

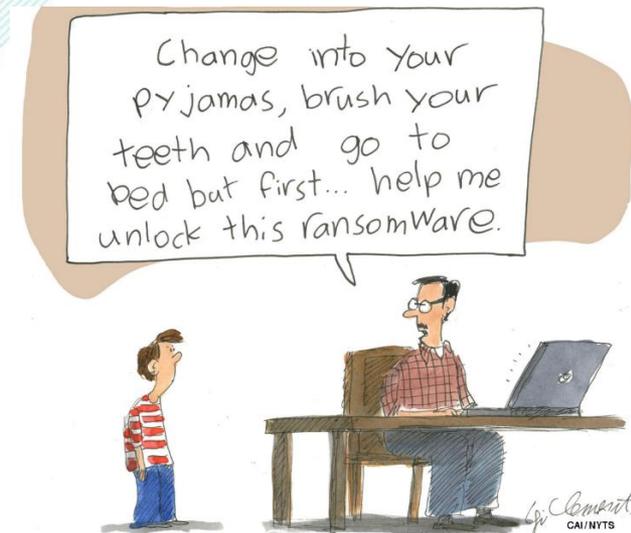


# Ensure Your Home Network Device is not the Next Botnet

Bernard Kan  
Senior Consultant  
HKCERT

# Agenda

- About HKCERT
- HKCERT Security Incident Report
- Potential Trend in 2018
- IoT Attacks
- Guideline for Selecting Smart Devices



# Hong Kong Computer Emergency Response Team Coordination Centre



香港電腦保安事故協調中心

- Established in 2001
- Funded by the HKSAR Government
- Operated by **Hong Kong Productivity Council**  
(香港生產力促進局)
- Mission
  - As the coordination of local cyber security incidents, serving Internet Users and SMEs in Hong Kong
  - As the Point of Contact of cyber security incidents across the border

