NETWORK SECURITY STARTS FROM US

By HKCERT

HKCERT

Agenda

- Current Network Security Threat
- Major cause of the Threat
- Counter measure against the Threat
- HKCERT action on Network Security Threat

HKCERT

CURRENT NETWORK SECURITY THREAT

Internet Connection Speed

- Global Peak Connection Speed: ~21 Mbps
- Hong Kong: 66 Mbps, Rank no. 2

	Country/Region	Q1 '14 Peak Mbps	QoQ Change	YoY Change
–	Global	21.2	-8.6%	13%
1	South Korea	68.5	6.5%	52%
2	Hong Kong	66.0	-3.3%	0.3%
3	Singapore	57.7	-2.5%	32%
4	Israel	57.6	5.3%	53%
5	Japan	55.6	4.7%	17%
6	Romania	54.4	7.0%	13%
7	Taiwan	52.6	2.1%	61%
8	Latvia	48.6	-1.0%	15%
9	Uruguay	45.4	24%	206%
10	Netherlands	45.2	3.6%	22%

Figure 15: Average Peak Connection Speed by Country/Region

HKCERT

Internet Connection Speed

- Global 4K Ready (>15Mbps) Connection: 11%
- Hong Kong: 26%, Rank no. 3

	Country/Region	% Above 15 Mbps	QoQ Change	YoY Change
–	Global	11%	19%	99%
1	South Korea	60%	15%	272%
2	Japan	32%	20%	52%
3	Hong Kong	26%	19%	39%
4	Switzerland	23%	14%	85%
5	Latvia	23%	25%	40%
6	Netherlands	22%	-0.9%	75%
7	Sweden	20%	5.6%	49%
8	Norway	18%	24%	85%
9	Finland	18%	29%	116%
10	Czech Republic	17%	-5.6%	75%

