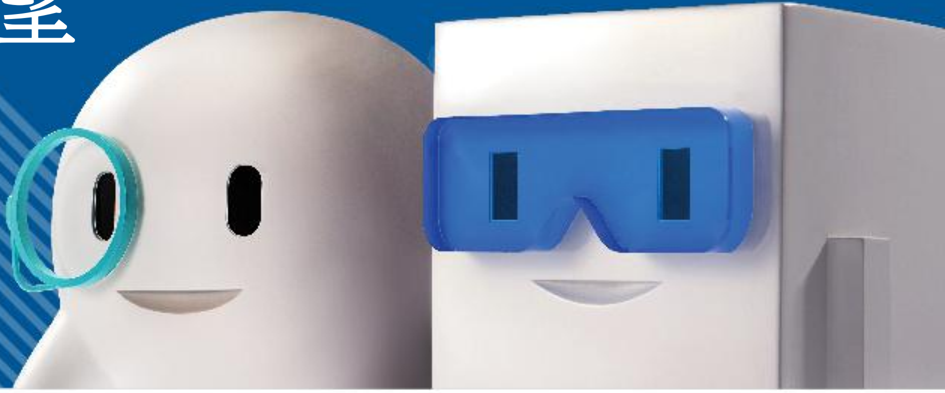
HKCERT

HKPC

Hong Kong Information Security Outlook 2015

香港資訊保安展望



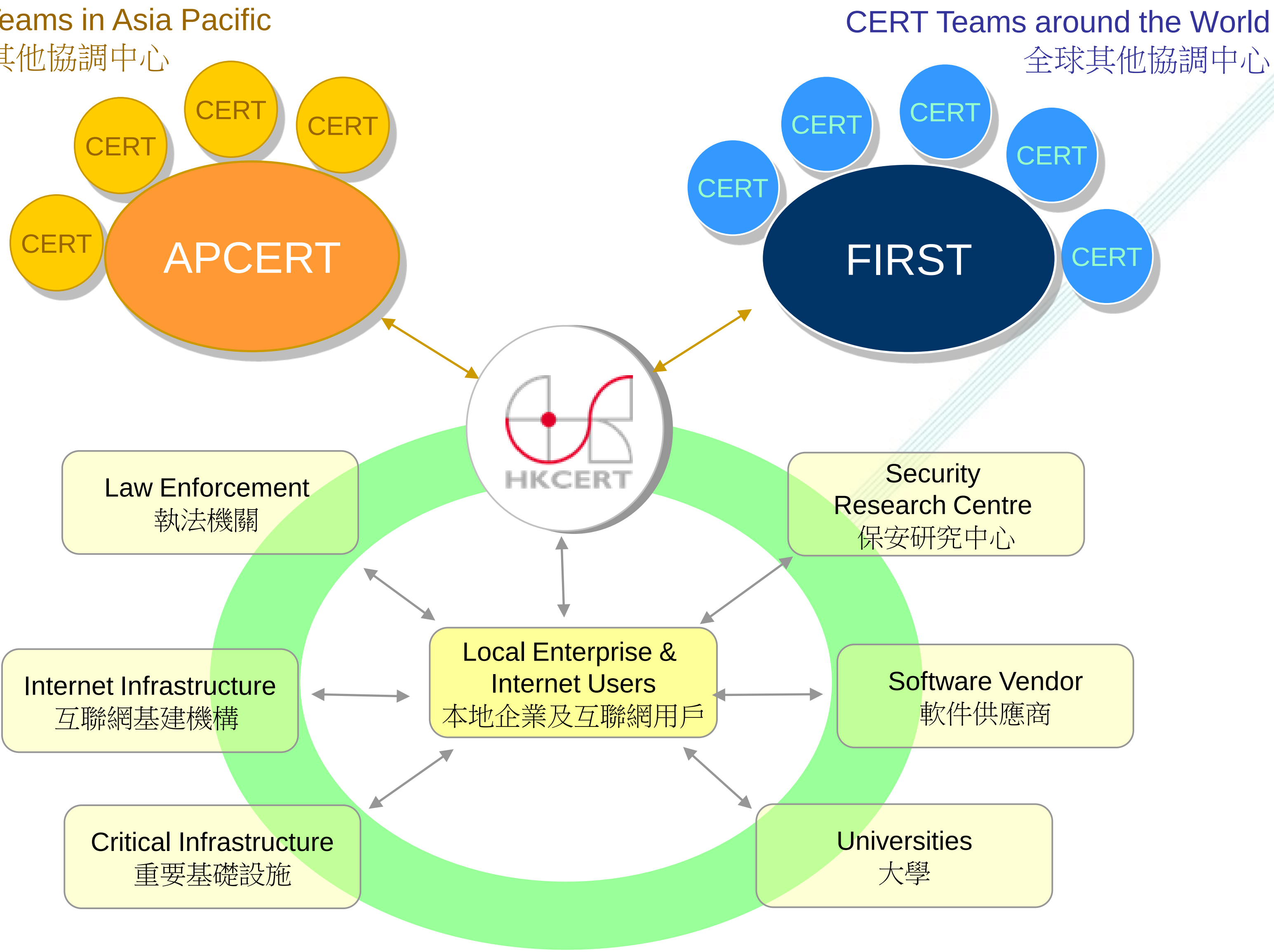
All-round Productivity Partner
全方位企業伙伴

Agenda

- Information Security Trends
  - Year 2014 in Review
  - Outlook for 2015
- Advice to the Public