# HKCERT Services



- Incident Report

**24-hr Hotline: 8105-6060**



- Security Watch and Warning

**Free subscription**

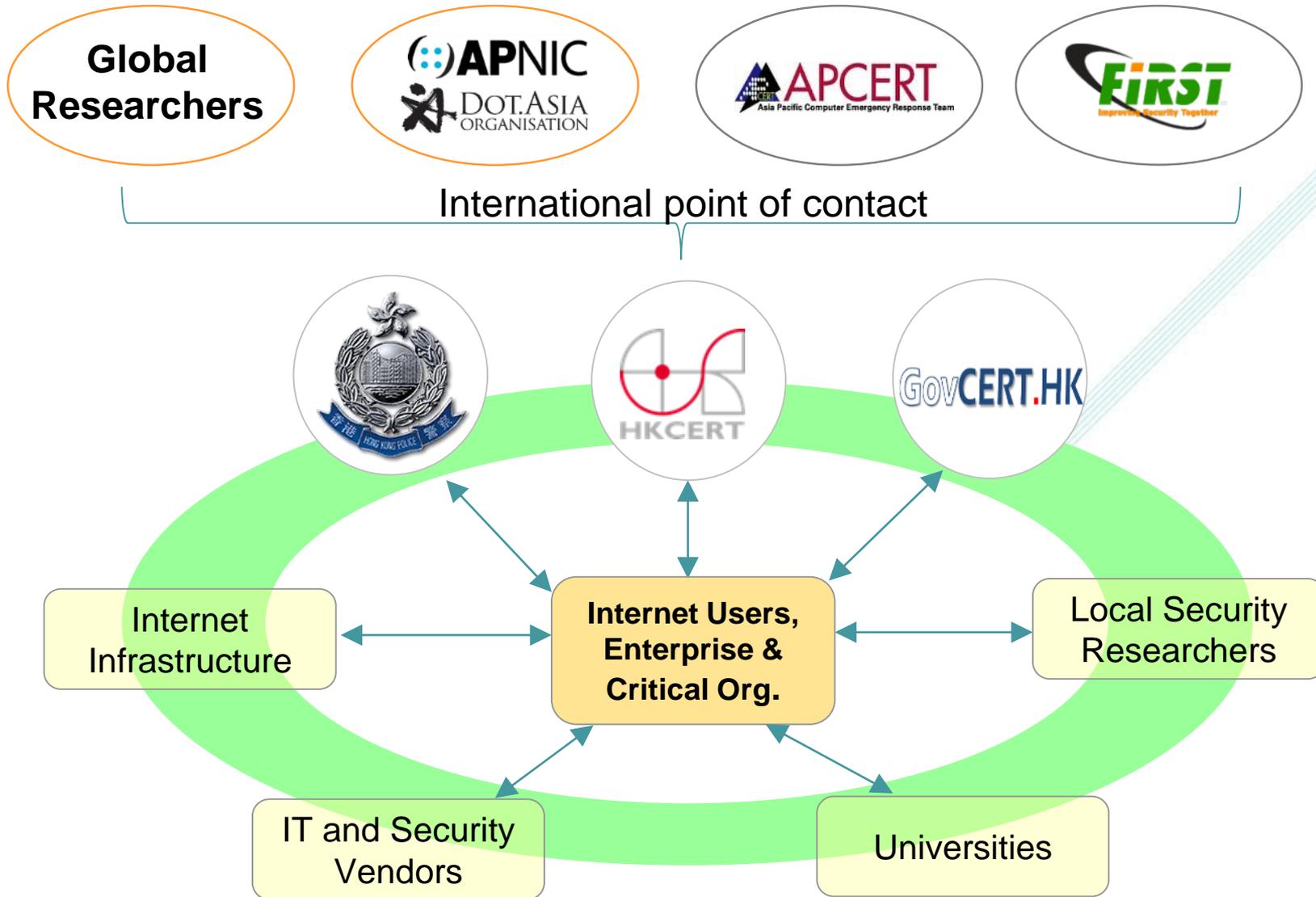


- Cross-border collaboration



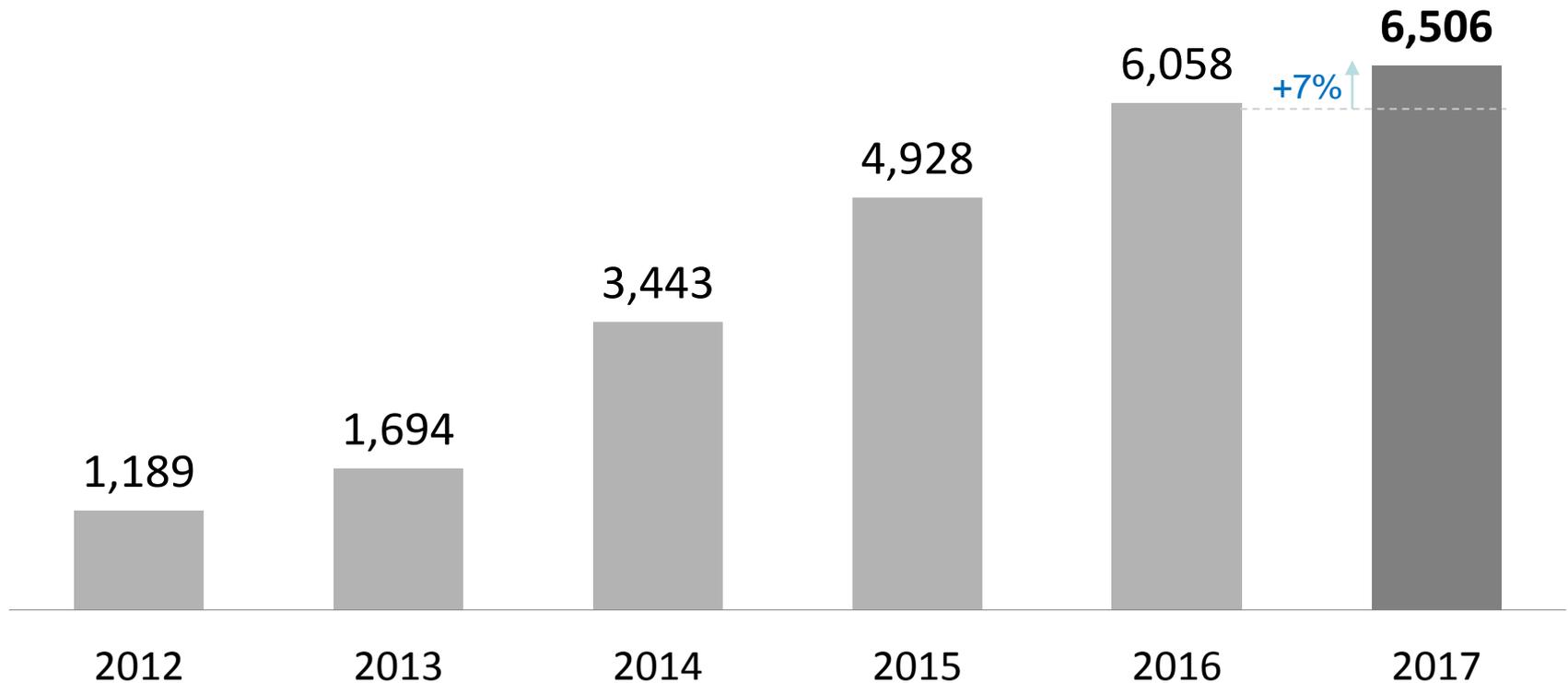