Figure 18: 4K Ready (>15 Mbps) Connectivity

HKCERT

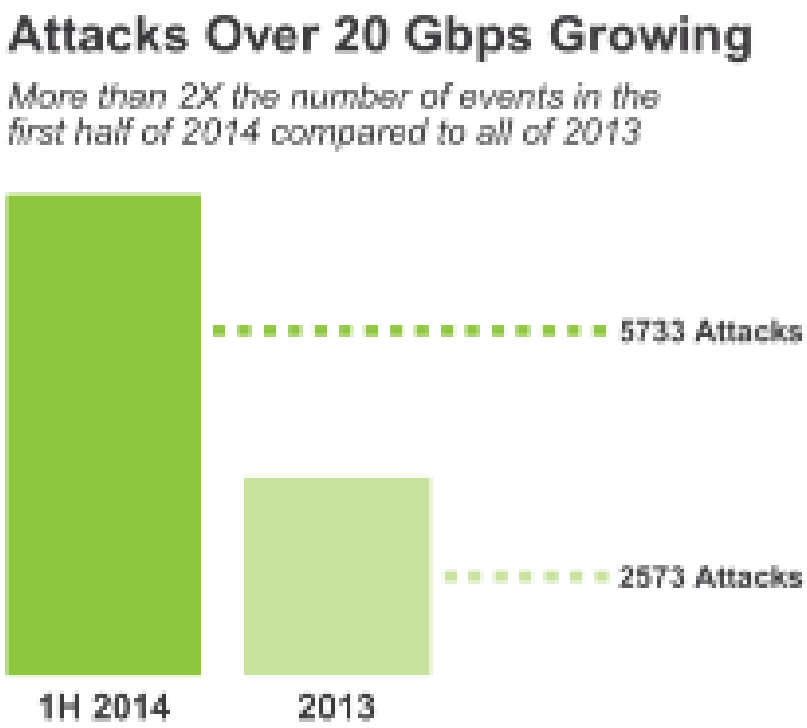
Internet Connection Speed

- Hong Kong Mobile Connection Speed:
- Avg. 4.9Mbps
- Peak 23.4Mbps

Country/Region	Q1'14 Avg. Mbps	Q1'14 Peak Mbps	% Above 4 Mbps
AFRICA			
Egypt	2.0	11.6	2.5%
Morocco	1.8	14.6	1.1%
South Africa	1.7	6.0	4.8%
ASIA			
China	4.8	12.2	57%
Hong Kong	4.9	23.4	42%
India	1.3	8.7	2.7%
Indonesia	2.0	10.8	3.5%
Iran	2.0	5.0	3.9%
Japan	5.7	47.3	61%
Kazakhstan	2.0	7.8	1.7%
Kuwait	3.5	33.1	17%
Malaysia	2.3	19.8	7.6%
Pakistan	1.5	14.7	2.8%
Singapore	3.6	23.2	19%
South Korea	14.7	41.3	78%
Sri Lanka	2.3	23.7	3.6%
Taiwan	3.4	27.8	13%
Thailand	2.0	35.1	4.6%
Vietnam	1.1	6.5	0.1%

