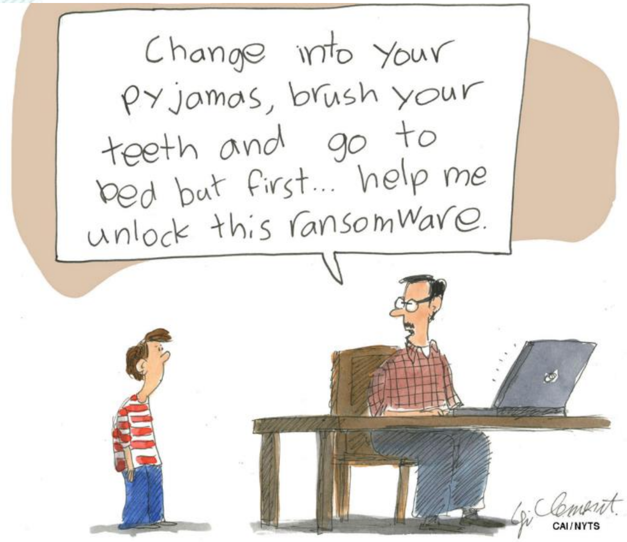
Build a Secure Cyberspace 2018

Cybersecurity Outlook 2018 &
Supply Chain Security

Bernard Kan
Senior Consultant
HKCERT

Agenda

- About HKCERT
- HKCERT Security Incident Report
- Potential Trend in 2018
- Supply Chain Attacks


Change into your pyjamas, brush your teeth and go to bed but first... help me unlock this ransomware.
CAI / NYTS