- Awareness education and guideline

# As the Coordination Centre



# HKCERT Security Incident Reports

## 保安事故報告



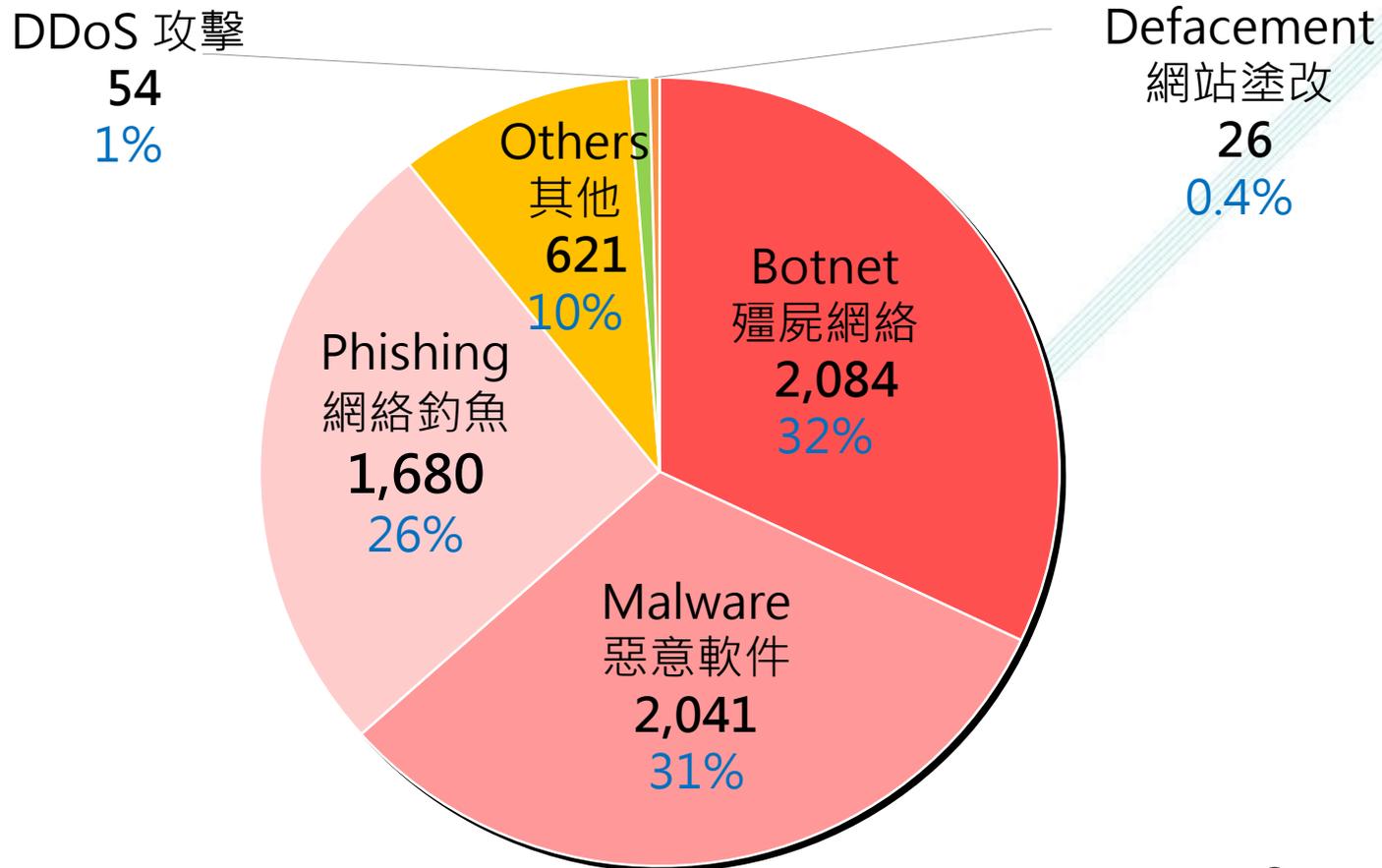
Referral cases with global collaboration accounted for **91%** of cases