HKCERT

DDoS Attack Trend



- http://www.arbornetworks.com/corporate/blog/5243-volumetric-with-a-capital-v

HKCERT

DDoS Attack Target

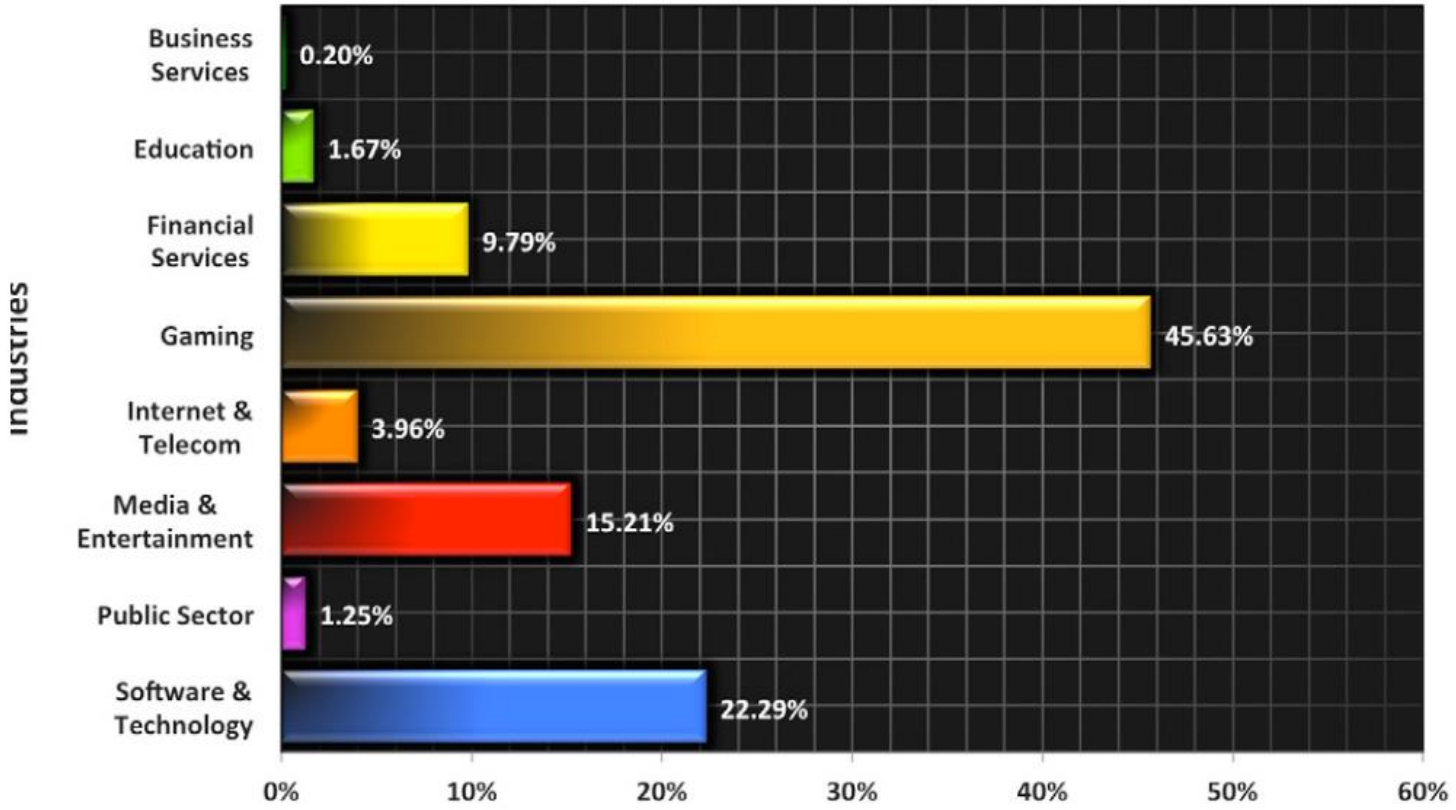


Figure 5: Industries most frequently targeted by DDoS attacks in Q2 2014

- http://www.akamai.com/html/about/press/releases/2014/press-072214.html

HKCERT

The Largest network attack

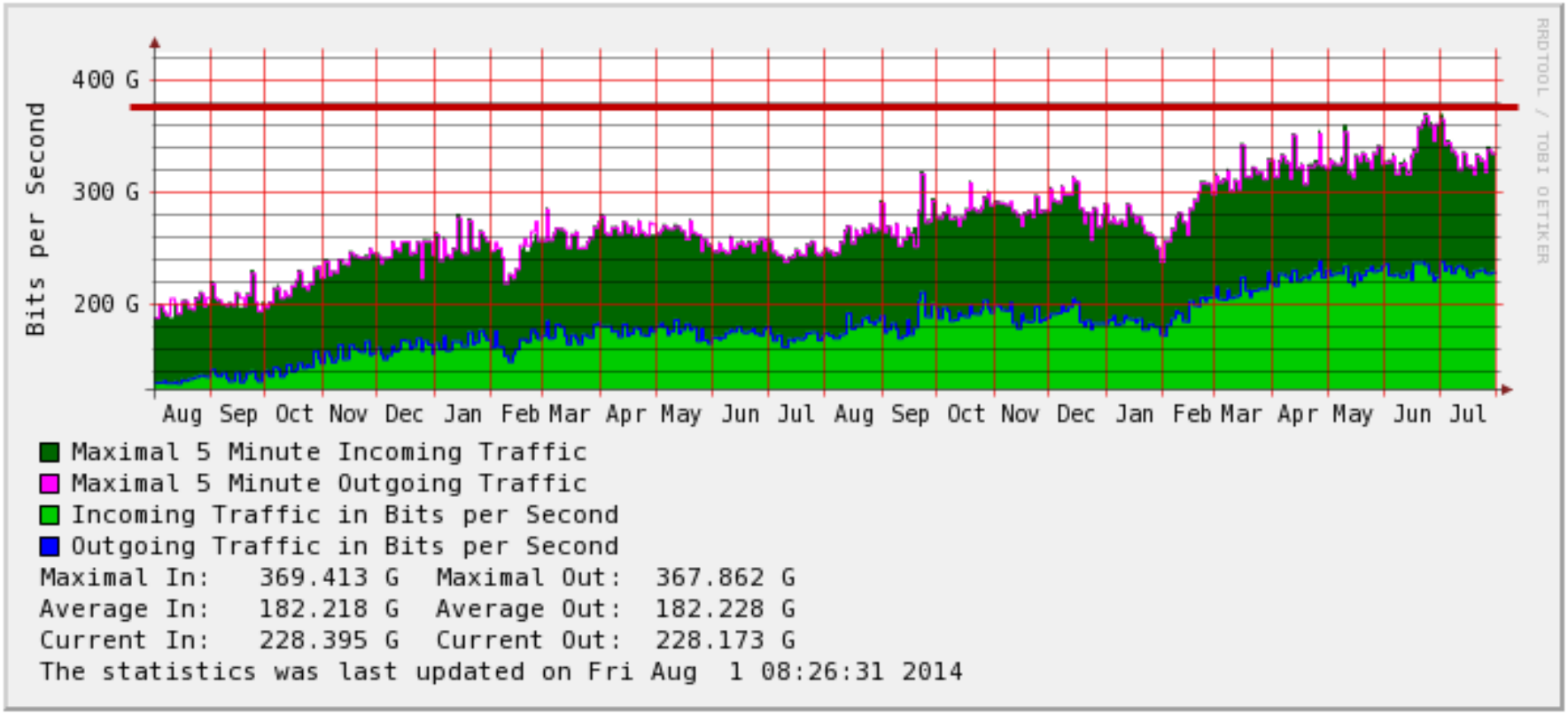
- Recorded by Cloudflare in Feb 2014
- Peak Traffic: 400Gbps
- NTP amplification attacks
- 4,529 NTP servers running on 1,298 different networks
- Each server directed to the victim (87 Mbps)

http://blog.cloudflare.com/technical-details-behind-a-400gbps-ntp-amplification-ddos-attack