Hong Kong Computer Emergency Response Team Coordination Centre

HKCERT

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

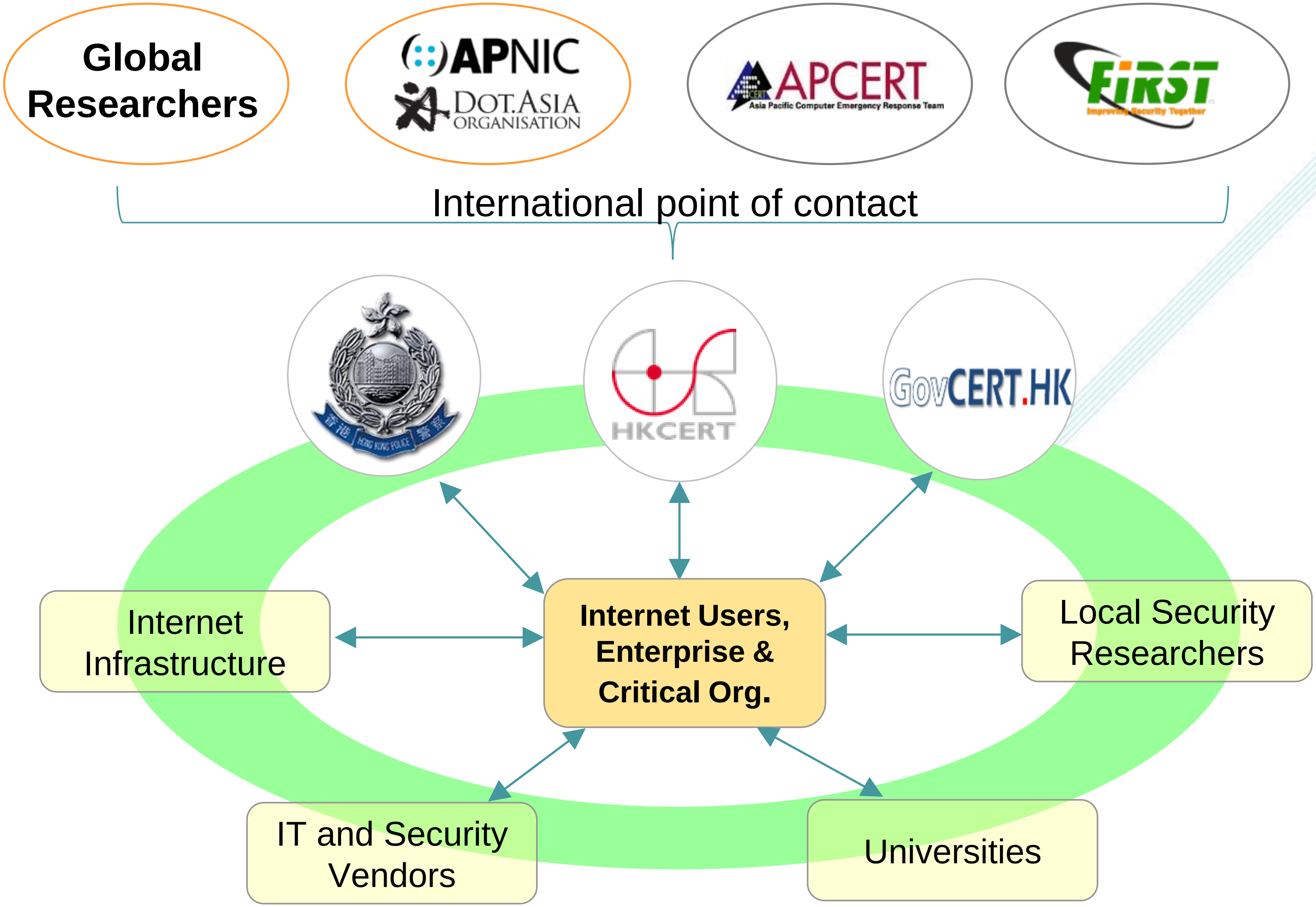
- Security Watch and Warning

Free subscription

- Cross-border collaboration

- Awareness education and guideline

As the Coordination Centre



Global Researchers

International point of contact

Internet Users, Enterprise & Critical Org.