Hong Kong Computer Emergency Response Team Coordination Centre

- 香港電腦保安事故協調中心 **(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

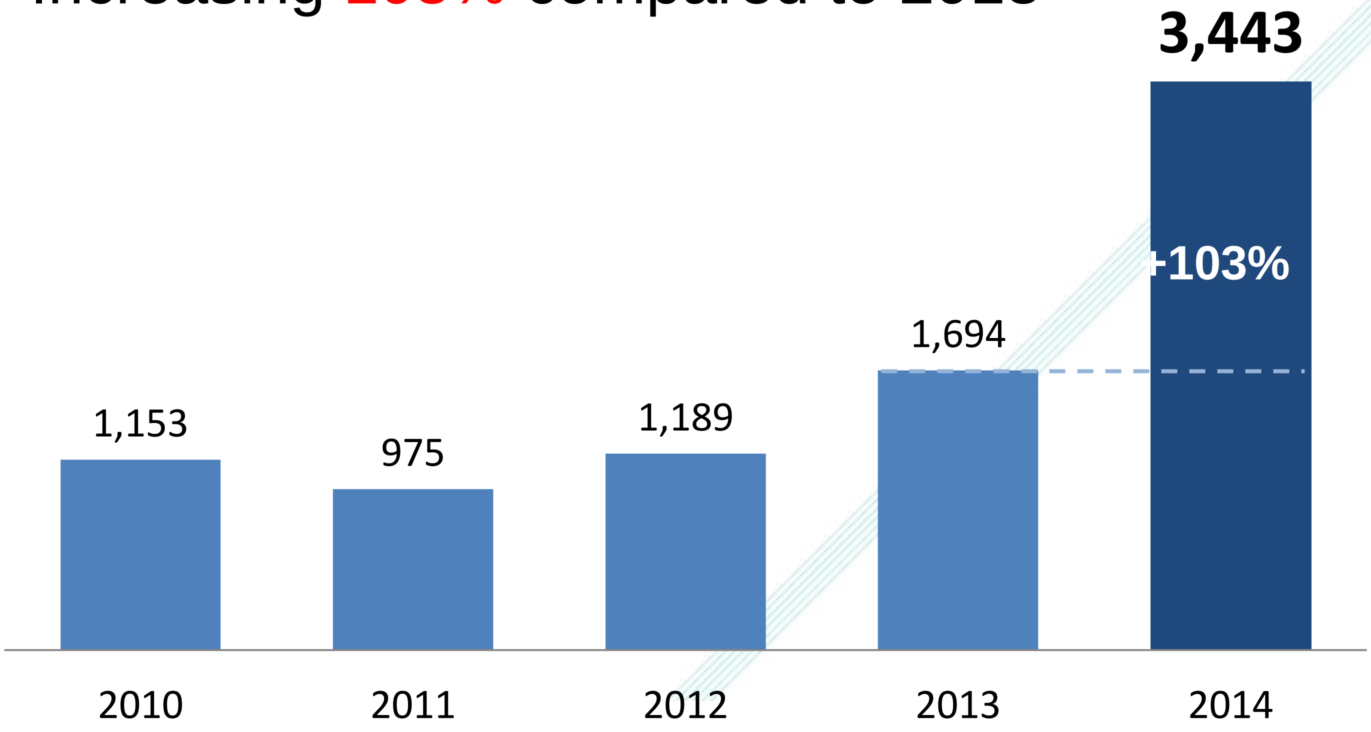
Summary of HKCERT Incident Reports for 2014