與全球資訊保安機構合作, 2017年 **91%** 個案屬於轉介個案。

Source: HKCERT

# HKCERT Incident Reports in 2017 by Type

**Total : 6,506 (↑7%)**



# Potential Trends in 2018

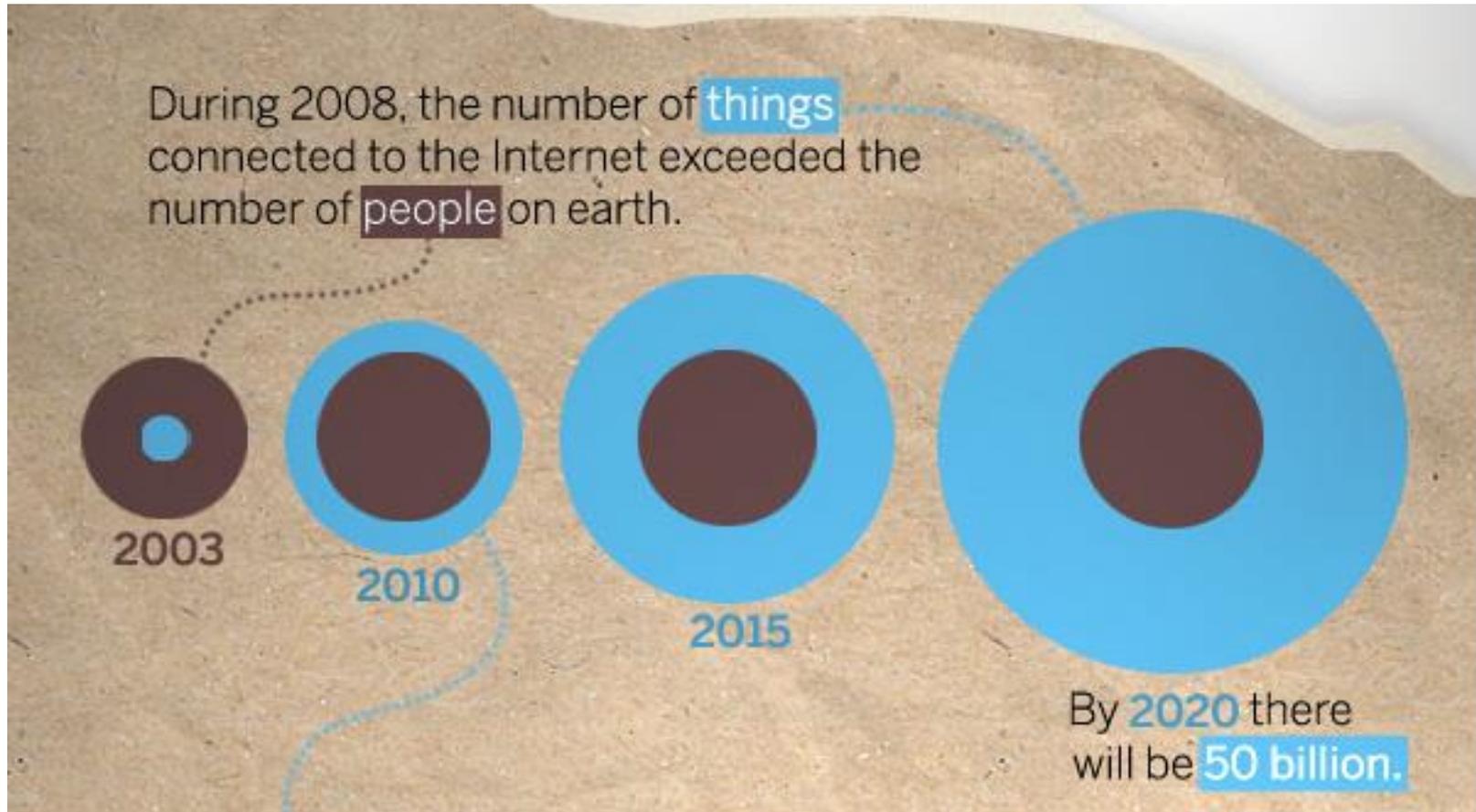


- 1. Financially Motivated Cyber Crimes** continue to proliferate  
以榨取金錢為目標的網絡攻擊持續上升
- 2. Internet of Things (IoT) attacks** on the Rise  
物聯網攻擊上升
- 3. Mobile Payment Apps** as New Attack Targets  
流動付款程式或成為攻擊對象
- 4. More Regulation** for Security and Privacy  
更多有關網絡安全和隱私的規管
- 5. Supply Chain Attacks** bypass Enterprise Defense  
供應鏈攻擊繞過企業的防禦

# What is Internet of Things (IoT)?

- A network of physical objects that contain embedded tech to communicate, sense, and interact with internal states or external environment (Gartner)
- “Uniquely identifiable objects (things) and their virtual representations in an Internet-like structure.” (Wikipedia)
- More general, the Internet of Things as non-traditional personal computing devices connected to the Internet either directly or indirectly.