Internet Infrastructure

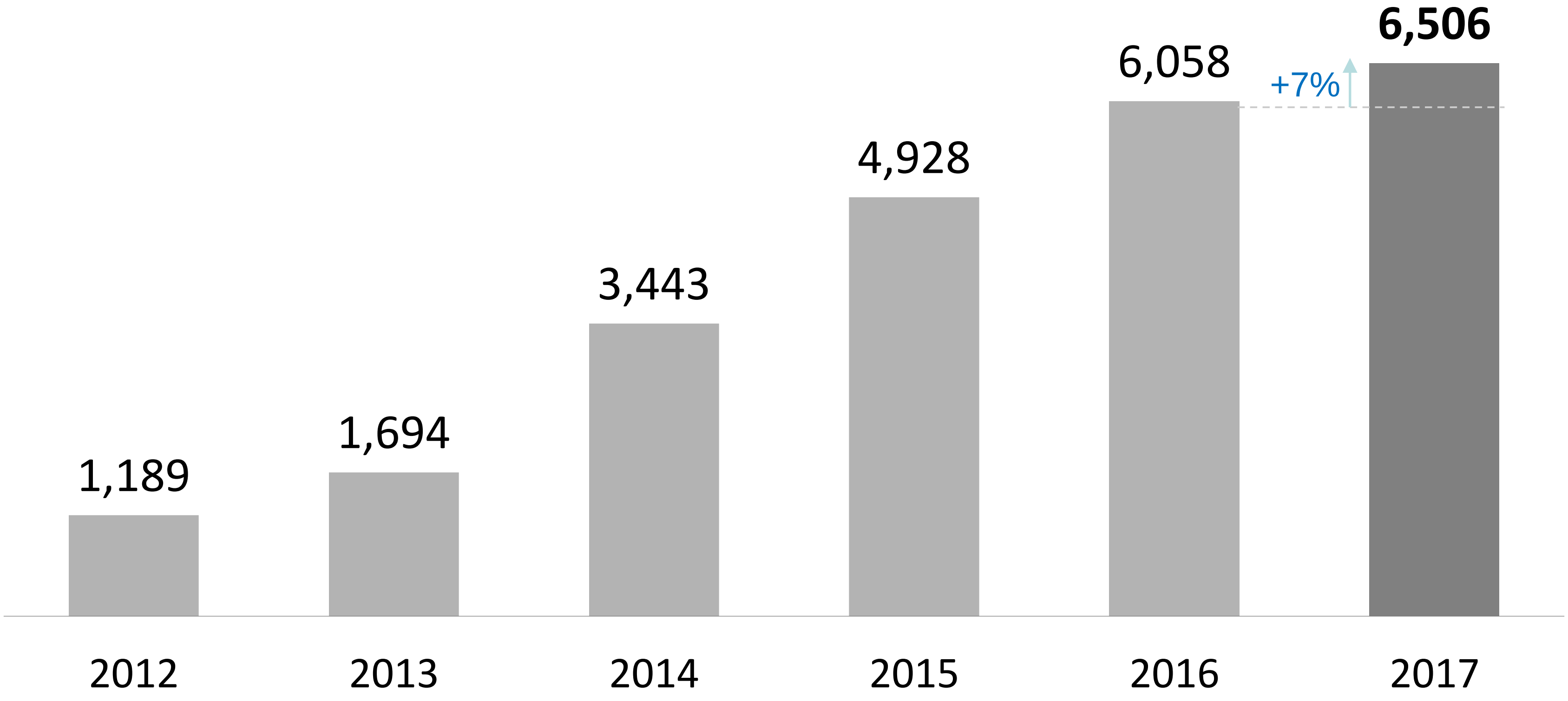
Local Security Researchers

IT and Security Vendors

Universities

APNIC
DOT.ASIA ORGANISATION
APCERT
Asia Pacific Computer Emergency Response Team
FIRST
Improving Security Together
HONG KONG POLICE
HKCERT
GovCERT.HK

HKCERT Security Incident Reports
保安事故報告



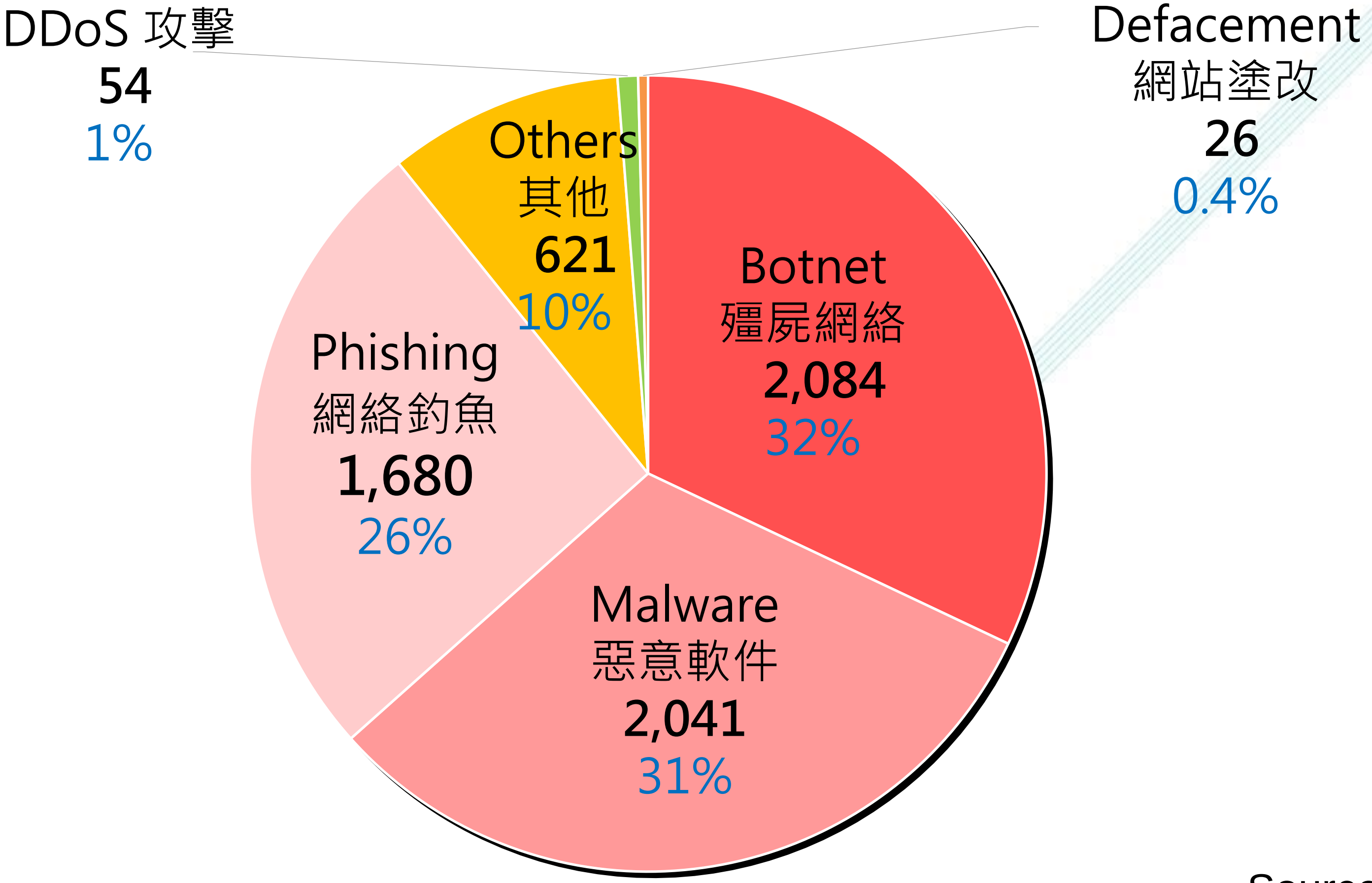
Referral cases with global collaboration accounted for **91%** of cases