香港電腦保安事故協調中心
2014年保安事故報告摘要

Security Incident Reports
保安事故報告

Total Incident: 3,443

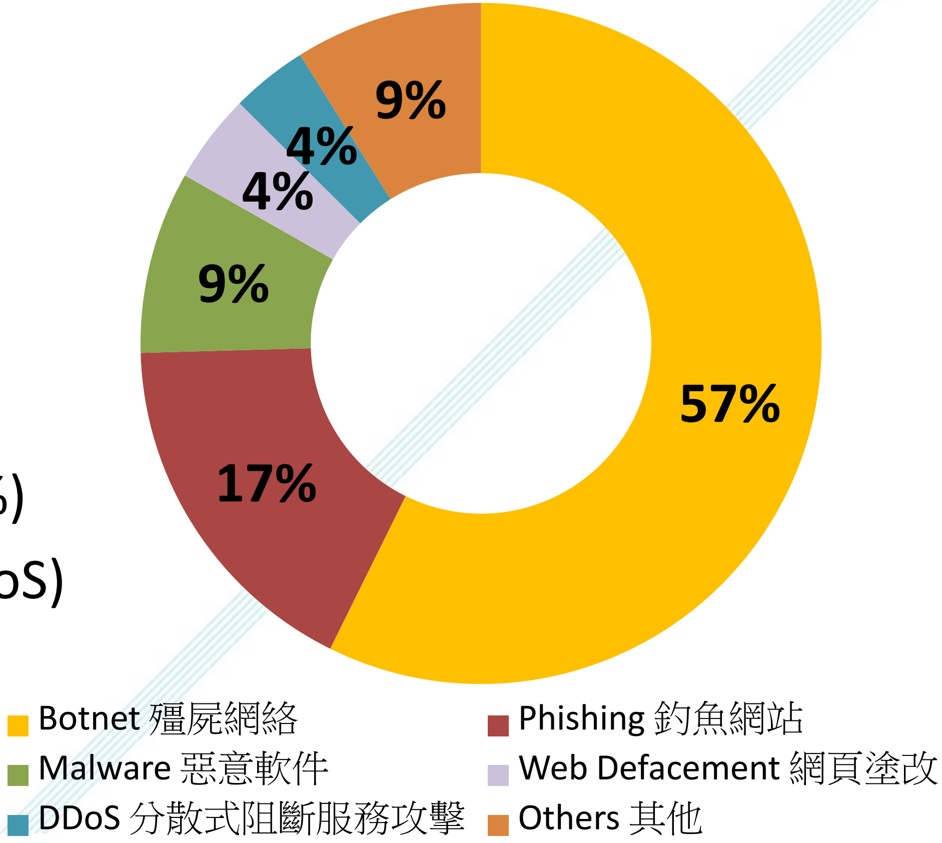
Increasing 103% compared to 2013



Incident Reports Breakdown in 2014
2014年保安事故報告的分佈

Total 總數: 3,443

- Botnet (殭屍網絡): 1,973 (57%)
- Phishing (釣魚網站): 594 (17%)
- Malware (惡意軟件): 298 (9%)
- Defacement (網頁塗改) : 146 (4%)
- Distributed Denial-of-Service (DDoS) (分散式阻斷服務攻擊): 125 (4%)



Growth of Major Incident Reports

- Botnet (殭屍網絡)
  - **1,973** cases in 2014 vs **432** cases in 2013 (↑357%)

- Phishing (釣魚網站)
  - **594** cases in 2014 vs **384** cases in 2013 (↑55%)

Increasing number of Incidents on Mobile and Internet Devices

- **Mobile Devices related** 流動設備
  - **154** cases in 2014 vs **35** cases in 2013 (↑340%)

- **Internet Devices related** 互聯網設備 **(new trend)**
  - **15** cases (**332** devices involved)

Security Outlook 2015

Potential Trends in 2015

1. **Scale of Attack 規模**
   - DDoS attack more powerful
   - Multiple servers attacked in single campaign

2. **Targets 目標**
   - Mobile and Cloud Platforms
   - Higher Value Targets
   - Internet Devices and “Internet of Things” (物聯網)

Potential Trends in 2015

3. **Mode of Attack 攻擊模式**
   - Botnets (殭屍網絡)
   - Ransomware (加密勒索軟件)
   - One-click Attack (一按攻擊)

1. Scale of Attack

- **DDoS attacks more powerful (100s of Gbps)**
  - More devices, higher bandwidth, online attacking tools

- **Multiple victims / servers attacked in a single campaign**
  - **Collateral damages** – no one is a bystander
  - Local compromised computers involved in attacks

2. Targets

Mobile and Cloud Platforms

Mobile botnet (流動殭屍網絡)

- Botnet command centres and hosting found

More iOS malware

WIRELURKER: A New Era in iOS and OS X Malware

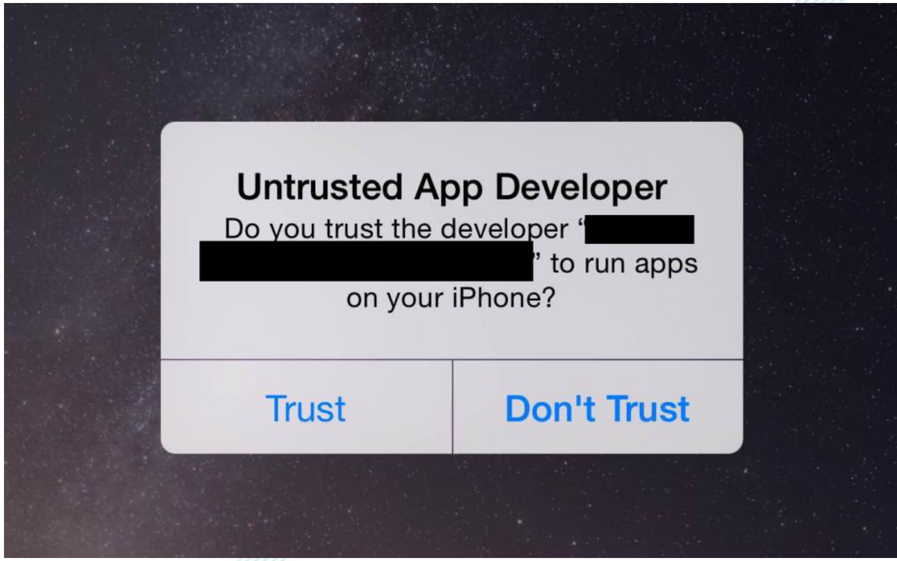
REPORT BY CLAUD XIAO unit42

Wirelurker infected JB & non-JB devices

- Infections via synchronization with desktop
  - Host Mac malware on piracy app store 麥芽地
  - Mac malware monitor USB connection, and sync with iOS device to infect it with WireLurker
- Use Enterprise provision profile to install malware not published on Apple app store

“Masque” iOS attack
- in Malware We Trust

- Enterprise provisioning vulnerability – no check on digital certificate
- Malicious app can replace genuine app with the same bundle identifier
- can even access the original app's local data



Untrusted App Developer

Do you trust the developer ‘[redacted]’ to run apps on your iPhone?

2. Targets

Personal Cloud

- Personal cloud services account breach
- Attackers break into personal cloud accounts to obtain personal data or make fraudulent transactions.