# “Things” Connected to the Internet



Source: CISCO

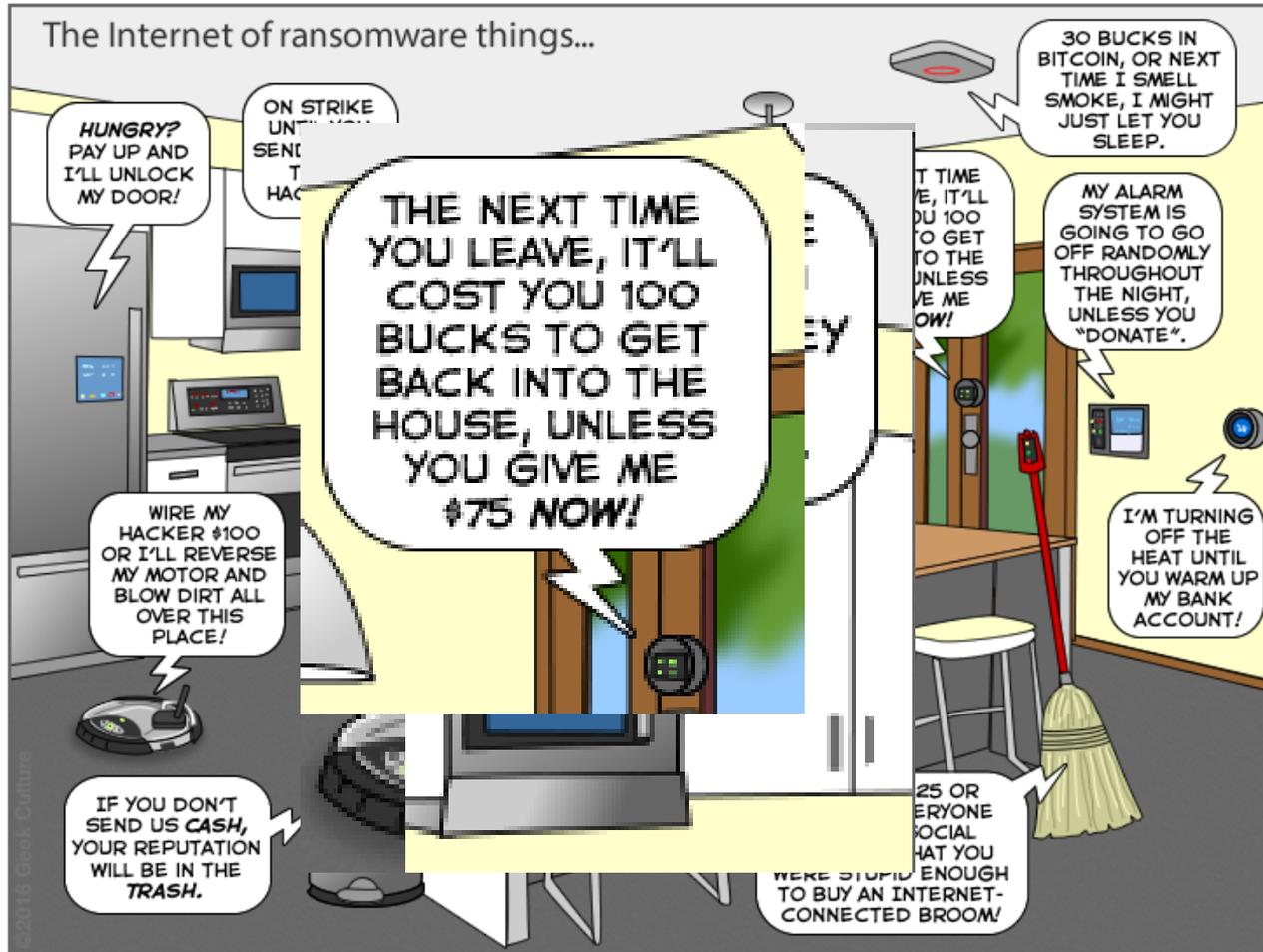
# Do I have IoT devices at home?





# What happen if IoTs were infected by ransomwares?

The Joy of Tech™ by Nitrozac & Snaggy



# What Can Go Wrong with IoT?

## Prying webcams used by artist to capture unsuspecting Hongkongers in controversial UK exhibition

Privacy experts have criticised a London artist for unfairly accessing peoples' personal data after home devices were used without consent to collect images from inside homes

