	
☆ + + <香港電腦保安事...	[保安博錄] 每週通美保安簡訊 (2013年11月29日)	29/11/2013 15:22	-
往 香港電腦保安事故協調中心宜安快訊 -- 警報及博錄精選			
主旨 [保安博錄] 小心來歷不明的簡訊通知電郵		22/11/2013 16:16	
網站 https://www.hkcert.org/my_wel/zh/blog/13112202			
Route	Local message.	hops -	view -
		其他動作 -	

近日，HKCERT 收到某互聯網公司報告，多名 Yahoo 電郵用戶舉報收到一封互聯網服務逾期結單通知電郵，偽冒由 admin@one.yahoo-mail.com 發出。我們發現收件人都不是該互聯網公司的客戶，而電郵內的客戶名稱亦不是收件人。這封電郵表面上沒有網址連結，也沒有附件檔案，一般都被誤以為是錯誤傳送的電郵。但我們分析電郵 HTML 原始碼後，發現內容其實隱藏了一個黑客的網址連結，開啟了這封電郵的用戶可能會被導向至一個 Yahoo 電郵的釣魚網站和在背後被收集電腦上的操作系統和軟件版本資訊並傳送到黑客的伺服器。

Join HK Cyber Security Drills



2009 Hong Kong Incident Response Drill 2009

2010 Theme: Fighting financial crime on the Internet

2011 Theme: Handling Phishing Scams on Web Forum

2012 Theme: Defending Against Hacktivist Cyber Attack

2013 Theme: Responding to Targeted Attack

Proactive Measures

- ▶ Botnet Takedown
- ▶ Cyber Threat Intelligence
- ▶ Network Monitoring
- ▶ Network Hygiene – clean up vulnerable servers
- ▶ Cyber Security Drill

Security is not an Island

- ▶ Information security attacks are globalized
- ▶ HKCERT is sharing information and exploring collaborate with ISPs to make the Internet a safe place for all.

Thank You

A grayscale image of a hand holding a business card. The hand is positioned on the left side of the frame, with fingers gripping the card. The card is a light gray color and contains contact information for SC Leung.

SC Leung

- E scleung@hkcert.org
- W www.hkcert.org
- T 8105-6060 (hotline)