Mitigation

- Use strong password and two factor authentication

Image credit
http://technews.tw/2014/12/29/apple-denies-breach-in-celebrity-icloud-hack

2. Targets

- ➢ **Higher Value Targets**
  - **Credential data in Point of Sales Systems (POS)**

    入侵銷售點系統，盜竊信用卡和個人資料圖利
    - – Malware scans memory of POS for unencrypted credit card and personal credentials
    - – US large retail stores had tens or millions of customer data leaked

POS 系統被廣泛應用於零售、餐飲、酒店行業。

2. Targets

Protect POS

- Do not connect POS to the Internet or guest Wi-Fi
- Install security software on POS
- Change default administrator password
- Patch it regularly

2. Targets

- **Internet Devices and Internet of Things (IoT)**
  - **Hackers control Internet devices to steal data, or use them to launch attacks**
    - IP Camera – leaking personal privacy
    - Broadband routers – compromised by hacker to launch DDoS
    - TV Box – compromised by preloaded malware
  - **Potential threats for IoT (物聯網)**
    - Smart Home, Smart Watch or Industrial Control System (ICS) connected to the Internet

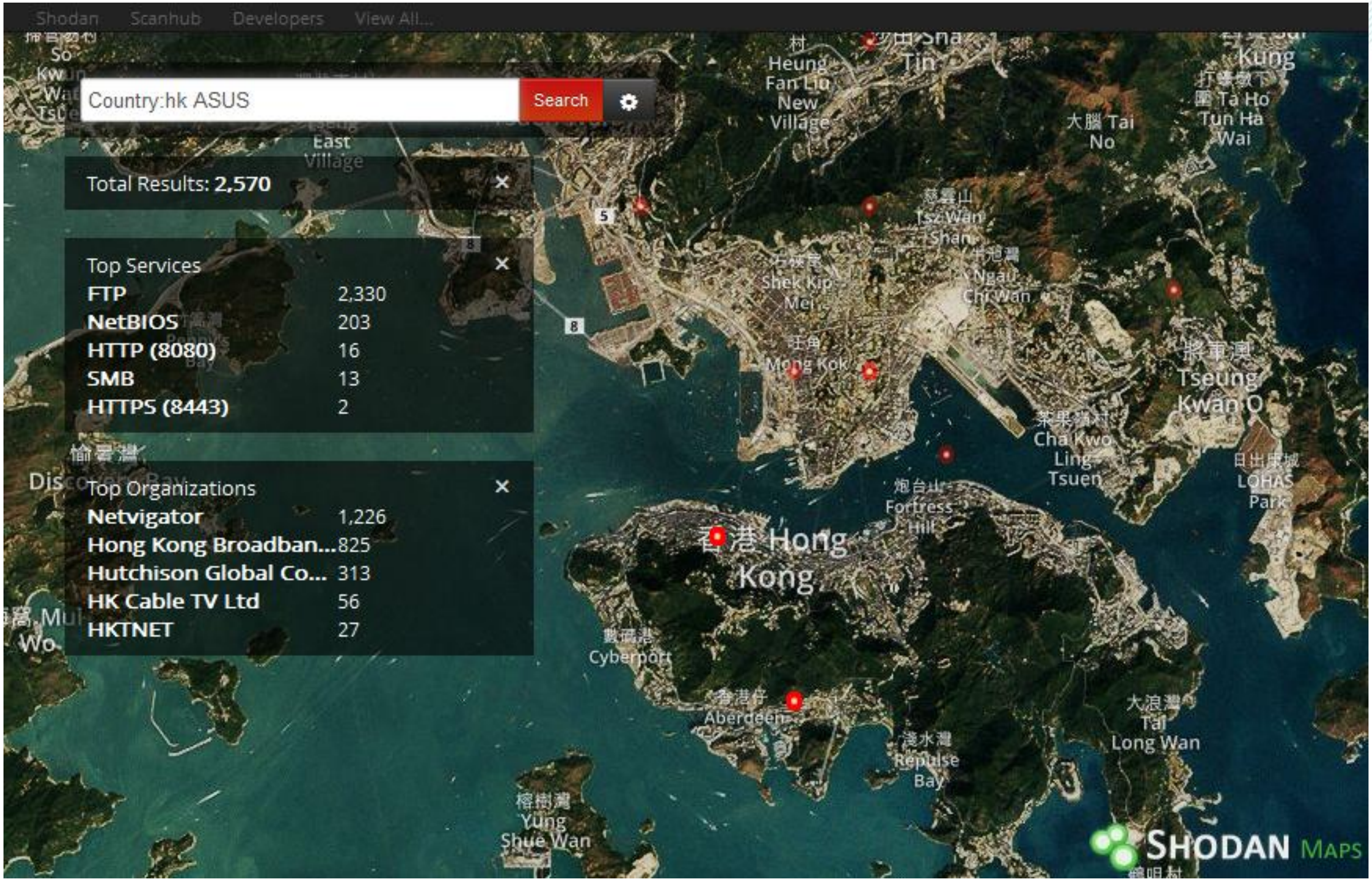
2. Targets

BB Router firmware vulnerability

- Some ASUS router models has unauthenticated command execution vulnerability
- Listen on port 9999 on LAN and WAN interface
- https://github.com/jduck/asus-cmd