PUBLISHED : Tuesday, 16 August, 2016, 2:03am

UPDATED : Wednesday, 17 August, 2016, 7:48pm

COMMENTS: 3

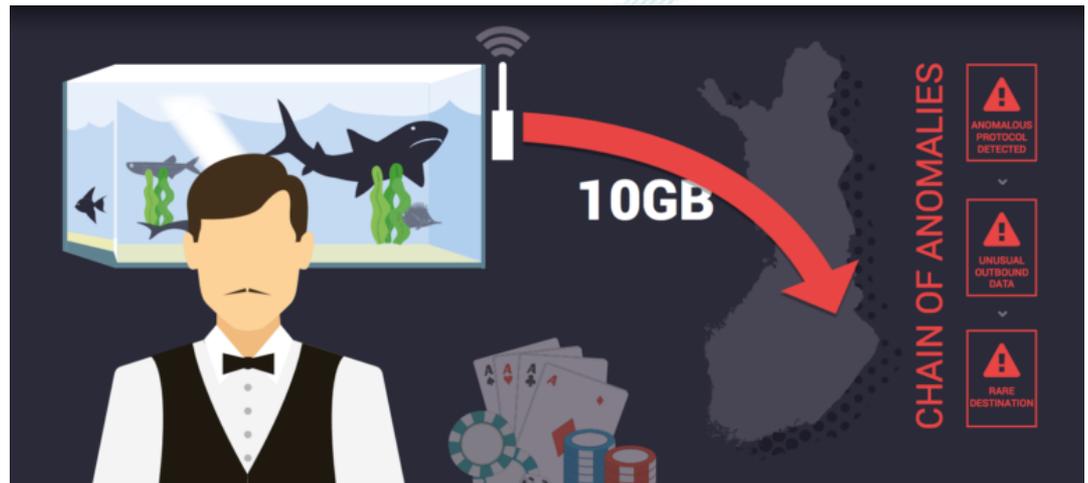


# What Can Go Wrong with IoT?



# What Can Go Wrong with IoT?

**A Casino Was Hacked Thanks To The Internet Of Broken Things & A Fish Tank Thermometer**



# Mirai Botnet

- Mirai is a piece of malware designed to launch multiple types of DDoS attacks
- The malware scans the internet for telnet servers then attempts to log in and infect them using a list of hard-coded passwords (most of which correspond to internet connected CCTV systems and routers)
- A botnets using the Mirai malware was responsible for the largest DDoS attack ever recorded, which peaked at 1.1 Tbps
- It exploits well-known hardcoded login credentials in IoT devices
- It uses segmented command-and-control which allows the botnet to launch simultaneous DDoS attacks against multiple, unrelated targets

# Mirai Botnet

```
USER:          PASS:
-----
root           xc3511
root           vizxv
root           admin
admin          admin
root           8888888
root           xmhdlpc
root           default
root           juantech
root           123456
root           54321
support        support
root           (none)
admin          password
root           root
root           12345
user           user
admin          (none)
root           pass
admin          admin1234
root           1111
admin          smcadmin
admin          1111
root           666666
root           password
root           1234
root           klv123
Administrator admin
service        service
supervisor     supervisor
guest          guest
guest          12345
guest          12345
```

```
USER:          PASS:
-----
admin1         password
administrator 1234
666666        666666
888888        888888
ubnt          ubnt
root          klv1234
root          Zte521
root          hi3518
root          jvbzd
root          anko
root          zlxx.
root          7ujMko0vizxv
root          7ujMko0admin
root          system
root          ikwb
root          dreambox
root          user
root          realtek
root          00000000
admin         1111111
admin         1234
admin         12345
admin         54321
admin         123456
admin         7ujMko0admin
admin         1234
admin         pass
admin         meinsm
tech          tech
mother        fucker
```



# The Reaper Botnet

- A new Botnet relying on more sophisticated takeover techniques
  - Spreads via nine different IoT vulnerabilities
- At least partially based on Mirai code
- Reports of up to 3.5 million infected devices
- Currently dormant: intention unknown
- Reaper includes an update mechanism

The image shows a debugger window with assembly code on the left and a world map on the right. The map is titled "TOP COUNTRIES" and shows several countries highlighted in red, including the United States, Canada, and parts of Europe and Asia. The word "REAPER" is written in large, bold, white letters across the map. The assembly code on the left is as follows:

Control	Jump	Base	+ Offset	= Address	Action
		0x2AAE2000	+ 0x00029244	= 0x2AB0B244	li \$a0,1
					jalr \$s4
		0x2AAE2000	+ 0x00055C60	= 0x2AB37C60	li \$a0,1
					jalr \$s1
		0x2AAE2000	+ 0x000202D0	= 0x2AB022D0	li \$a0,1
					jr 0x28+var_4(\$sp)
		0x2AAE2000	+ 0x0003C140	= 0x2AB1E140	li \$a0,1
					jr 0x28+var_4(\$sp)
		0x2AAE2000	+ 0x0003C1F8	= 0x2AB1E1F8	li \$a0,1
					jr 0x28+var_4(\$sp)
		0x2AAE2000	+ 0x0003CE70	= 0x2AB1EE70	li \$a0,1
					jr 0x28+var_4(\$sp)
		0x2AAE2000	+ 0x0003CF94	= 0x2AB1EF94	li \$a0,1
					jr 0x28+var_4(\$sp)
		0x2AAE2000	+ 0x0003D034	= 0x2AB1F034	li \$a0,1
					jr 0x28+var_4(\$sp)
		0x2AAE2000	+ 0x0003D57C	= 0x2AB1F57C	li \$a0,1
					jr 0x28+var_4(\$sp)
		0x2AAE2000	+ 0x0003D62C	= 0x2AB1F62C	li \$a0,1
					jr 0x28+var_4(\$sp)
		0x2AAE2000	+ 0x0003F1A4	= 0x2AB211A4	li \$a0,1
					jr 0x58+var_4(\$sp)