HKCERT

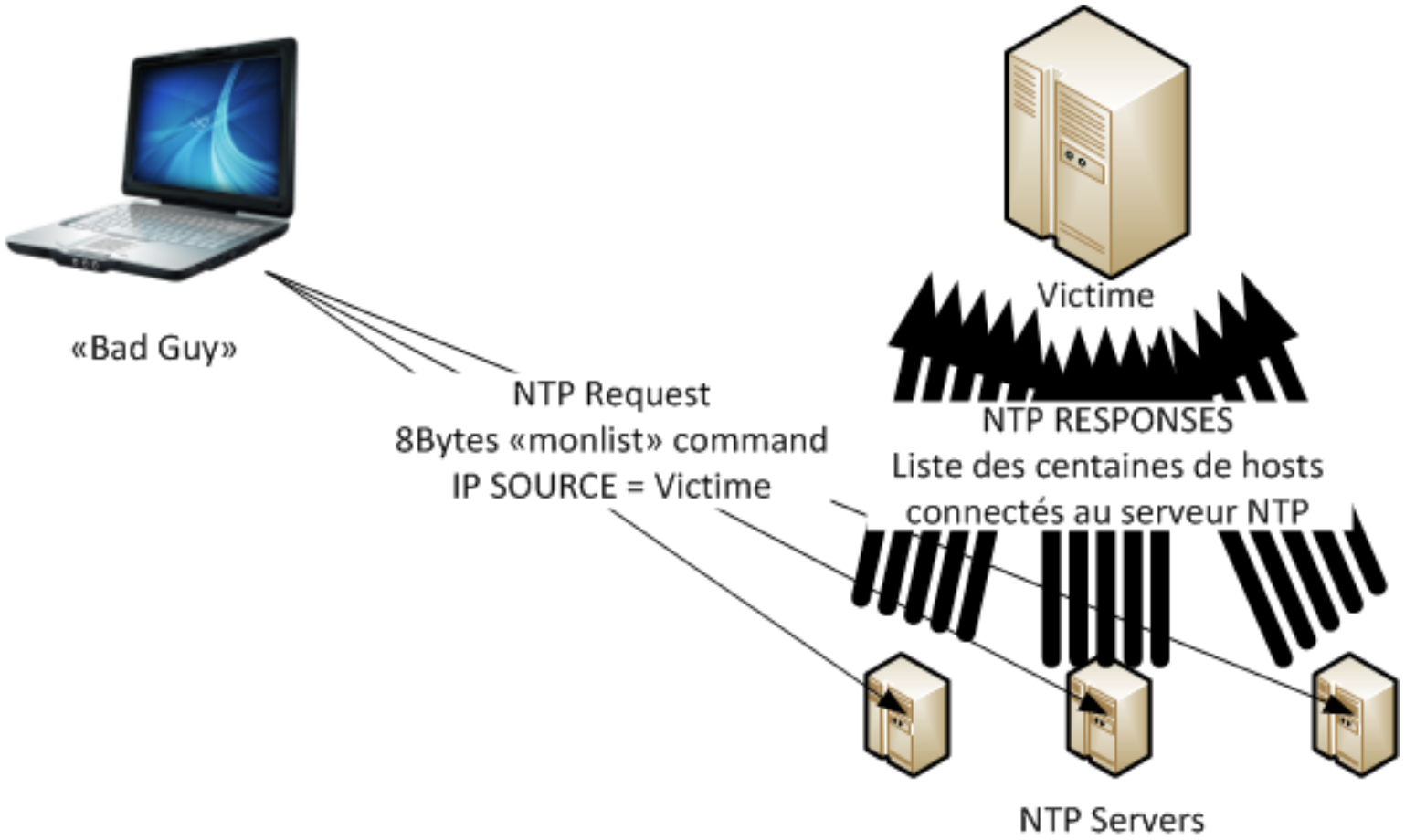
Bandwidth Utilization in Hong Kong

`Yearly' Graph (1 Day Average)