2. Targets

- Search engine for the Internet of Things



Country:hk ASUS

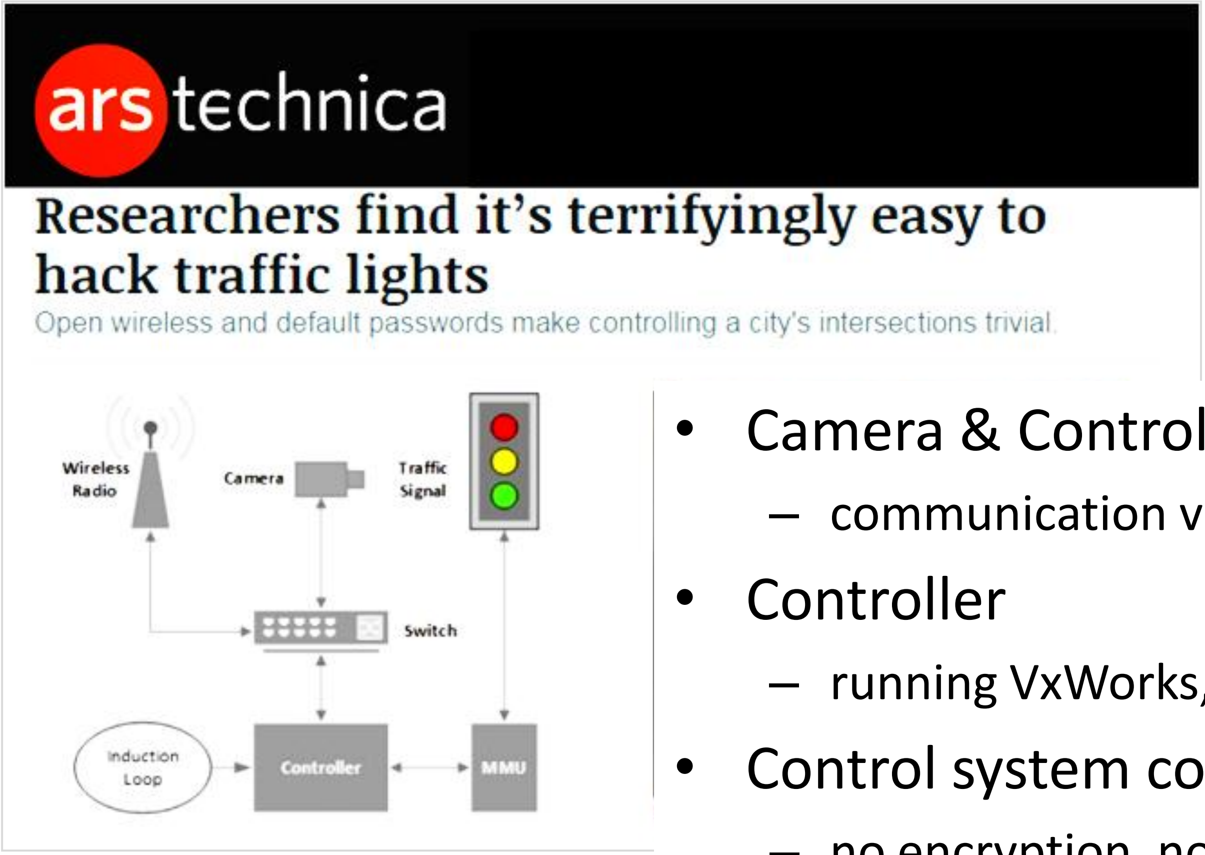
Total Results: **2,570**

Top Services	
FTP	2,330
NetBIOS	203
HTTP (8080)	16
SMB	13
HTTPS (8443)	2

Top Organizations	
Netvigator	1,226
Hong Kong Broadban...	825
Hutchison Global Co...	313
HK Cable TV Ltd	56
HKTNET	27

Attack Scenarios of Internet of Things

Smart Transport



ars technica

Researchers find it's terrifyingly easy to hack traffic lights

Open wireless and default passwords make controlling a city's intersections trivial.

- Camera & Controller of traffic light
  - communication via Wi-Fi
- Controller
  - running VxWorks, debug port open
- Control system communication
  - no encryption, no authentication

Researchers @ University of Michigan with road agency
August 2014

Smart Meters

Researchers: Spain electricity smart meters hack-able

Smart meter hack could leave homes in the dark

Possibilities

- Shut down home electricity
- Over/Under bill
- Forward data out
- Install network worm

Reference
http://www.itpro.co.uk/security/23251/smart-meter-hack-could-leave-homes-in-the-dark

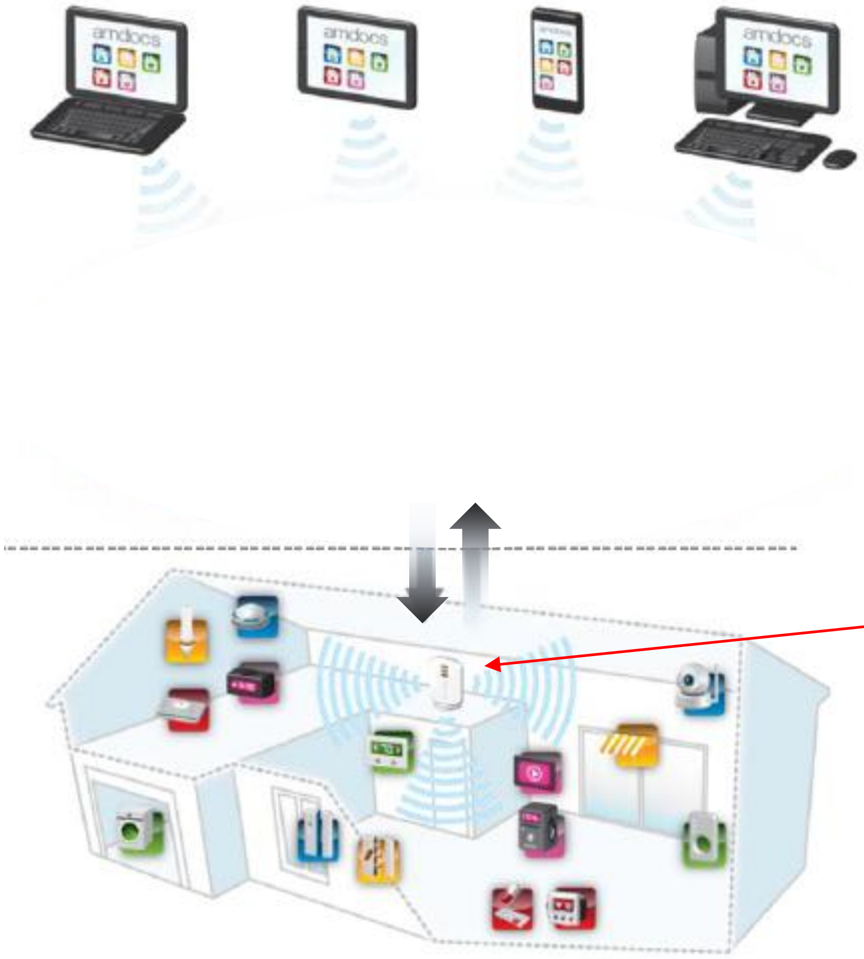
- Nest Thermostat
- Smart device integration
  - Mercedes-Benz tells Nest you’re on the way home → adjust temperature
  - Jawbone UP24 tells Nest your wake up
  - Nest Protect detects smoke or CO at home → inform you to call emergency
  - LG, Whirlpool refrigerator energy saving
  - LIFX mimic occupied house via lighting