The world map on the right shows the following assembly code overlaid:

```
LOAD: 0004BCF0
LOAD: 0004BCF4
LOAD: 0004BCF8
LOAD: 00035840
LOAD: 00035840 loc_35840:
LOAD: 00035844
LOAD: 00035848
LOAD: 0003584C
LOAD: 00035850
LOAD: 00035854
LOAD: 00035858

move $t9, $s2
jalr $t9
nop

move $t9, $s1
lw $ra, 0x28+var_4
lw $s1, 0x28+var_8
addiu $s0, 0x28+var_C
jr $a0, 0xC
addiu $t9, $s0
```

# VPNFilter: New Router Malware with Destructive Capabilities



Image courtesy: Talos

Security research group Talos has released a report on a potentially destructive malware called "VPNFilter", which has infected at least 500,000 home routers and network-attached storage (NAS) devices in at least 54 countries [1].

According to the report, here are the known devices affected by the malware (updated on 2018-06-07):

- **ASUS:** RT-AC66U, RT-N10, RT-N10E, RT-N10U, RT-N56U, RT-N66U
- **D-LINK:** DES-1210-08P, DIR-300, DIR-300A, DSR-250N, DSR-500N, DSR-1000, DSR-1000N
- **HUAWEI:** HG8245
- **Linksys:** E1200, E2500, E3000, E3200, E4200, RV082, WRVS4400N [patch information]
- **MIKROTIK:** CCR1009, CCR1016, CCR1036, CCR1072, CRS109, CRS112, CRS125, RB411, RB450, RB750, RB911, RB921, RB941, RB951, RB952, RB960, RB962, RB1100, RB1200, RB2011, RB3011, RB Groove, RB Omnitik, STX5 [patch information]
- **Netgear:** DG834, DGN1000, DGN2200, DGN3500, FVS318N, MBRN3000, R6400, R7000, R8000, WNR1000, WNR2000, WNR2200, WNR4000, WNDR3700, WNDR4000, WNDR4300, WNDR4300-TN, UTM50 [patch information]
- **QNAP NAS:** TS251, TS439 Pro, Other QNAP NAS devices running QTS software [patch information]
- **TP-Link:** R600VPN, TL-WR741ND, TL-WR841N [patch information]
- **UBIQUITI:** NSM2, PBE M5
- **UPVEL:** Unknown Models
- **ZTE:** ZXHN H108N

Over 500,000 Routers  
Infected with destructive  
Malware - VPNFilter



# Why IoT Devices are so vulnerable?

- There's poor or non-existent security built into the device itself
- The device is directly exposed to the Internet because of poor network segmentation
- There's un-needed functionality left in OS based on generic and often Linux-derivative hardware & software
- Default credentials are often hard coded
- Security patches deployment is difficult

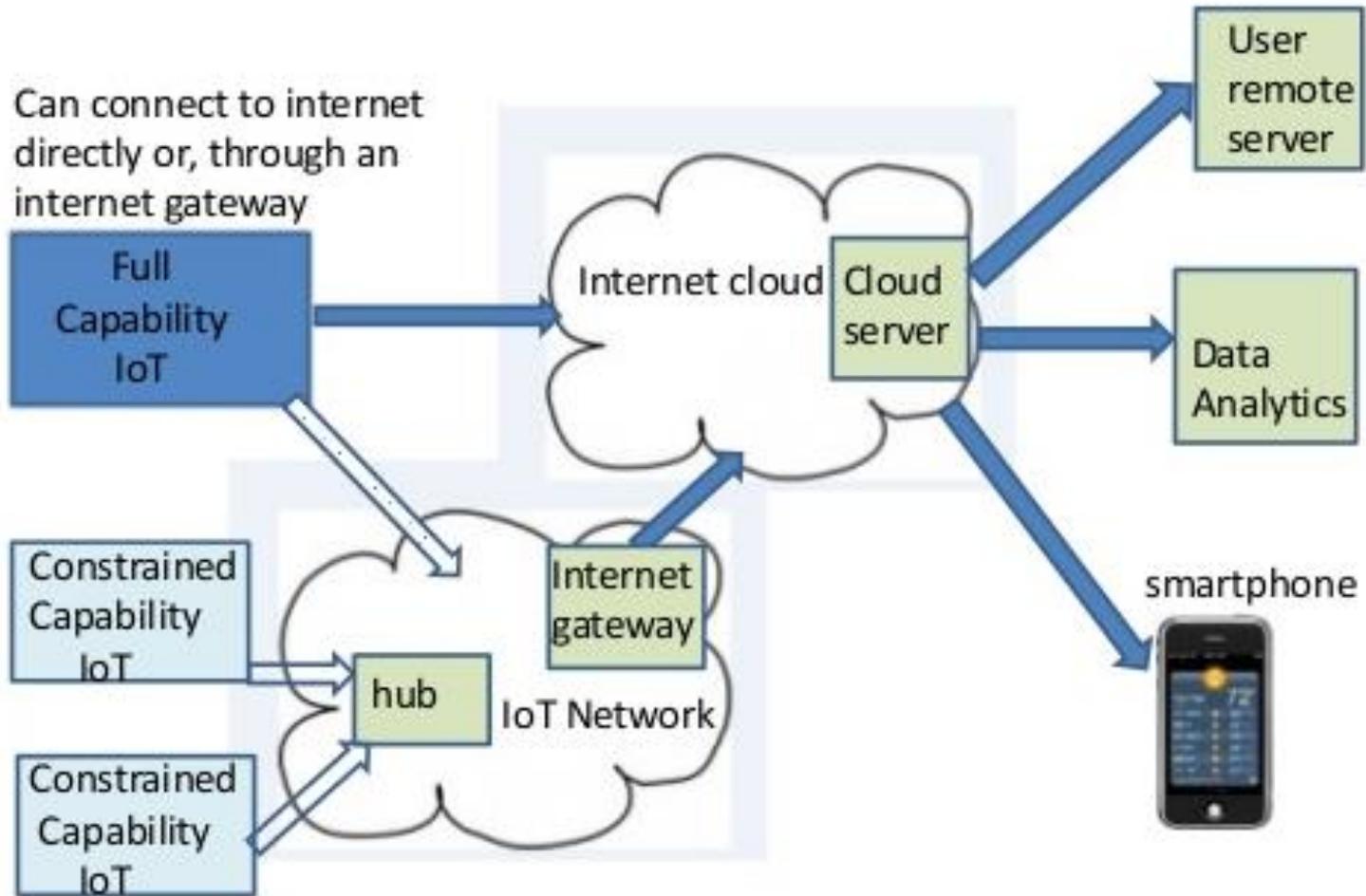
# Consumers and Business - How to Protect IoTs