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%)



Source: HKCERT

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 Supply Chain Attack?

- "Supply Chain" refers to flow of business activities of certain products or services of participating parties
- Activities involved are material supply, manufacturing, assembly, distribution (wholesales and retail) to end consumer.
- Supply chain exists in any industry, from the financial sector, manufacturing industry, software industry to government sector.
- Supply chain attack leverages on **trust** on supply chain partners to bypass traditional defenses and compromise a large number of computers.

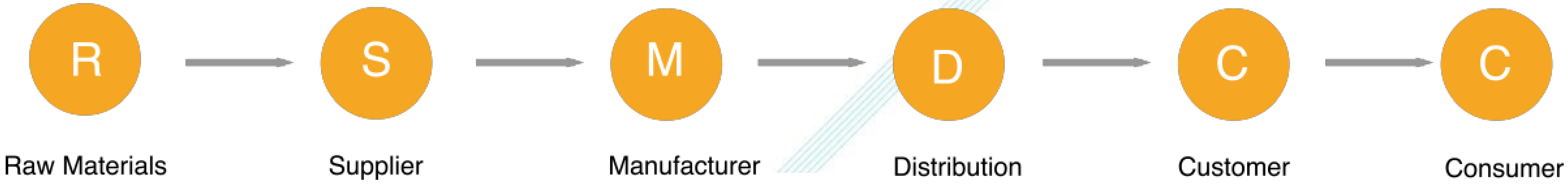


Image source: https://www.wikiwand.com/en/Supply_chain_attack#/citenote30

Forms of Supply Chain Attacks

- Software Update Contamination
- Software Library Contamination
- Firmware Contamination
- Waterhole Attack

Image credit: http://managedit.nyc/author/gpkalm

Supply Chain Attacks in 2017

Software Update Contamination 污染軟件更新機制

- NotPetya ransomware Jul 2017
  - Contaminated accounting software in Ukraine
- Avast’s CCleaner backdoor Aug 2017
  - 2.3M contaminated copies downloaded
  - Attacker targeted 20+ companies with more malware

Legitimate Website Compromise

利用被入侵的合法網站攻擊訪問者

- Bad Rabbit ransomware Oct 2017
  - Citizens in Russia, Ukraine, etc. attacked when visiting popular public websites injected with exploit codes

New challenges to the supply chain in digital transformation

- Cloud services brokerage (CSB)
  - IT role & business model to add values for cloud services
  - Provides aggregation, integration & customization
  - Provides network interface & software API
- Fintech
  - Startups in innovation technologies
  - Blockchain, artificial intelligence, machine learning & aggregation of marketplace
  - Provide services or API to FI
- Smart city and Internet of Things (IoT)
  - Growing number of sensors, actuators, cameras, smart meters, AI, machine learning & analytics services
- Smart Industry (Industry 4.0)
  - Vertical integration of smart factory production line & horizontal integration of supply chain partners
  - Aggregation of production data for big data analytics

Tackling Supply Chain Attacks

- Put third party security management in place
  - Third party risk management, cyber security risk assessment, controls in contract (e.g. right to audit), network separation, software & updates test before deployment

- Require service providers to implement security measures in service provision
  - Incident handling (contact points, timely notification), transparency to security controls, proof of authenticity & integrity to software updates, staff security awareness

- Involve partners and contractors in company-side security awareness programme

https://www.hkcert.org/my_url/en/guideline/18041201

Q&A

HKCERT Hotline: 81056060

www.hkcert.org