http://www.techhive.com/article/2864067/works-with-nest-program-explodes-with-15-new-smart-device-integrations.html

- Nest users not aware of log content and cannot turn off
- Nest thermostat bootup has backdoor - bypass verification (Researchers @ University of Central Florida)
  - Can boot via USB and install any code
  - Can read log file that contains local Wifi credentials in plaintext
  - Can block sending log back to server

https://www.blackhat.com/docs/us-14/materials/us-14-Jin-Smart-Nest-Thermostat-A-Smart-Spy-In-Your-Home.pdf

Smart Home & Personal Cloud



- Remote Control
  - Mobile Devices
- Personal Cloud
  - Managed Service
- Home Gateway
- Home Devices

Reference:
http://www.gsma.com/connectedliving/wp-content/uploads/2012/05/Marcos-Zart-Amdocs_Connected_Home-SmartCity-2012-June.pdf

Security vulnerabilities

Devices

- Physical access
- Communication vulnerability
- DDoS
- Malware

Back End System

- System Auth. & Access Control
- Communication vulnerability
- DDoS
- Software API

Users

- Cloud account
- Malware
- User hacks device and breaks security

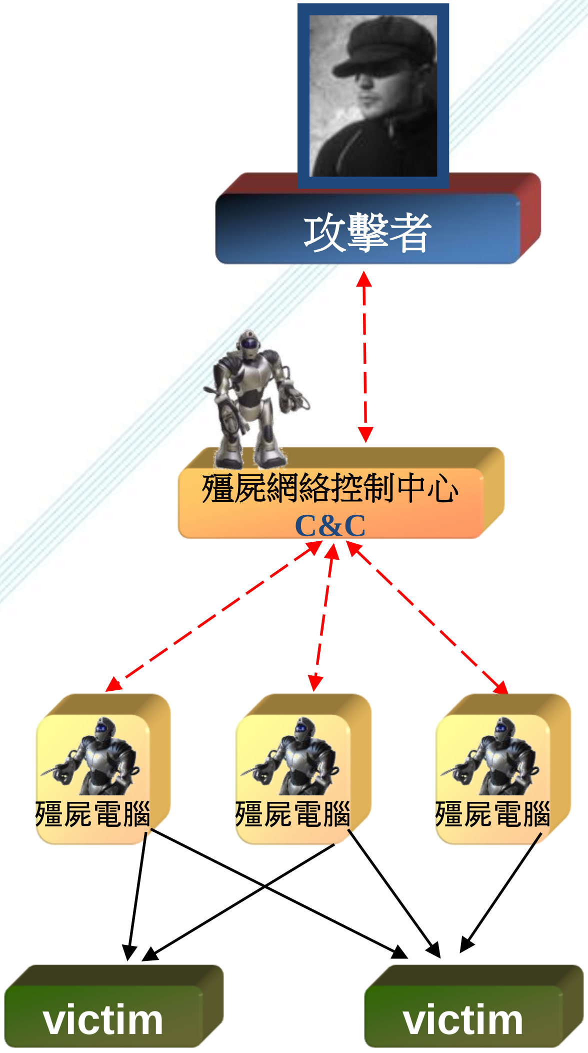
Security Impacts in Physical World

- Smart Systems connect with the physical world by automated Responses (with intelligent decision making algorithms based on sensor data)
  - Early Warning
  - Health Advice
  - Safety Control
  - Traffic Control
  - Other Controls
- What is the Consequence of attacks?