HKCERT

NTP Amplification Attacks



HKCERT

Amplification (UDP based) Attacks

Common protocols used in Reflection Attack

Protocols	Bandwidth Amplification Factor
NTP	~557
Chargen	~359
QOTD	140.3
DNS	Max. 54
SSDP	30.8
SNMP	6.3
Netbios	3.8

Reference

https://www.us-cert.gov/ncas/alerts/TA14-017A

HKCERT

Open Network service status

- Scanning Project conducted by Shadowserver in 2014
- Querying all computers with routable IPv4 addresses that are not firewalled from the internet

http://blog.shadowserver.org/2014/03/28/the-scannings-will-continue-until-the-internet-improves/

Open NTP

- **4,819,628** distinct IPs have responded to our NTP Mode 6 query

Top 20 Countries With Accessible NTP (Mode 6)

Country	Total
United States	1,062,816
Korea, Republic of	667,118
Russian Federation	382,694
China	356,531
Japan	310,307
Germany	220,119
France	128,239
United Kingdom	124,186
Italy	89,738
Brazil	88,076
India	82,418
Australia	79,495
Canada	75,709
Mexico	60,346
Sweden	57,920
Thailand	50,154
Hong Kong	47,032
Norway	40,942
Romania	36,061
Netherlands	36,018

https://ntpscan.shadowserver.org/

HKCERT

Open resolver (DNS)

- **7,029,195** distinct IPs appear to be openly recursive.

Top 20 Countries With Recursive DNS Servers

Country	Total
China	1,812,063
United States	685,542
Korea, Republic of	575,666
Taiwan	449,556
Brazil	364,717
Russian Federation	318,449
India	259,576
Japan	155,843
Turkey	130,848
Chile	130,436
Italy	121,544
Spain	100,243
Hong Kong	93,442
France	88,326
Colombia	80,321
Iran, Islamic Republic of	80,008
Poland	74,459
Mexico	67,062
Argentina	63,768
Philippines	60,331

https://dnsscan.shadowserver.org/

HKCERT

Open SNMP

- **6,028,996** distinct IPs have responded to our SNMP public query

Top 20 Countries With Open SNMP

Country	Total
Brazil	1,309,625
United States	826,179
India	642,659
Vietnam	264,298
China	228,228
Turkey	224,488
Russian Federation	188,941
Japan	188,073
Korea, Republic of	185,894
Italy	145,220
Iran, Islamic Republic of	129,711
Spain	125,409
Thailand	94,932
Malaysia	89,952
Canada	79,057
Colombia	77,383
Poland	73,080
Germany	71,768
Argentina	70,929
Egypt	70,778