- Evaluate if the devices you are bringing into your network really need to be smart. It's better to treat IoT tech as hostile by default.
- Segment the network
- Change the default credentials
- Apply patches and update whenever possible

# Developer Actions to Protect IoTs

- Have a red team audit the devices prior to commercial release.
- Force a credential change at the point of setup. (i.e., Devices will not work unless the default credentials are modified.)
- Require https if there's web access
- Remove unneeded functionality
- Provide mechanism for product update
- Security by design

# A Simplified IoT Architecture



# IoT Components Attack Surface

Components	Attack Surface
<b>Devices (Sensors, Gateways)</b>	Device memory, firmware, physical interfaces like USB ports, web interfaces, admin interfaces, Update Mechanism
<b>Communication Channel</b>	Device Network traffic using LAN, Wireless (Wi-Fi, ZigBee, Bluetooth)
<b>Cloud Interface</b>	Getting access to sensitive data/PII stored on cloud by Injection attacks, weak passwords or default credentials, Insecure Transport encryption.
<b>Application Interface (Web and mobile)</b>	Getting access to sensitive data or PII by exploiting vulnerabilities like OWASP web and mobile Top 10, in application interfaces.

# Buying and installing tips for Smart Devices

## To select the product, you need to:

- Understand the brand's credit
- Understand the product issues and handling methods of vendor in the past two years
- Understand the frequency of firmware update provided by the vendor
- Whether the product has an official verification
- Make sure the network connection is using encryption
- You can download the user manual to find out if enough security controls are provided
- Make sure the management interface is using encryption
- The device is easy to update the firmware
- The device is easy to install

# Buying and installing tips for Smart Devices (Cont')

## Regarding device installation you should:

- Install in internal network, not connecting the internet directly
- Separate trusted and untrusted network. If possible establish an additional separate network for smart devices
- Disable the Universal Plug and Play (UPnP) function on the router
- Keep the firmware up-to-date, check at least twice a year whether the manufacturer's website has new firmware updates
- Use a strong password and change it regularly. If possible use one password for one device
- Management interface should not open directly on the Internet. Only open necessary service
- If the device is not necessarily connected to the cloud, please disable it. Enable cloud connection will increase security risk
- When internet service is not in use (such as SmartTV), unplug the network connection
- Use the search engine (such as Google) regularly. Try to enter the equipment brand name and model to search if there are any security issues.

# Summary

- Internet of Things (IoT) attacks are expected to rise as number of IoT devices continue to grow in coming years
- Securing IoT devices may be difficult due to constraints of hardware & software
- Consumers and business need to consider their real needs in selecting IoT devices and secure the devices as far as possible
- IoT developers and manufacturers need to adopt a security by design approach
- Consumers need to take extra care to ensure that the device is secure and will be not compromised by hackers

# Q&A

**HKCERT Hotline: 81056060**

**[www.hkcert.org](http://www.hkcert.org)**