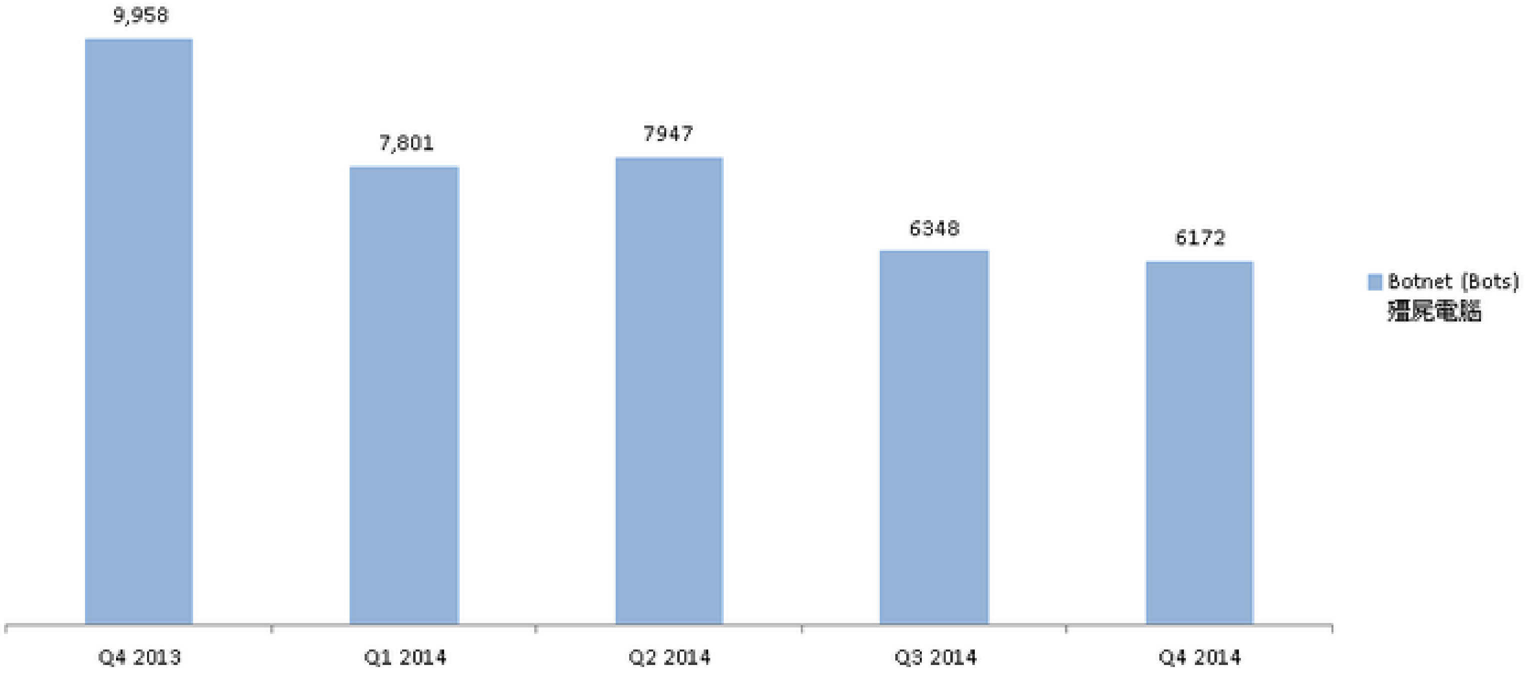
3. Mode of Attack

Botnet (殭屍網絡)

- Large number of computers or devices (bots) infected by malware (from thousands to millions)
- Controlled by attacker via botnet control centre



Trend of Botnet (Bots) security events
殭屍網絡(殭屍電腦)安全事件趨勢

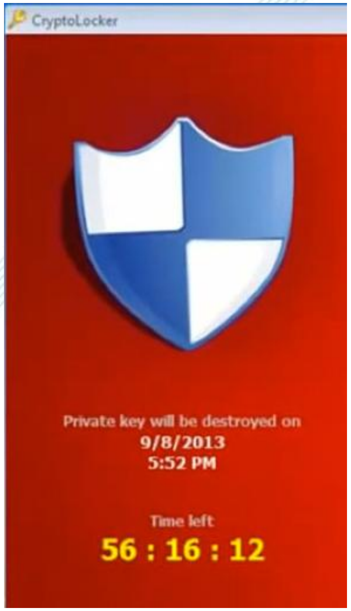


HKCERT: Hong Kong Security Watch Report Q4 2014

3. Mode of Attack

➢ Ransomware (加密勒索軟件)

- Encrypt victims’ data → demand ransom
- Targets
  - → **PC** (CTB-Locker, Cryptolocker, CryptoDefense, CryptoWall …)
  - → **Network attached storage** (SynoLocker)
  - → **Mobile devices** (SimpLocker)



Private key will be destroyed on
9/8/2013
5:52 PM

Time left
56 : 16 : 12

- New ransomware may **spread like virus**

3. Mode of Attack

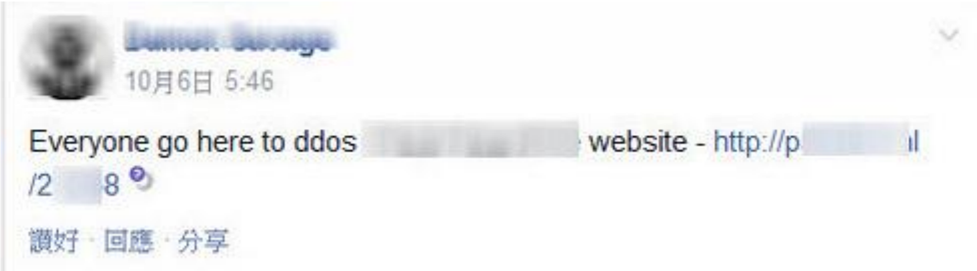
➢ One-click Attack (一按攻擊)