https://snmpscan.shadowserver.org/

MAJOR CAUSE OF THE THREAT

Mis-configuration

Allow access from everyone

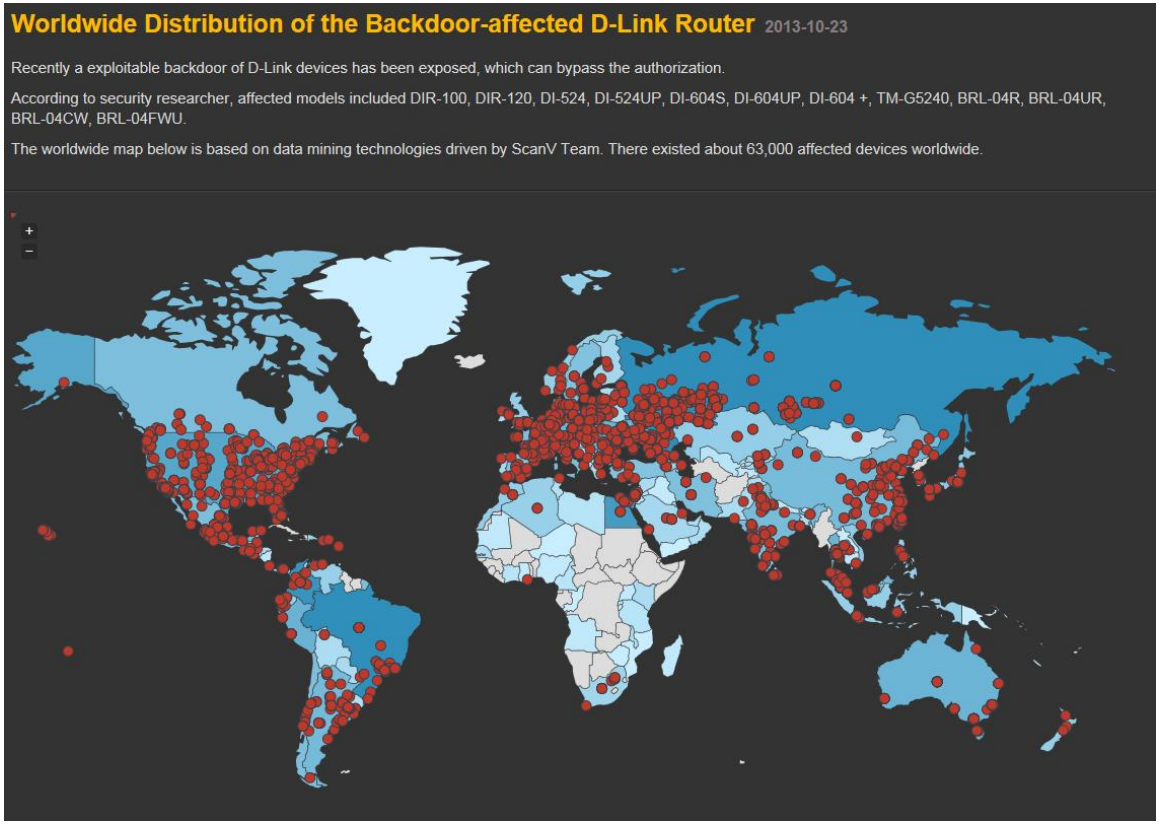
- DNS
  - Recursive name query
- SMTP
  - Open Relay
- NTP
  - Monlist

Weak password

Weak or Default Password

Network device management interface

- IPCam
- Router



- http://www.zoomeye.org/lab/dlink

HKCERT

Vulnerabilities

Unpatched Web Application

- CMS (Wordpress, Joomla, SugerCRM etc)
- Exploit Vulnerable Joomla to install bots
- Brobot target to US based bank
- DDoS attack since Sep-2012
- Up to 150Gbps

Incident Report in Hong Kong

Year to Date

- NTP amplification attacks

19

https://www.hkcert.org/my_url/en/blog/14022401

- DNS

2

https://www.hkcert.org/my_url/en/alert/14020701

- Joomla

32

https://www.hkcert.org/my_url/en/blog/13112901

HKCERT

COUNTER MEASURE AGAINST THE THREAT

Counter Measures

- Adopt BCP38 to prevent IP spoofing
- Fix or take down the amplifiers, e.g., for NTP or DNS
- Introduce rate limiting (with limited impact, though), such as DNS RRL
- Strong password / Public key
- Keep the system/application Up to date

Self Check

Openresolver Project

- http://www.openresolverproject.org/

Open NTP Project

- http://openntpproject.org/

Spoofer Project

- http://spoofer.cmand.org/index.php

HKCERT

HKCERT ACTION ON NETWORK SECURITY THREAT

HKCERT

Hong Kong Security Watch Report

- Released the 2nd Quarterly Report (Q2 2014) in Jul 2014
- Discover 16,589 unique security events
- Report details

https://www.hkcert.org/my_url/en/blog/14022601

HKCERT

Botnet Clean Up

Action	Organization
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

https://www.hkcert.org/botnet

HKCERT

Cyber Security Drill Exercise

2009 Hong Kong Incident Response Drill 2009
2010 Fighting financial crime on the Internet
2011 Handling Phishing Scams on Web Forum
2012 Defending Against Hacktivist Cyber Attack
2013 Responding to Targeted Attacks

2014 Schedule on Oct 2014

- Trusted parties
  - Providers of Internet services, HKIX, HKIRC, …
- Test communication procedure and technical skills

HKCERT

ISAC Mailing List

- Information Security Advisory and Collaboration
- Closed Communication Group for Trusted parties
  - Providers of Internet services, CERT, OGCIO, Police
- Share 1st hand information and discussions
  - Emerging security trends
  - Network status of Hong Kong

HKCERT

Build a Secure Cyber Space, Start from us

HKCERT Contact

8105-6060

hkcert@hkcert.org

www.hkcert.org/

HKCERT