- Cyber criminals provide online attack tools

  網絡犯罪分子提供網上攻擊工具
- Lure people to click a link to help participate in attacks

  引誘市民參與「一按攻擊」, 作為幫兇

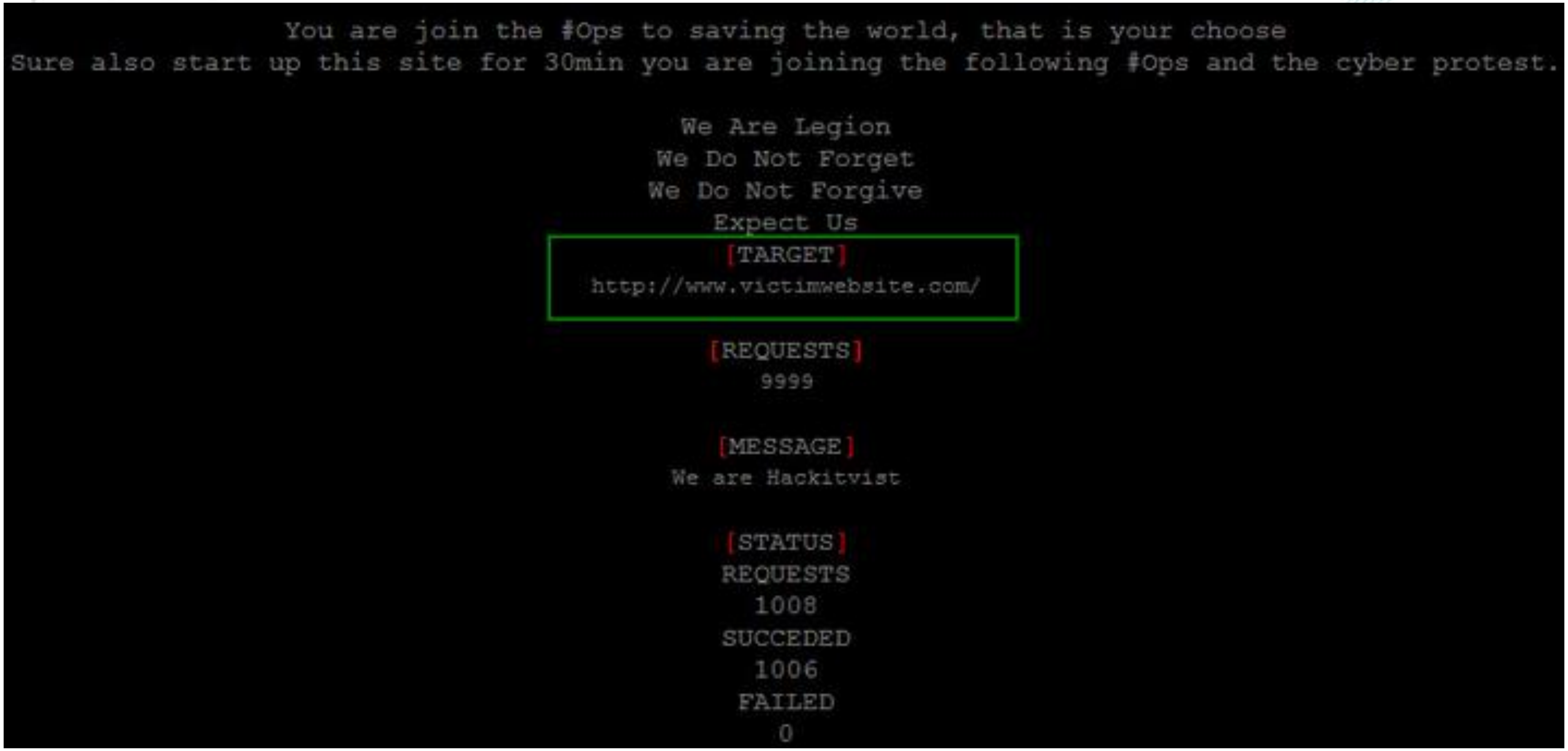
3. Mode of Attack



[redacted]
10月6日 5:46

Everyone go here to ddos [redacted] website - http://p[redacted]l /2[redacted]8

Attacker post a message with One-click attack URL on social networking site



```
         You are join the #Ops to saving the world, that is your choose
Sure also start up this site for 30min you are joining the following #Ops and the cyber protest.

                                  We Are Legion
                                 We Do Not Forget
                                 We Do Not Forgive
                                     Expect Us
                                      [TARGET]
                           http://www.victimwebsite.com/

                                     [REQUESTS]
                                        9999

                                     [MESSAGE]
                                  We are Hackitvist

                                      [STATUS]
                                      REQUESTS
                                        1008
                                      SUCCEDED
                                        1006
                                       FAILED
                                         0
```

Advice of HKCERT

Advice to Organizations

- **Patch servers**

  安裝保安修補程序

- **Strengthen POS system protection**

  加強銷售點系統保護

- **Proper management of BYOD**

  妥善管理 “自攜流動設備”

- **Backup data and keep offline copy**

  備份數據，並保持離線副本

- **Be cautious of social network, email / IM communication. Verify information via alternate channels (e.g. phone)**

  小心電郵/即時通訊，用其他渠道驗證信息 (例如電話)

Advice to Individual Users

- Do not participate in “One-click Attack”

  切勿參與「一按 DDoS攻擊」活動

- Patch computers
- Protect personal cloud services accounts
- Avoid becoming a bot 避免成為殭屍電腦

  殭屍電腦檢測和清洗步驟指南: https://www.hkcert.org/botnet

- Secure mobile devices 保護流動設備

  流動手機安全指南: https://www.hkcert.org/my_url/zh/guideline/13022802

- Secure Internet devices
- Be cautious of hyperlinks in SNS, SMS, IM communication

Q&A

HKCERT Contact

8105-6060

hkcert@hkcert.org

www.hkcert.org

香港電腦保安事故協調中心